Mailgate Ltd.

MailGate
User Manual

King & Associates (www.edking.com) wrote this manual and the help files for Mailgate Ltd.

Revised, Amended and Edited by Lani K. and David D. Thompson.

Contents

Figures

1 Getting Started

MailGate Overview

What is MailGate?

MailGate is a complete Internet access software package. It comprises two integrated parts - a mail server and proxy gateway.

Technical Definition

Mail

MailGate is a LAN POP3 and SMTP Email server with Internet Service Provider (ISP) connection integration for Internet email transmission and collection. It supports Internet Server Providers based on SMTP or POP3 client delivery and works with many different POP configurations at the ISP end.

Gate

MailGate is a full Proxy gateway for HTTP and FTP protocols, Realtime Audio Visual, Liquid Audio and the SOCKS TCP/IP proxy server protocol. In addition it will relay DNS requests and with the 'custom' proxy feature you can setup proxies to do pretty much whatever you want.

The MailGate software package consists of:

- the mail and proxy server software
- an administration program to setup, configure and control the servers
- a setup wizard to get you started fast
- a log file viewing utility to make fine tuning of the system easy
- a number of optional extensions to add extra functionality to your system

Non-Technical Tutorial

For the non-technical users (most of us), see the sections below to go over the terms and concepts used in MailGate.

» **What is a Mail Server?** below

» **What is a Proxy Server?** on page 1-4

What is a Mail Server?

A mail server is a program that resides on one computer in your network that:

- Collects mail from your Internet Service Provider(s)
- Sends outgoing mail to your Internet Service Provider
- Sorts and distributes mail to your users and may have other functionality, such as automatic forwarding of mail. See **What can the MailGate Server Do?** on page 1-5 for more information.

To send and collect your mail, your client mail program connects to the local mail server.

The diagram below shows how a simple mail server works.

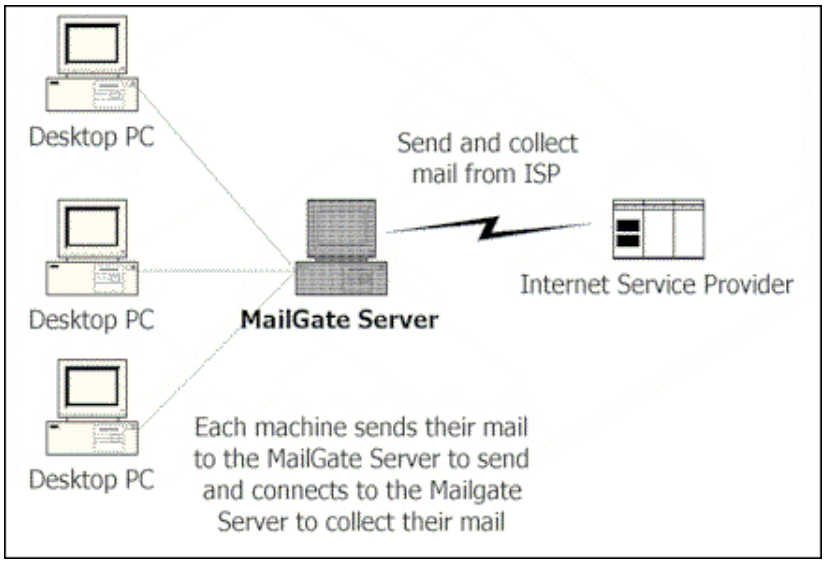

Figure 1 - Simple Mail Server

To continue learning about mail and mail servers, see:

» **What are POP3 and SMTP mail?** on page 1-3

» **What can the MailGate mail server do?** on page 1-3

What can the MailGate Mail Server do?

In addition to collecting, sorting and sending mail, MailGate has a number of features to make management of your email easy. Here are some examples of the more common features:

Automatic Replies

MailGate can send a preset message any time mail is received in a specific mailbox. For example:

- if someone mailed to info@yourdomain you could send a specific information message back as email
- you can also set this to reply that you are on vacation for a specific period and who they should contact in the meantime.

Automatic Forwarding

MailGate can automatically forward mail from one mailbox to another. For example:

- you are on vacation and the mail should be handled by someone else
- several people should see the mail

Send Mail Locally to Other Users

MailGate is a LAN email server. You can also use MailGate to send mail to other users on your network without sending them to your Internet Provider and back again.

Forward Mail to another Mail Server

MailGate can forward mail for defined addresses to another mail server. This can be used to add a POP3 collection capability to mail servers which do not have this facility.

What are POP3 and SMTP Mail?

POP3 (Post Office Protocol) and SMTP (Simple Mail Transport Protocol) are different ways mail can be collected and sent. SMTP is always used to send mail. In a very few cases, your ISP may also use SMTP to deliver mail instead of POP3.

Mail at your ISP can be configured in several ways. It is important to check with your ISP for the exact configuration.

Common POP3 Configurations

Single user at your ISP domain

This configuration gives you a mailbox with a name at your host domain, such as:

- yourname@your_ISP
- jane@mailgate.com

Hostname at your ISP domain

This configuration gives you an unlimited number of mailboxes. Mail is sent to any number of people at the hostname at your ISP domain, such as:

- anyname@yourhost.your_ISP
- mary@myco.your_ISP
- support@myco.demon.co.uk

Your own domain

This configuration gives you an unlimited number of mailboxes. Mail is sent to any number of people at your hostname, such as:

- anyname@your_domain
- support@mailgate.com
- johnb@myco.com

Note

In some situations, your ISP may forward several single accounts to a specific POP3 account for collection. This lets you collect many accounts from a single point. MailGate will sort the mail into individual MailGate mailboxes as it collects them.

What is a Proxy Server?

The word proxy can be defined in general usage as "A person authorized to act for another; an agent or a substitute".

In computer terms, the proxy is a program that acts as your agent between you and some other computer

For example, below is a simple HTTP Proxy Server The proxy server sits between you and the Internet page, acting as your agent.

When you request information from the Web, the proxy server checks to see if it already has that information. If it does not, it then goes to the Web and collects the page for you.

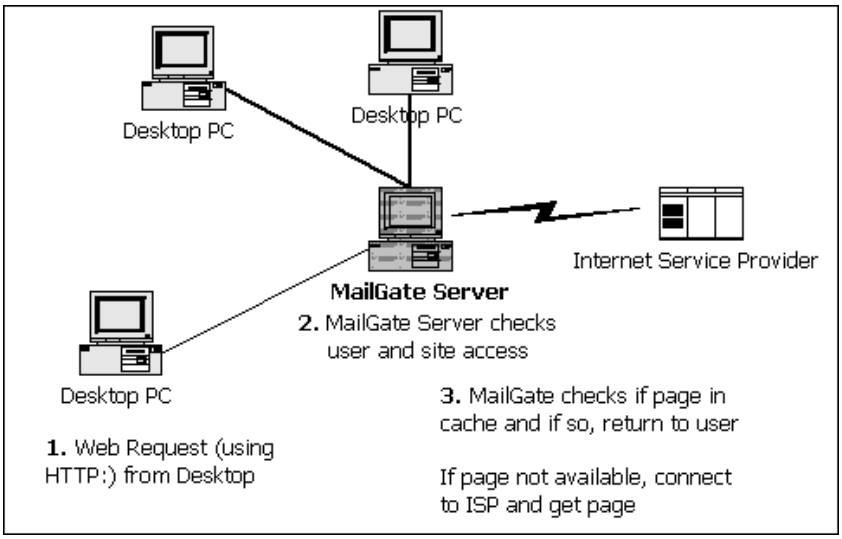

Figure 2 - Simple Proxy Server

To learn more about MailGate and Proxy Servers, see:

What can the MailGate Proxy Server do? below

What are Protocols? below

What are Gateways and Ports? on page 1-6

What can the MailGate Proxy Server do?

MailGate provides a cost-effective way to avoid the problems of putting a modem and phone line on every desktop. It allows low cost concurrent multi-user Internet access and avoids the need for expensive dedicated leased lines and routers.

In addition, with MailGate you can:

- decide **when** people can access the Internet
- decide **who** can access the Internet
- decide **sites** where individual users can/can't access on the Internet

What are Protocols?

A protocol is language that computers use to talk between themselves. Some protocols are formally agreed upon by international standards groups.

Common protocols used with MailGate are:

- POP3 - Post Office Protocol used for mail

- SMTP - Simple Mail Transport Protocol used to send mail and sometimes for receiving mail
- NNTP - Usenet News Transport Protocol used for newsgroups
- HTTP - HyperText Transfer Protocol used with the Web
- TCP/IP - Transmission Control Protocol/Internet Protocol

Fortunately, you don't need to know the details of the protocols used. You do need to know the different names and what areas they relate to so you can fill in the configuration for MailGate.

What are Gateways and Ports?

Envisage that MailGate has created a security wall around your network. It isolates you from the rest of the world. MailGate creates specific named gateways through that security wall.

Consider a medieval walled city, with heavily armoured gates. Each gate leads out of the city to a specific road. Each gate has a patrol monitoring and controlling traffic in and out of the city. It is not much good using the South Gate if you are planning to journey North. In computing terms, these gates are called ports.

In the figure below, each gateway has a name, such as HTTP, FTP. Within each gate, specific ports, given numbers, identify the port and allow traffic in and out.

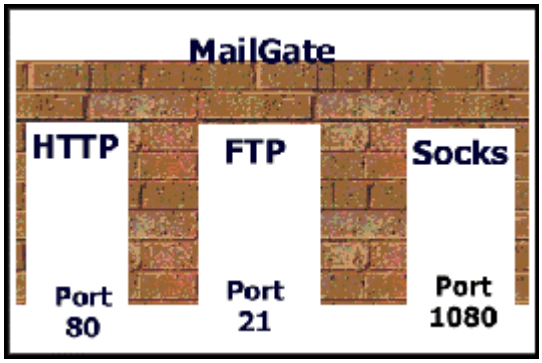

Figure 3 – Gateways and Ports

Using MailGate Gateways

For your workstations to be able to access the Internet successfully you need to use the gateways that MailGate has authorised for traffic in and out of the network.

Real life is a little more complicated than the diagram above. MailGate does the following:

- Listens to a specific port on your network
- Directs traffic on the port to a specific outgoing port

The following figure shows MailGate listening and then directing the traffic to a specific port. Note the two port numbers are not necessarily the same.

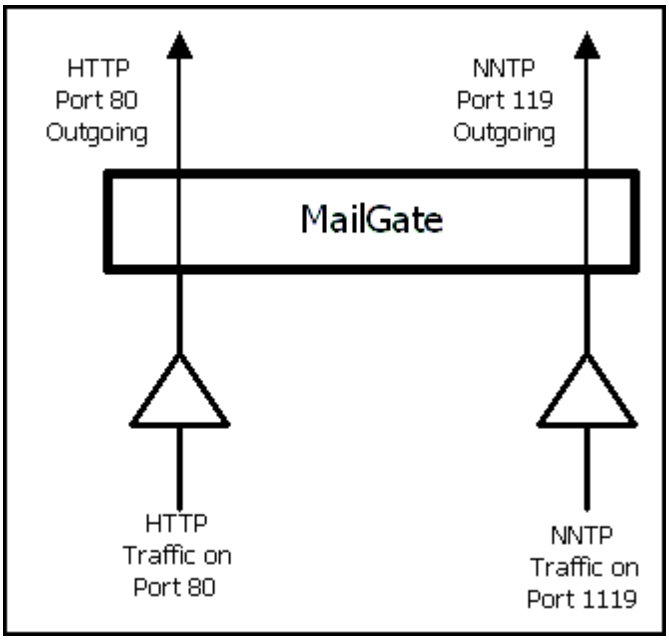

Figure 4 - MailGate Listen and Redirect of Ports

Each service or proxy that MailGate supports uses a specific port. You need to configure each user's workstation browser to point at the MailGate gateways. See **Configuring Clients for MailGate** on page 8-1 for more information on typical client programs.

Note

Only one software application can be linked to any one port. If the MailGate server is **also** a Web or FTP server then the MailGate ports may need to be changed from the defaults. See the **Gateway Setup** chapter on page 3-3 for more detail.

System Requirements

System Requirements

The following is a list of the requirements for a typical setup of MailGate. You should ensure you have completed any setup needed before proceeding with your MailGate setup.

You will need to have the following:

a) TCP/IPGlossTCPIP set up on each computer on your network which will use the MailGate server. If you're unfamiliar with TCP/IP, read the TCP/IP section in this manual or refer to your Windows documentation.
b) Decide on how you wish the MailGate server to connect to the Internet. If this is to be a dial-up connection, then you need to install your hardware, configure dial-up networking and test your connection. If you wish to use a router, then confirm there is a working connection between the MailGate machine and the Internet.

You will need to know the following:

a) The account name and password with your ISP and the name of the dial-up networking configuration.
b) The IP address/name of the machine running MailGate
c) The name and password for the POP account(s) that you wish to collect from
d) Your ISP's POP and SMTP server addresses

To configure your client machines, you will need:

a) The IP address/name of the MailGate server.
b) The users mailbox and password settings.
c) The ports used for each proxy service (if changed).

MailGate TCP/IP Requirements

MailGate uses TCP/IP for all it's network communications. TCP/IP is configured as part of the operating system and must be correctly setup for MailGate to operate successfully.

Static IP Addresses

In most small networks, the easiest way to configure TCP/IP is to use *Static* addressing. With this each machine is given a unique IP number (for example 192.168.1.10). When you want

to connect to a remote machine you refer to it using it's IP number address.

If you use static addresses, when you setup your client machines, you will need to know the IP address of the MailGate machine and it is this you use to identify the server.

Using Names

In larger networks and the Internet it would be difficult to remember the IP numbers associated with each machine. To make it easier, these large networks are normally configured using machine names. To be able to make a connection, these names must be converted to the actual IP number by the IP protocol. This process is called *Name Resolution* and the IP protocol follows a sequence of events to try to find the IP number to use.

When configuring your MailGate server with this type of network you need to ensure every client machine can resolve the IP address successfully. If your network uses DHCP to allocate IP addresses, it is best to use a fixed address for the MailGate machine.

For more information on the setup of TCP/IP, see the **Network Requirements** Section on page 7-1 later in this manual.

Internet Connection Requirements

As MailGate simply uses TCP/IP to connect to other machines, any Internet connection which uses TCP/IP can be used by MailGate. This includes all forms of dial-up connection as well as routed connections using dialing or fixed line routers.

Using Dial-Up Connections

MailGate is designed to make using a dial-up Internet connection easy by providing a comprehensive connection scheduler.

When using dial-up, MailGate passes a request to Dial-up Networking to establish the connection and start TCP/IP. Before configuring MailGate you should install any hardware required (Modem, ISDN Terminal Adaptor etc.) and configure Dial-up Networking to connect to your ISP. You may need to contact your ISP for assistance with the settings and account details required.

When you configure MailGate you will need to know the

phonebook entry name to use and the dial-up account name and password.

Using Routed Connections

When using a router based connection you need to ensure the MailGate machine has the required access to the Internet. If

you use a firewall you may need to adjust its settings to allow MailGate to connect correctly.

For more information on the setup of Dial-up Networking and TCP/IP, see the see the **Network Requirements** on page 7-1 later in this manual.

ISP Account Details

Your ISP account will give you access to both email and other Internet services like web browsing.

MailGate is mainly designed for use with ISP's who provide a POP3 service for incoming mail but it will also work well with those who wish to use the SMTP protocol.

For outgoing mail all ISP's provide access to an SMTP server. Often this can only be accessed if you connect using the particular ISP's connection service.

Your main ISP may also provide access to a proxy server for web browsing.

MailGate can collect mail from any number of POP3 accounts and this collection can be performed in two different ways. See **How MailGate Sorts into Mailboxes** on page 2-12 for more details.

For each ISP mail account you wish to use you will need to know the address (name) of the POP3 mail server and the mail account name and password. You will also need to know the address of your main ISP's SMTP server for outgoing mail.

If you wish to use other services provided like your ISP's proxy server or news server, you should note the details of these services.

Installing MailGate

Installation Overview

To successfully install MailGate on your network you should follow the following simple steps:

a) Install TCP/IP and establish your Internet connection. See **System Requirements** on page 1-8 for more details.
b) Obtain your ISP's account details for you. See **System Requirements** on page 1-8 for more details.
c) Install the MailGate program from your download or CD copy.
d) Configure MailGate using either the configuration wizard or the setup screens.
e) Configure your client machines and software to work with MailGate.
f) Test your installation.

For more information, see:

» **Installing MailGate** below

» **Client Configuration** on page 1-12

Installing MailGate

MailGate is supplied as a single self-extracting and installing executable program. To install MailGate, simply double click on the install file and follow the screen prompts.

When first installed, MailGate will run for 30 days with a 10 user limit. You may purchase a registration key at any time and when this has been entered into the registration screen, your copy of MailGate will become a fully licenced copy.

There are a number of optional modules available, each of which has it's own install executable. To install any of these first complete your MailGate installation then run the module install program and follow the screen prompts.

Configuring MailGate

Once the MailGate program has been installed successfully and you have completed the tasks outlined in the System Requirements section, you are ready to configure MailGate.

To assist with you initial setup you can run the MailGate

Wizard. You will be prompted with this option every time you start the MailGate user program until you either choose not to

use the wizard or complete the process. You can also run this wizard at any time by selecting it in the MailGate Start | Programs entry.

You may also configure MailGate using the setup screens available in the user interface. See **Configuring MailGate** on page 3-1 for more details.

We strongly recommend you take a look through the section Using MailGate to understand the configuration options available before proceeding.

Client Configuration

MailGate is designed as a server based program. To make use of the facilities you will need to install client software on your user machines. Any client program which uses the Internet standards supported by MailGate can be used be used.

In general you will need to configure the following settings:

Mail Clients - You should set both the POP3 and SMTP server addresses to the MailGate machine IP address. The account user name and password should be the users mailbox name and password.

Web Browsers - You should set the browser to connect using a LAN and to use a proxy server. Set the proxy server address for all protocols to the MailGate machine address and HTTP port.

FTP Clients - Set these to use a proxy or firewall and set the address to the MailGate machine. MailGate will expect the client to specify the target host and user name when connecting and the firewall type settings should be set accordingly.

Other Clients - See the client documentation on how to configure these for use with a proxy server. You may also need to make further settings in MailGate to enable these.

More detailed configuration guidelines for the more common client packages can be found in the section **Configuring Clients for MailGate** 8-1 and on our website www.mailgate.com.

2 Using MailGate

MailGate Main Window

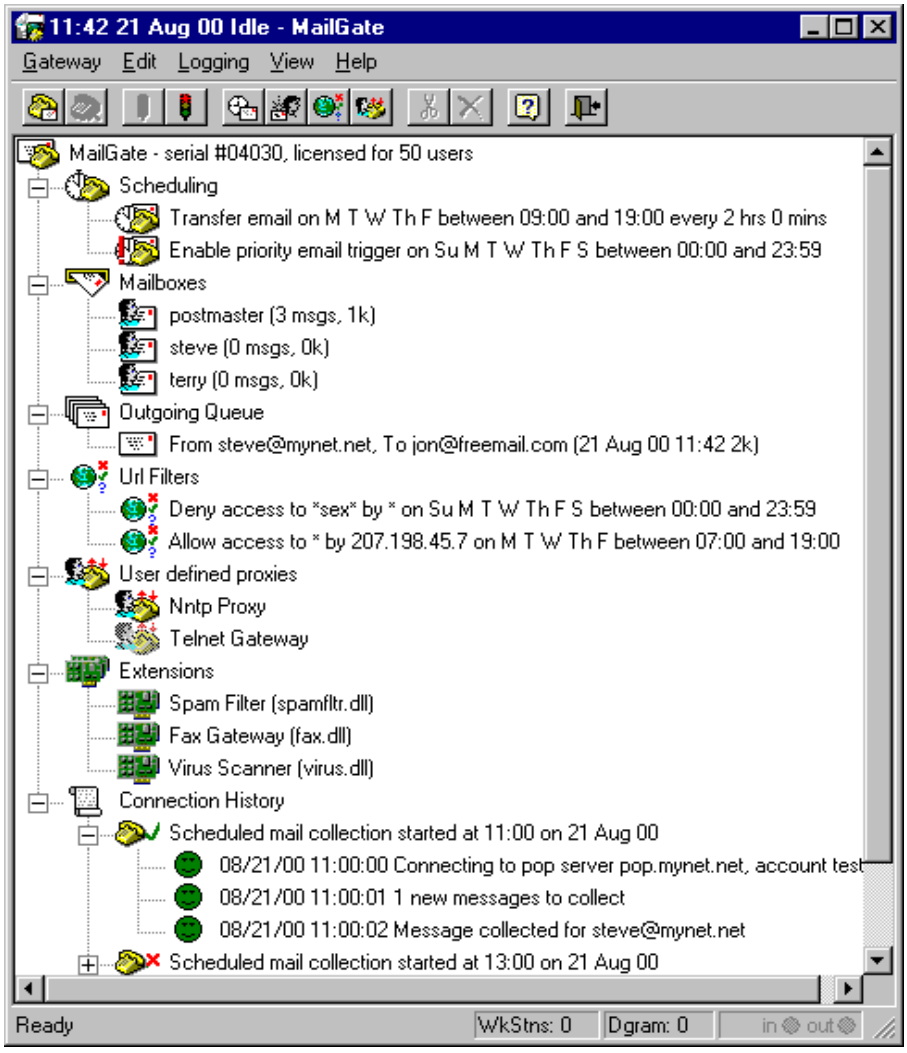

Figure 5 - MailGate Administration Window

MailGate Administrator Window Menus

Gateway Menu

The Gateway menu contains the main configuration options.

Setup - The main Setup dialog. (page 3-3)

Advanced Setup - System security and Timeout settings. (page 3-25)

Large Pop Message Control - Settings to manage the collection of large mail messages. (page 3-35)

Backup Configuration - Backup your settings to a file. (page 3-34)

Restore Configuration - Restore your backed up settings. (page 3-34)

Load Accounts - Create mailboxes from a text file. (page 3-36)

Manual Connect - Force MailGate to make a mail exchange.

Disconnect - Force MailGate to disconnect.

Startup Minimized - When checked the Admin program will start in a minimized state.

Run as Service - When checked the MailGate processing program will run as a background service.

Start Gateway Service - Start the MailGate processing program.

Stop Gateway Service - Stop the MailGate processing program.

Exit - Leave the Administrator Program.

Edit Menu

The Edit menu contains options to change certain settings.

New - Displays a sub-menu for creating new Schedule, Mailbox, Url Filter and Custom Proxy list entries.

Enabled - Check to enable the currently highlighted list entry.

Edit - Edit the currently highlighted list entry.

Info - Display information about the currently highlighted list entry.

Delete - Delete the currently highlighted list entry.

Move up - Move the currently highlighted list entry up in the list.

Move down - Move the currently highlighted list entry down in the list.

Logging Menu

The Logging menu contains options to manage your log files.

Purging - Set how much historical data you wish to keep. (page 3-37)

View Logs - Start the MailGate log file viewer utility.

Logging Options - Check options to define what data is written to the log files. (page 3-37)

View Menu

The View menu contains settings to customize your Administrator display.

Toolbar - Check to display the Toolbar.

Status Bar - Check to display the Status Bar.

Help Menu

The Help menu contains items to help you use MailGate.

MailGate Help - Access the help system.

Registration - Display the MailGate Registration dialog. (page 4-1}

Email for Support - MailGate's in built email creator for support requests. (page 4-2)

MailGate on the Web - Some useful URL's. (page 4-3)

About MailGate - Display the About Screen.

MailGate Administrator Window Icons

Manual Connection Icons

 Click on this icon to force a manual connection to your ISP for a mail exchange.

 When connected to your ISP, click on this icon to force a disconnect.

Service Status Icons

 This indicates the MailGate service process is stopped. Click here to start the Service.

 This indicates the MailGate service process is running. Click here to stop the Service.

For more information see **Starting MailGate** on page 2-7.

Toolbar Icons

 Click on this icon to create a new schedule entry.

See **Using Schedules** on page 2-25.

 Click on this icon to create a new mailbox entry.

See **Using Mailboxes** on page 2-10.

 Click on this icon to create a new URL filter entry.

See **Using URL Filters** on page 2-18.

 Click on this icon to create a new Custom Proxy.

See **Using Custom Proxies** on page 2-22.

 Click here to cut the current data.

 Click here to delete the current entry.

 Click here to display the help window.

 Click here to close the MailGate Administrator.

MailGate Administrator Window

Registration Information

Shows your system serial number and user count. See **Registration** on page 4-1 for information on how to register your copy of MailGate.

Schedule List

Shows a list of the connection schedules that are setup. See **Using Schedules** on page 2-25 for more information.

Note the icon is dimmed if the schedule is setup but not currently enabled.

Mailbox List

Shows a list of your local mailboxes. See **Maintaining Mailboxes** on page 2-14 for more information.

Each mailbox is shown with the number of messages currently stored and the amount of space used.

Outgoing Queue

Shows a list of all mail waiting to be sent out from MailGate to your ISP. See **Using the Queue** on page 2-16 for more information.

URL Filter List

Shows the list of URL filters that are setup to allow or deny access to the Web from specific machines or to specific Web sites. See **Using URL Filters** on page 2-18 for more information.

Note the icon is dimmed if a filter is setup but not currently enabled.

Custom Proxy List

Shows a list of any Custom Proxies that you have setup. See **Using Custom Proxies** on page 2-22 for more information.

Note the icon is dimmed if a Custom Proxy is setup but not currently enabled.

Extensions List

Shows a list of any Extension Modules you have installed. See **Using Extensions** on page 2-31 for more information.

Note the icon is dimmed if an Extension is installed but not currently enabled.

Connection History

Shows information about the last 25 connections MailGate has made. See **Using the Connection History** on page 2-30 for more information.

You can click on each connection report and expand it for more details. Note a green tick indicates a good connection and a red X indicates there has been an error message in the connection.

Administrator Window Status Bar

The Status bar contains:

- The current MailGate status.
- A counter showing the number of user workstations currently connected.
- A rolling counter showing the number of current sessions for each protocol. (Use the right mouse button menu to select what protocol is displayed in this part of the status bar.)
- In/Out lights that flash when MailGate is connected to the Internet and traffic is passing.

Starting the Service

Starting MailGate

When MailGate is installed, there are two parts: the administration and the service process.

If installed as service (the default), the service process is started at machine startup and the admin program can be used to configure and start/stop the service process.

If installed for desktop only mode service process starts and stops with admin program.

Stop and Restart MailGate

If you wish to temporarily stop and restart MailGate service, use the MailGate admin program.

The File | Stop Gateway Service turns off the MailGate services. The File | Start Gateway Services turns MailGate services back on. These options are only available if MailGate is in service mode. When initially installed MailGate will be in service mode.

For ease, click on the  on the toolbar to start the service and on the  to stop it.

Run as Desktop Mode

The desktop mode makes the service component of MailGate start and stop as you start and stop the admin component. In this mode you can think of the MailGate system as a single program.

You can switch MailGate into desktop mode by unchecking the 'Gateway | Run as Service' menu option. To switch back to service mode simply re-check this option.

Be aware that when in desktop mode MailGate's services will only be available to your network users whilst the admin program is running. Logging off your desktop session for example will stop the MailGate services.

For this reason we advise that for normal operation you stay in service mode.

See also **Command Line Options** on page 2-8.

Command Line Options

As long as the MailGate service is started, you can use either of the following command lines to start an email connection and transfer:

```
mailgate -connect

mgatesvc -connect
```

In addition the mailgate.exe program can be used to start or stop the MailGate service from a batch file or script:

mailgate –start	Starts the service
mailgate –stop	Stops the service

The mgatesvc.exe program can be used with the following command line options:

mgatesvc –start	Starts the service
mgatesvc –stop	Stops the service
mgatesvc –install	Installs mgatesvc as a system service
mgatesvc –remove	Removes mgatesvc from the system services
mgatesvc –console	Runs the mgatesvc process on the desktop in a console window

See also **Starting MailGate** on page 2-7.

Using the Mail Server

Mail Server Planning

Plan MailGate Setup

To plan the configuration of the Mail Server you will need information from:

a) Your Internet Service Provider with specific information for access to their system and your mailboxes. See **What is POP and SMTP Mail** on page 1-3 for information on type of mailboxes.

b) Information about your Network TCP/IP setup such as your domain name. For more information about setting up TCP/IP, see **Network Preparation** on page 7-1.

Setup Mail Server

To setup the Mail Server, you need to do the following:

a) Plan and then create the mailboxes in MailGate that you require and setup any special actions for mailboxes, such as forwarding to another account, that you require.

b) Setup the global information in the Gateway | Setup dialog, including the mail accounts to collect from your ISP.

For more information, see:

Setup the Mail Server below

Planning Mailboxes on page 2-10

Setup the Mail Server

This section is a quick overview of the information needed to setup the mail server.

To setup the mail server, you enter information on four tabs. To access the tabs select the Gateway menu and click on Setup. The following tabs are used for Mail Server setup:

Dialup Tab

If you use a dialup connection, the Dialup Tab specifies the

Dial-Up Entry of your Internet Service Provider and the account name and password used to logon.

This account is common for the Mail Server and all gateways.

If you have a leased line, specify NO DIALUP in the Dial-Up Entry.

For more information, see **Dialup Tab** on page 3-3.

POP Tab

The POP Tab lists the mailboxes to collect. These can be from any mail server than can be reached through your ISP connection.

For each account you must specify the account name, password and mail server to collect from

For more information, see **POP Tab** on page 3-5.

Domains Tab

The Domains Tab specifies any domain that you want to handle on your network and not forward to your ISP.

This allows mail to be sent from one local mailbox to another local mailbox without sending via the remote ISP mailbox(es).

The Domains Tab also specifies how to handle unknown addresses - whether to return to the sender or send to a specific MailGate mailbox.

For more information, see **Domains Tab** on page 3-9.

Email Tab

The Email Tab enables the Mail Server within MailGate.

For outgoing mail, you must also specify the mail server used by your ISP.

For more information, see **Email Tab** on page 3-11.

Lan Forward Tab

The Lan Forward Tab enables MailGate to forward mail to another mail server on you LAN using SMTP. This could be another copy of MailGate or servers such a Microsoft Exchange or Lotus Notes.

You define an address pattern match to use when deciding which mail is to be forwarded.

For more information, see **Lan Forward Tab** on page 3-14.

Using Mailboxes

Planning Mailboxes

You need to setup at least one local mailbox in MailGate for each person to collect their mail.

The name of the local mailbox is used by MailGate to determine where to sort collected mail. See **How MailGate Sorts into Mailboxes** on page 2-12 for more information.

Determine Mailbox Routing

In a very simple setup, each remote POP account would have a corresponding MailGate mailbox. The Postmaster account is used for any other mail received and when MailGate does not know where to sort mail.

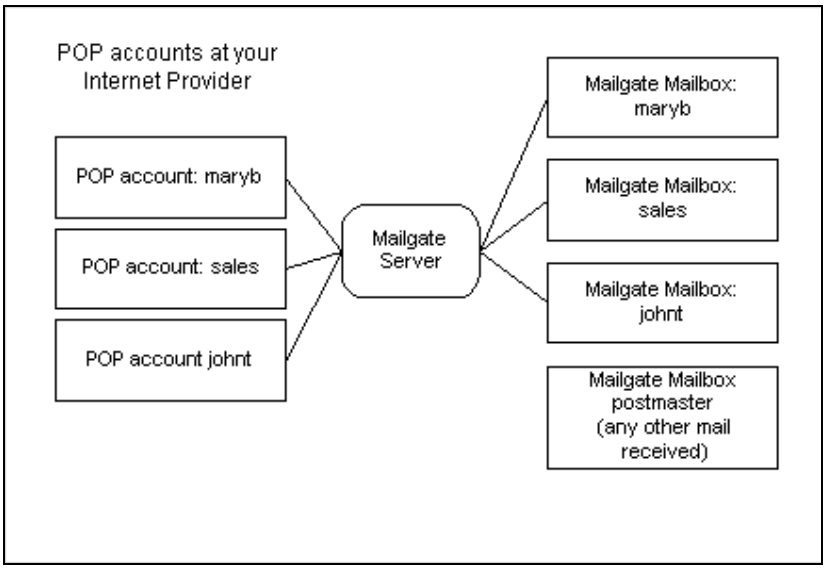

Figure 6 - Simple Mail Routing

For another example of mail sorting, see **Planning Mailboxes - Advanced Example** below.

Planning Mailboxes – Advanced Example

A support department wants all mail sent to their support account, copied to the individual support people. In addition, they want a mailbox where requests for common questions will be answered automatically.

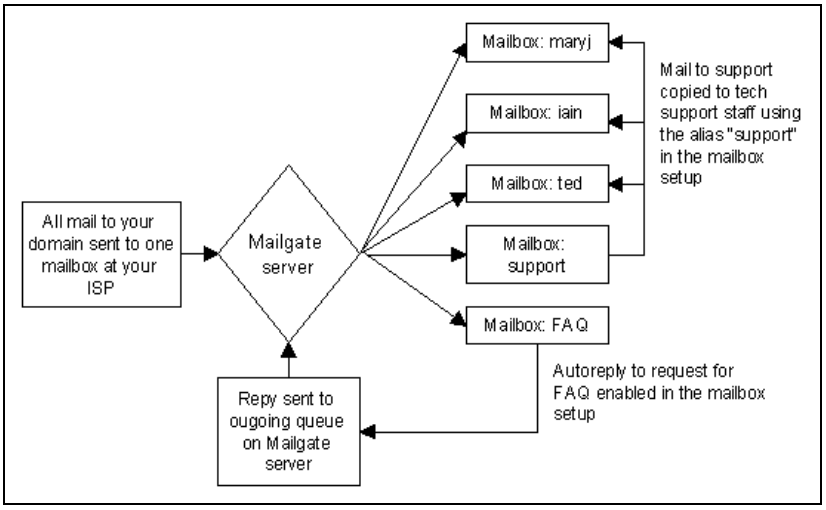

Figure 7- Advanced Mail Routing

How MailGate Sorts into Mailboxes

MailGate can be configured to collect POP3 mail by one of two methods.

If the collection details are specified against a user mailbox - see Mailbox Options on page 3-40 - then all collected mail is simply placed in that user's mailbox.

If the collection is specified in the POP collection tab on page 3-5 then MailGate uses rules to search the incoming mail headers and determine to which mailbox incoming mail should be delivered.

Analyze the Mail Header

The mail is analyzed in the following steps:

a) Search for specific header fields (listed below) and look for a match using the whole address. If found, deliver the mail to the mailbox.
b) If no match found on whole address, look for match of the address filter pattern specified when the mailbox was setup.
c) If the header fields are not found, continue the search for additional fields and look for match of the address filter pattern specified when the mailbox was setup.
d) Take the full address with the domain name and compare against all mailbox and aliases names.
e) If no match found, strip the domain name from the address and deliver to all mailboxes that have a matching name or alias.

By default, the address filter pattern is * means any text. You can set specific patterns. See **Set a Specific Pattern for Mailbox Sorting** on page 2-13 for more information.

Header fields searched first

The mail header is scanned for the following fields:

- Apparently-To:
- X-Apparently-To:
- X-Originally-To:
- Envelope-To:
- <the string entered in the custom field on the pop dialog>

If the field is found, it is compared to the address filter pattern and if matched (the default is *) this address is selected and searching stops.

If more than one of the above exist whichever is nearer the start of the header and matches the filter will be used.

Special Routing

If the custom header field for routing entry contains:

To:*

MailGate sorts using only the TO and CC header fields.

If header fields not found

If none of the above result in a match, the search is then done for a "Received: * for * field" with an address that matches the address filter pattern.

If this fails then email addresses are taken from the TO and CC fields if they match the address filter pattern. When matching TO and CC fields, the emails 'Message-Id:' field is also checked against a list of recently received Message-Ids. If the message id has been already processed the email will be discarded.

This is done since if an email is sent to multiple recipients within an organization there may be multiple copies in the ISP pop account. The to/cc method will deliver a copy to all recipients when processing the first message. The recent message id file expires entries older than 3 days.

After the filter has been applied, any options specified in Remove Occurrences or Map Address are applied.

Delivery to mailbox when address found

Each address obtained above then has the domain part stripped and is then delivered to the mailboxes that have a matching name or alias.

Note that if multiple accounts have the same alias and that is the delivery address, each account will receive a copy.

Setting a Specific Pattern for Mailbox Sorting

MailGate analyses the email headers as described in **How MailGate Sorts into Mailboxes** on page 2-12.

If an address matches the pattern filter, then MailGate will accept the mail and sort it into a mailbox. You can have more than one pattern, but each must be on a separate line.

For example if you set the filter as *@mailgate.com, MailGate will ignore any addresses not for that domain. In particular, if MailGate uses the To/CC addresses to route email, set the filter to your domain to ignore other address in these fields.

See Using Wildcard Expressions in MailGate for more information.

For information on mail sorting rules, see **How MailGate Sorts into Mailboxes** on page 2-12.

Tip

You can put your domain name as the filter (*@yourdomain) so MailGate only looks at those addresses to sort mail.

You can also use Aliases for a mail box for sorting. See **Aliases for a Mailbox** on page 3-41 for more information.

Maintaining Mailboxes

After you have planned your local mailboxes, you need to actually create them and set any options.

 Create New Mailbox

a) Click on the above toolbar icon or select the Edit menu, click on New and select Mailbox.
b) Enter the name for the local mailbox
c) Enter the password and then re-enter in the confirmation box

For more information, see MailBox Settings.

Once you have created local mailboxes, you may want to change or remove them later.

Edit a Mailbox

a) Select the mailbox to edit
b) Double click on the mailbox name or select the Edit menu and click on Edit

Delete a Mailbox

a) Select the mailbox to delete
b) Select the Edit menu and click on Delete
c) MailGate will ask you to confirm deletion of the mailbox, which includes deleting any unread mail.

Tip

If you have a large number of mailboxes to create, you can use a text file to enter the accounts. See **Load Accounts** on page 3-36 for more information.

Checklist for Mail Box Planning

	Task
☐	What remote mailboxes do you have from your ISP?
☐	Which remote mailboxes at your ISP should go to which local mailboxes in MailGate?
☐	Should any special patterns be set for sorting into local mailboxes?
☐	Should any mail be copied from one local mailbox to another local mailbox?
☐	Should any local mailbox be autoresponded to?
☐	Should mail be deleted or forwarded after the auto response?
☐	What will be the default local mailbox and who will read it?
☐	How do you want to handle large messages?

Figure 8 - Checklist for Mail Box Planning

Using the Outgoing Queue

Outgoing Queue

The Outgoing Queue shows all mail that is waiting to be sent the next time MailGate connects.

For each mail message, the following is displayed:

a) Who sent the message (FROM field)
b) The intended recipient (TO field)
c) The date the message was put in the queue
d) The size of the message

Delete Message from the Queue

You can not edit a message once it is in the outgoing queue but you can delete it.

1. Select the mail message
2. Select the Edit menu and click on Delete
3. Confirm that you want to delete the message

Requeue if Errors

If there is a problem sending a mail message, MailGate will requeue the message and try on the next connection.

Information about Outgoing Messages

You can get some additional information that is very useful for tracking errors. In addition to the standard information shown, you can highlight an outgoing message and use Edit | Information to display the **Queued Message dialog** (see 3-44) with the following:

- Queued - when the messages was re-queued for sending after an error
- Last tried - the last time MailGate tried to send the message
- Last error - the last error message

Note

Outgoing mail is stored in the QUEUE subdirectory under the MailGate system directory.

Using the Proxy Gateways

Proxy Gateway Overview

MailGate supports the following standard proxies:

- Web - World Wide Web proxy and cache.
- FTP - File Transfer Protocol
- SOCKS - version 4 and version 5
- DNS Relay
- RealTime Audio Visual
- Liquid Audio

In addition you can configure any number of Custom Proxies to provide a proxy capability for other applications.

For further information on using the proxies, click see below:

» **Using the Web Proxy** below

» **Using URL Filters** on page 2-18

» **Using the FTP Gateway** on page 2-19

» **Using the SOCKS Gateway** on page 2-19

» **Using DNS Relay** on page 2-20

» **Using RealTime Audio Visual** on page 2-21

» **Using Liquid Audio** on page 2-22

» **Using a Custom Proxy** on page 2-22

Using the Web Proxy

The Web proxy will pass HTTP protocol or browser requests to the Internet.

To use the Web proxy you should set your workstation browsers to '*Use a proxy server*' and specify the MailGate machine address to identify the proxy. See the section on **Configuring Clients** on page 8-1 for guidelines.

You can control your users access to this service in a number of ways. See the pages below on how this may be done.

» **Require User Authentication** on page 3-16

» **Using URL Filters** on page 2-18

» **Setting Advanced Security** on page 3-25

» **Using the Scheduler** on page 2-25

To use the Web proxy, you will also need to consider the following:

Internet Connection

Ensure you have established your method of connecting to the Internet. See **Internet Connection Requirements** on page 1-9 for more detail.

The Web Tab on page 3-16

Enable the Web proxy. Optionally you can change the port used by this service and enable MailGate to pass web requests through your ISP's web proxy.

Cache Tab on page 3-24

Review the settings for the management of your web cache. MailGate constantly runs a low priority job to monitor and clear the web cache. This operates only when no other activity is on the computer.

URL Filters on page 3-45

You can create URL filters to control your users access to the web.

The DNS Tab on page 3-21

If your users are going to use certain web applications you may need to enable the DNS relay.

Using URL Filtering

URL filtering applies only to the Web Proxy. It allows you to:

- allow or deny machine in your network to access the Web
- allow or deny access to Web sites
- set what times the filters are active

You can use wildcards (see 9-1) when specifying either which machines have access or Web sites may be visited. See **Using Wildcard Expressions** on page 9-1 for more detail.

 To Create a URL Filter

Either click on the above icon on the toolbar or select the Edit menu and choose URL Filter. This will display the **URL filter detail** dialog on page 3-45.

Order of Filters

The order of the filters is important. When there are multiple filters, MailGate uses the first filter entry it finds with a match

for both the machine name and the URL and will act on the Allow/Deny setting.

You can drag and drop the filters in the main MailGate window or use Move Up/Down on the right mouse button menu to change the order.

For example, if you want to limit access only to a few specific web

sites on all machines, you would list the ones they could access first and the last URL filter would deny access to all other web sites:

- Allow access to www.macromedia.com* by * (all machines)
- Allow access to *.microsoft.com* by * (all machines)
- Allow access to *.mailgate.com* by * (all machines)
- Deny access to * by * (all machines)

You can have the machine and URL patterns in different filters:

- Deny access to *sex* by * (all machines)
- Allow access to * by MACHINE1
- Deny access to * by MACHINE2

Machine1 can access the web, but not any sites with the letters SEX in them. Machine2 can not access the web at all.

Using the FTP Gateway

The FTP proxy will pass FTP protocol requests to the Internet.

To use the FTP proxy you should set your workstation FTP client to use a proxy or firewall. MailGate requires the client to pass the target FTP host and user name to the proxy in the format USER *userid@hostname*.

You can control your users access to this service in a number of ways. See the pages below on how this may be done.

Setting Advanced Security on page 3-25

Using the Scheduler on page 2-25

To use the FTP proxy you will also need to consider the following:

Internet Connection

Ensure you have established your method of connecting to the Internet. See **Internet Connection Requirements** on page 1-9 for more detail.

The FTP Tab on page 3-18

Enable the FTP proxy. Optionally you can alter the port used for this service.

Using the Socks Gateway

The Socks proxy will act as a Socks server and pass Socks requests to the Internet.

Socks is a protocol wrapper which allows applications to pass data requests to a Socks server. The Socks server then *unwraps* the request and communicates directly with the target host. To use Socks

either your client application must be able to communicate using the Socks protocol or you will need to install a Socks client and run your application from within this. For more information about Socks, visit www.socks.nec.com.

You can control your users access to this service in a number of ways. See the links below on how this may be done.

Setting Advanced Security on page 3-25

Using the Scheduler on page 2-25

To use the Socks proxy you will also need to consider the following:

- **Internet Connection**

  Ensure you have established your method of connecting to the Internet. See **Internet Connection Requirements** on page 1-9 for more detail.

- **The Socks Tab** on page 3-19

  Enable the Socks proxy required. Both Socks Ver 4 and 5 are supported. Optionally you can change the port used by this service and enable MailGate to pass web requests via the Web proxy, making use of the cache.

- **The DNS Tab** on page 3-21

  If your users are going to use certain applications you may also need to enable the DNS relay. This is often a requirement when using Socks V4.

Using DNS Relay

The DNS relay will pass client DNS (name resolution) requests to your ISP's DNS server.

To use the DNS relay you should set the DNS server setting found in the TCP/IP properties on your client workstations to the MailGate machine address if your network does not have a DNS server. If your network already has a DNS server, then you should consult your network administrator before making any changes.

Notes

1. DNS relay is required for some web based Java applets to work and should be enabled if you are using these through the Web Proxy.
2. Socks 4 systems often require this if there are any references by machine name.
3. This service is NOT required to allow the MailGate machine to resolve addresses when communicating with the Internet. Correct configuration of your Internet connection will enable this capability.

If you are not sure if you need this service, it is generally best **NOT** to enable it as it can result in MailGate making unnecessary connections due to general DNS requests being passed around your network.

You can control your users access to this service in a number of ways. See the page below on how this may be done.

Setting Advanced Security on page 3-25

To use the DNS Relay you will also need to consider the following:

- **Internet Connection**

  Ensure you have established your method of connecting to the Internet. See **Internet Connection Requirements** on page 1-9 for more detail.

- **The DNS Tab**

Enable the DNS relay and specify your ISP's DNS server address(es). You can optionally enable DNS reverse look-up for security checks. See the **DNS Tab** on page 3-21 page for more details.

Using the RealTime Audio Visual Gateway

The RealTime® Audio Visual proxy will pass Realtime client requests to the Internet.

To use the RealTime proxy you should set your RealTime client to use a proxy and specify the MailGate server address. Be aware that once the client is active, you may see un-requested connections being made. The client software, by default, will try to connect to update itself.

For more information about RealPlayer® see www.realaudio.com.

You can control your users access to this service in a number of ways. See the sections below on how this may be done.

Setting Advanced Security on page 3-25

Using the Scheduler on page 2-25

To use the RealTime proxy you will also need to consider the following:

- **Internet Connection**

  Ensure you have established your method of connecting to the Internet. See **Internet Connection Requirements** on page 1-9 for more detail.

- **The Realtime AV Tab** on page 3-20

  Enable the RealTime proxy. Optionally you can alter the port used for this service.

Using the Liquid Audio Gateway

The Liquid Audio proxy will pass Liquid Audio client requests to the Internet.

To use the Liquid Audio proxy you should set your Liquid Audio client to use a proxy and specify the MailGate server address.

For more information about LiquidAudio® see www.liquidaudio.com.

You can control your users access to this service in a number of ways. See the links below on how this may be done.

Setting Advanced Security on page 3-25

Using the Scheduler on page 2-25

To use Liquid Audio proxy you will also need to consider the following:

- **Internet Connection**

  Ensure you have established your method of connecting to the Internet. See **Internet Connection Requirements** on page 1-9 for more detail.

- **The Liquid Audio Tab** on page 3-23

  Enable the Liquid Audio proxy. Optionally you can alter the port used for this service.

Using Custom Proxies

Using Custom Proxies

The Custom Proxy facility allows you to create your own proxy services to pass non-standard protocol or client requests to the Internet.

A default installation of MailGate includes two examples of Custom Proxies, supplied to support NNTP and Telenet. To configure and use these services, see the pages below.

Using the NNTP Proxy on page 2-23

Using the Telenet Proxy on page 2-23

To use your own Custom Proxy you will need to instruct your client application to use a Proxy or a Firewall and specify the MailGate server address. You will also need to know the Port number the application uses, the host server to communicate with and the type of data used. For full details on making these settings, see the **Custom Proxy detail** on page 3-47.

You can also make settings for each proxy to control your users access to the service based on both time and IP address settings.

If your client application requires multiple ports, then you should consider using the Socks facility instead of a number of Custom Proxies.

Using the NNTP Proxy

The NNTP example Custom Proxy will pass NNTP (News) protocol requests to the Internet.

To use the NNTP Proxy, you should set your Newsreader client to reference MailGate. See **News Client Configuration** on page 8-9 for information on some common newsreaders.

To configure the NNTP proxy for use, follow the steps below:

1. Double click on the NNTP Example Custom Proxy
2. Title - give the Custom Proxy a name
3. Check Proxy Enabled
4. Proxy listens on port - the standard NNTP port is 119
5. Select Streams Connection
6. Valid requests passed through - enter the name of the news server to connect to
7. The requests are normally passed through port 119, the standard NNTP port
8. Check when the proxy is active
9. Check "The proxy uses the dial up connection" if this is your method of connection
10. Review any security settings required

For full details on any of the screen fields, see the Custom Proxy Settings on page 3-47.

Using the Telnet Proxy

The Telnet example Custom Proxy will pass Telnet protocol requests to the Internet.

To use the Telnet Proxy, you should set your Telnet client to reference MailGate.

The Telnet Proxy has an associated script that asks for the site you want to connect to with Telnet. This allows one Proxy to access multiple telnet locations.

To configure the Telnet proxy for use, follow the steps below:

1. Double click on the Telnet example Custom Proxy
2. Title - give the Custom Proxy a name
3. Check Proxy Enabled
4. Proxy listens on port - the standard Telnet port is 23
5. Check the 'Run Script' box
6. Check when the proxy is active
7. Check "The proxy uses the dial up connection" if this is your method of connection
8. Review any security settings required

For full details on any of the screen fields, see the Custom Proxy Settings on page 3-47.

Using the Scheduler

Using the Scheduler

The MailGate scheduler has three types of schedule which serve slightly different purposes.

To create a new schedule, select Edit | New | Schedule to open the schedule dialog or click on the  icon on the toolbar. To edit an existing schedule, highlight the schedule and select Edit | Edit or double click on it. For full details on the available fields, see **Schedule Details** on page 3-39.

Types of Schedule

Each of the different schedules is listed below. See the pages below for more detail on the settings available.

Email Transfer Schedules

These schedules allow you to fine tune how MailGate uses your Internet connection to transfer external email.

Email Transfer on page 2-26 - Fixed periodic connection to transfer external email.

Priority Email Trigger on page 2-26 - An override to send mail marked as high priority.

Outgoing Email Trigger on page 2-27 - An override to send any outgoing mail.

Email Transfer after Idle Period on page 2-27 - Makes a connection if there has been no other activity within a given period.

Service Availability Schedules

Each proxy service in MailGate has it's own **Service Enabled Schedule** on page 2-28. Each of these works in the same way and they are listed in the schedule dialog as Web Proxy Enabled, Ftp Proxy Enabled, Socks Gateway Enabled, Realtime AV Gateway Enabled and Liquid Audio Gateway Enabled. With this type of schedule you can control what times your users can access the service. **Note** - If you want a service to be available all the time then you do not need to create a schedule for it.

Connection Control Schedules

These allow you to fine tune how your Internet connection is used.

Keep Connected on page 2-28 - Once established MailGate will not close the connection during the active period.

Timeout Override on page 2-28 - Overrides the standard timeout period to make best use of minimum call duration charges.

You can create as many schedules as you wish to allow different connection profiles to be active at different times of day or days of the week.

Email Transfer Schedule

The "Email Transfer" option is the basic email connection option.

This schedule allows you to collect mail on a periodic schedule within a time frame, such as during the week, weekends and evenings.

You can set several schedules for Email Transfer to meet your needs, such as:

- Every hour during the week and working hours
- Every four hours during the evening during the week
- Once a day on the weekend

Minimum redial time

An amount of time that must pass between the last mail collection and the time this schedule is to run.

For example,
The minimum redial is set at 15 minutes
MailGate is scheduled to collect mail on the half hour.
At 10:20 during a proxy connection, MailGate checks for new mail
At 10:30 after checking the minimum redial time, MailGate will not run this occurrence of email transfer, since less than 15 minutes has passed since the last mail collection.

Priority Email Trigger Schedule

The "Priority Email Trigger enabled" option allows mail to be sent immediately if it contains a priority field.

When MailGate receives mail to send out, it reads the mail header looking for a Priority field in the header. MailGate will read both a Priority and X-Priority field.

If the priority is set High and Priority Mail Trigger is enabled in the scheduler, MailGate will connect immediately and send all waiting mail.

If the Priority Mail Trigger is not enabled, the mail is sent on the next connection to your ISP.

You can set the day(s) of the week and the hours that this schedule is enabled.

Minimum redial time

An amount of time that must pass between the last mail collection and the time this schedule is to run.

For example,
The minimum redial is set at 5 minutes
MailGate is scheduled to collect mail on the half hour.
At 10:20 during a proxy connection, MailGate checks for new mail
At 10:30 priority email is received by MailGate. Since the minimum redial time has passed, MailGate will send the mail immediately.
At 10:33 another priority email is received. This time, MailGate will wait until 10:35 to send the mail.

Outgoing Email Trigger Schedule

The "Outgoing Email Trigger enabled" lets you set a time period where MailGate will connect as soon as it receives mail to be sent to your ISP.

You can set the minimum redial dial time.

Minimum redial time

An amount of time that must pass between the last mail collection and the time this schedule is to run. This allows you to make sure that outgoing mail does not wait too long to be sent.

For example,
The minimum redial is set at 5 minutes
At 10:20 during a proxy connection, MailGate checks for new mail
At 10:30 outgoing mail is received by MailGate. Since 5 minutes has passed since the last mail collection, MailGate sends the mail immediately.

Email Transfer after Idle Period Schedule

The "Email Transfer after Idle Period" lets you define a periodic interval to connect and collect mail after the last connection was made. You can define what days of the week and hours you want this schedule to be active.

After

The After value, specifies how much time (in hours and minutes)

must pass since the last mail connection was made. Once this time has been reached, MailGate will connect and collect mail.

This option works with all other scheduling options. For example, you can collect mail during proxy connections, but make sure mail is collected if there has not been a proxy connection recently:

In Gateway | Setup | POP tab, set MailGate to check for mail whenever a proxy connection is made and check during the connection for the specified time period.

Set an "Email Transfer after Idle Period" to 1 hour. If there has been no proxy connection for an hour, then MailGate will collect email.

Service Enabled Schedule

Each proxy service has it's own enabling schedule. These schedules schedule set the days of the week and the start and end time that the proxy service can be used.

By default, all the services can be run at any time. Use the scheduler to limit the time period.

Keep Connected Schedule

The "Keep Connected" schedule keeps the line connected during the specified time period.

If the connection is lost for any reason, MailGate will re-connect the next time the line is requested.

Timeout Override Schedule

Many telecommunications providers vary their charges according to the time of day and/or day of the week. The "Timeout Override" schedule allows you to define a call timeout profile to match your telecommunications provider. The schedule defines both the minimum call time and the subsequent timeout, within a given overall time period.

Example

Your telecommunications provider charges a minimum of one unit and then uses per second billing. At the weekend one unit is 5 minutes, but during the week, one unit is 3 minutes.

You wish to ensure the best use is made of the unit cost, but ensure the line is dropped within 1/2 a minute when per second billing is on.

Timeout Schedule #1:

- Check days for Monday through Friday
- Set the minimum call to 0:3 (3 minutes)

- Set the timeout to 0:30 (30 seconds)
- Set the start time to 00:00 and the end time to 23:59
- Check the schedule enabled box

Timeout Schedule #2:

- Check the days Saturday and Sunday
- Set the minimum call to 0:5 (5 minutes)
- Set the timeout to 0:30 (30 seconds)
- Set the start time to 00:00 and the end time to 23:59
- Check the schedule enabled box

Using the Connection History

Using the Connection History

When MailGate connect to your ISP, it creates a log of the session activity. This log is displayed in the main MailGate window under Connection History and is stored in the LOG subdirectory as the file HISTORY.DAT

The log is automatically purged and shows the last 25 connections. Icons in the connection history display information about the connection:

 Indicates an error in the connection

 Indicates there was no error in the connection

 The action had an error

 The action completed successfully

This log is a summary of the activity only. Full details of the connection can be found in the main MailGate log files. See **Logging** on page 3-37 for more information.

Using Extensions to MailGate

There are a number of optional extension module which can be used to add to the capability of MailGate. For details of the current options and their functionality, visit our web site www.mailgate.com.

When an extension is installed in will appear in the Extensions section of the MailGate administrator screen. To configure the extension, highlight it and select Edit | Edit or double click on the icon. For full details, see the help associated with the module.

When an extension is installed, MailGate processes emails in the following way:

- MailGate receives the email and builds a list of all recipients to send it to.
- Each recipient address and a copy of the mail is passed to each extension installed. The address is passed to each extension in the order displayed in the Admin screen.
- If the extension returns a "continue processing" flag, the address is passed to the next extension.
- If the extension returns a "stop processing" flag, all processing of the address ceases.
- Once the address has been passed to all extensions and a "continue processing" flag is passed, MailGate processes the address for normal mail delivery.

The Extensions section lists all extensions currently installed modules and shows them in the processing order. You can highlight an extension and use the Edit | Move Up/Move Down buttons to change the order.

3 Configuring MailGate

Configuring MailGate

Once the MailGate program has been installed successfully and you have completed the tasks outlined in the System Requirements section, you are ready to configure MailGate.

To assist with you an initial setup you can run the **MailGate Wizard**. You will be prompted with this option every time you start the MailGate user program until you either choose not to use the wizard or complete the process. You can also run this wizard at any time by selecting it in the MailGate Start | Programs entry. This wizard will guide you through a set on the most common settings to get you started.

You may also configure MailGate using the setup screens available in the user interface. If you wish to extend you usage of MailGate or set it to do something a little more unusual then you will need to use these screens.

We strongly recommend you take a look through the section **Using MailGate** to understand the configuration options available before proceeding.

In this section you will find details of all the settings and features available on a screen-by-screen basis.

See the pages below to learn about individual configuration areas.

Gateway | Setup on page 3-3 - For the main setup dialogs for MailGate.

Gateway | Advanced Setup on page 3-25 - For system security and timing settings.

Gateway | Large pop Message Control on page 3-35 - To set your controls for large messages.

Gateway | Backup/Restore on page 3-34 - To save your MailGate settings.

Gateway Setup

Gateway Setup

The Gateway | Setup section contains the screens for most of MailGate's operational settings.

Dialup Tab

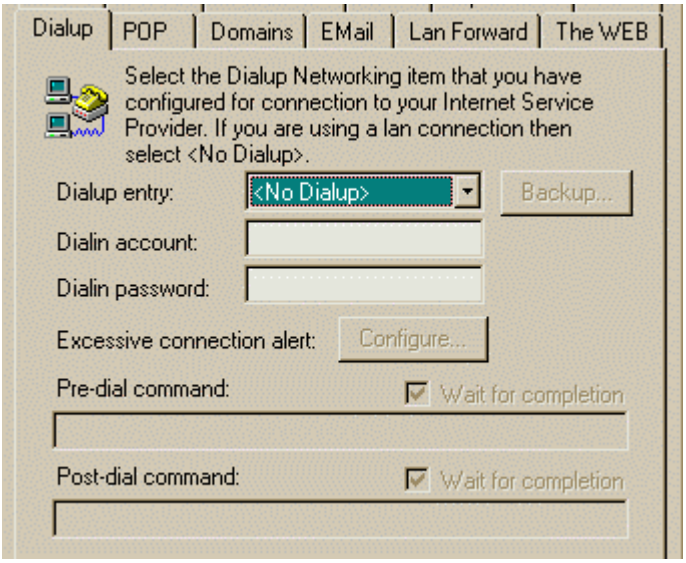

Figure 9 - Dialup Tab

Connection Method

The Dialup Tab specifies the primary method to connect to the Internet and an optional backup connection. For leased lines or open connections to your ISP, specify <No Dial Up> as the DUN entry. See **Backup Dialup Entry** on page 3-4 for more information on alternative connection to use.

The account name and password are the information from your ISP to logon to your account.

Pre-dial and Post-dial Command

The pre-dial and post-dial command options allow you to specify any command to happen before or after dialing your connection. Check "wait for completion" to make sure the command(s) complete before the next action.

See **Excessive Connection Alert** on page 3-4 for information on closing the connection after a specified time.

Backup Dialup Entry

The Backup Dialup Entry allows you to specify an alternative Dialup Phonebook entry to use if the primary connection can not be made.

Select the alternative entry using the dropdown and specify the username and password for this alternative account.

Note - Many ISP's will not allow access to their mail servers (particularly SMTP) from an external connection. You may find that when MailGate uses your backup dialup that mail sending and collection errors occur.

Excessive Connection Alert

The Dialup Networking Alert dialog sets the maximum time for a connection in hours and minutes and what to when the amount of time is reached.

When the time limit is reached, MailGate can do one or more of the following:

Force a disconnection

Send the MailGate administrator an advisory mail. The administrator mail address is set on the Gateway | Setup | Email Tab in the "System reports to" field.

Sound an audible alarm on the machine where MailGate is running.

POP Tab

Figure 10 - POP Tab

The POP tab lists all POP accounts that MailGate collects from. Pressing the ADD or EDIT button, calls the POP Collection dialog box with details for each account.

See **POP Collection Details** on page 3-6 for more information on individual account settings.

Options

In the options section of the dialog you can tell MailGate how often to check for incoming mail while the connection is active for a proxy session and you can adjust the length of time MailGate will wait while inactive before dropping the connection.

All mail collected by these settings will be passed to the mail routing system. See **How MailGate Sorts into Mailboxes** on page 2-12 for more detail on this process. You can also collect mail by setting a pop collection against a user mailbox. In this case the sorting process is bypassed. See **Maintaining Mailboxes** on page 3-40 for more detail on this option.

POP Collection Details

The POP Collection dialog has the details for each POP account that MailGate collects from. It may also be used to trigger other processes, such as starting an SMTP mail feed from your ISP.

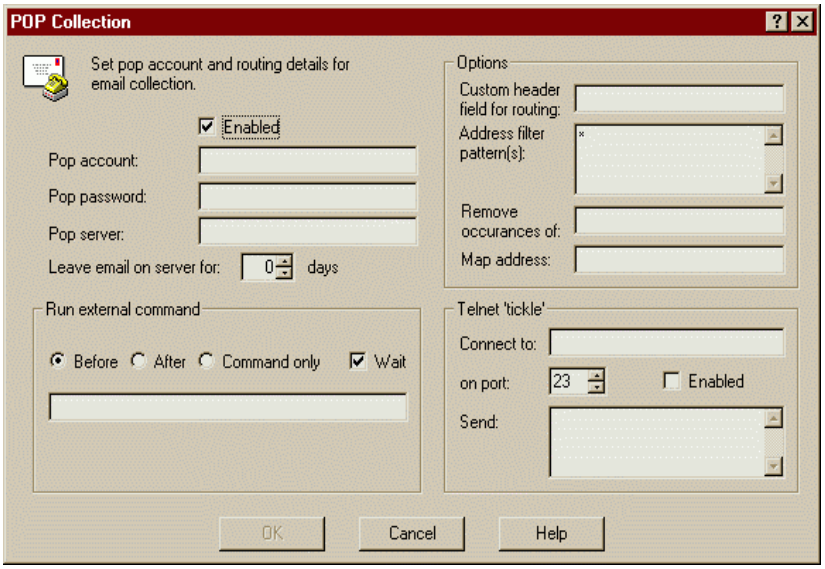

Figure 11 - Details for POP Account Setup

POP Collection Mode

For a standard POP collection you will need to complete:

- the account name
- the password for this account
- the POP mail server to collect from

These details will have been supplied by your ISP.

You should select the Login Method to use. Most ISP's require the standard User + Pass method. If in doubt you should try this setting first.

You may also set the Leave Mail on Server option. This option allows mail that you've collected to be retained on your ISP's mail server for the specified number of days. This can be used as a backup or to allow you to collect the mail from different locations, such as at home and the office. There are three options:

- 0 to delete mail immediately after collection
- 1-30 for number of days to leave on the server. MailGate will automatically manage a list of the mail it has collected.
- -1 to leave the mail on the server forever. Note this may be a problem with some ISPs if the mailbox size gets very large.

Using this option requires your ISP to support the UIDL command for mail tracking. If it is not working, please consult your ISP.

Optional Settings

There are a number of optional settings which can be made to help adjust the mail routing process to allow for the range of different processes used by ISP's.

To fully understand the process you should refer to **How MailGate Sorts into Mailboxes** on page 2-12 before making any changes.

Custom Field for Routing

This field allows you to specify a mail header field to look for to determine which local mailbox to place the mail in. By default the mail header is scanned for the following fields:

- Apparently-To:
- X-Apparently-To:
- X-Originally-To:
- Envelope-To:
- <the string entered in the custom field on the pop dialog>

If the field is found, it is compared to the address filter pattern (below) and if matched (the default is *) this address is selected and searching stops.

If more than one of the above exist whichever is nearer the start of the header and matches the filter will be used.

There is also a special setting of *To:** which may be used here to force MailGate to use the To: and Cc: fields for address data.

Address Filter

Set a filter pattern here to reject any addresses which are not yours. If an address matches the pattern filter, then MailGate will accept that address and sort it into a mailbox.

For example if you set the filter as *@mailgate.com, MailGate will ignore any addresses not for that domain. In particular, if MailGate uses the To/CC addresses to route email, you must set the filter to your domain to ignore other address in these fields.

You may also use the *negate* wildcard setting (!) to exclude specific addresses from being accepted. For example, with the above an additional entry of !mail@mailgate.com will prevent this address from being accepted.

Remove Occurrences of

This option allows you to specify a string to be removed before the mail address is processed.

Some ISP or mail systems may add additional data to the normal

mail address for security or system purposes. This option allows the additional string to be removed before processing by MailGate.

Map Address

This option is used mainly with **LAN forward** option on page 3-14 to allow the mail address to be manipulated before forwarding.

The "Map Address" setting allows the alteration of email addresses extracted from the collected messages, using the following rules:

If the setting is blank, no alterations are done

If an email domain is specified, such as "mydomain.com" or "@mydomain.com", then the domain part of each address is replaced with the domain name specified in the map address option

If the setting is a complete email address, such as "tech@mydomain.com", then every email address is replaced with the address specified in the map address option.

Run External Command

This option gives the ability to run a program or script as part of a mail collection. (For example to "finger" a SMTP server).

The command can be set to run:

- Before the POP Collection
- After the POP Collection
- Only run the command. With this POP account need be specified and no collection will be done.

The Wait check box controls whether the collection process waits (suspends itself) until the spawned process terminates or carries on straight away.

Telnet tickle

If your ISP is using SMTP instead of POP3 to send your mail they may require a connection or some text to be sent in order to wake up the mail delivery. The telnet tickle option can be used to do this. As with the Command Only option above, telnet tickle may be used without performing a POP collection.

You will require the following information:

- The machine address to connect to. Your ISP should have this information
- The port to use - the default is 23 for telnet.
- The text characters to send, if required

Domains Tab

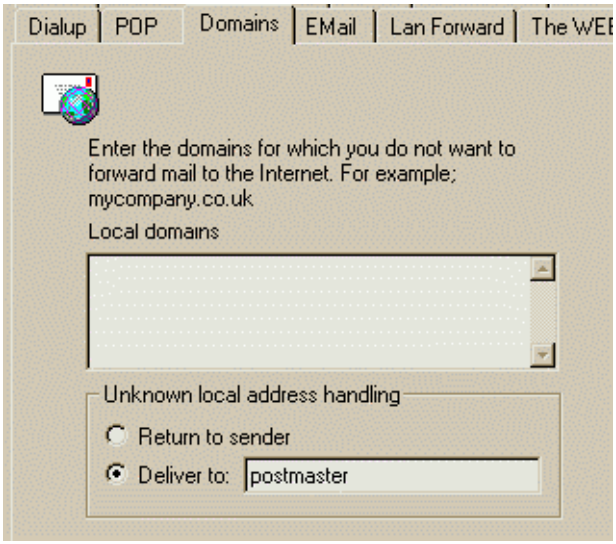

Figure 12 - Domains Tab

Domain Handling

The Domains Tab sets which email domains are for local delivery and which are sent by your Internet Service Provider. In addition, on the Domains tab you specify what to do with mail addressed to an unknown user (i.e. there is no matching mailbox).

In most cases, the Domains Tab will contain the local network Domain name so mail from one person to another within the domain is sent locally.

Exceptions to Local Domain

In addition to the domain name, it is possible to specify a specific user address to be included or excluded from the local list. For example, if the Domains tab contained:

mydomain.net	Mail to anyone@mydomain.net would be handled locally, unless an exception is listed below
!jim@mydomain.net	The ! negates the rule, so that mail to jim@mydomain.net will be sent externally to your ISP.

This is useful for organizations with more than one office but only one email domain.

If most mail is to be sent to your ISP, you can list only the user IDs that should be sent locally. Note that the domain name is not specified.

jim@mydomain.net
fred@mydomain.net

So those particular accounts are local and anything else in a domain

gets sent by your ISP.

Unknown Local Address Handling

If MailGate does not know in which mailbox to place a message, it looks to this option to decide what to do. You can:

1. Have the mail returned to the sender. This will be done including a standard failed delivery message. If you wish to create your own message, create a text file containing your message using the file name bounce.txt and place in the MailGate system folder.
2. Have the mail sent to a specific MailGate mailbox

For more information, see **How MailGate Sorts into Mailboxes** on page 2-12.

Email Tab

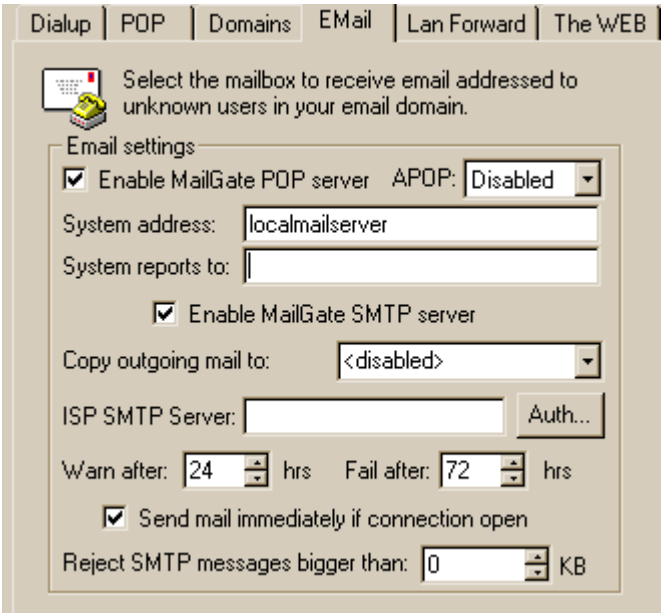

Figure 13 - Email Tab

The Email tab is used to set many of the general settings for MailGate's mail servers. On this tab you can enable the MailGate POP server, used by your users to collect their mail, and the SMTP server, used by your users to send mail into MailGate for delivery.

Normally Required Settings

The following settings are normally required by MailGate's email system.

ISP SMTP Server - If you use MailGate to send external mail, you must specify the address of your ISP's SMTP server. All outgoing mail will be sent to this server for distribution around the Internet. If your ISP requires you to use authenticated login before sending mail, click on the **Auth...** button to turn on authentication.

System address - the FROM field to be used by MailGate admin reports and messages. This should be a full email address, generally in your local domain, such as mailserver@yourdomain.com.

Note: if your forward your administration messages to an external address, be sure to use a full email address for the System Address. Some ISPs validate the FROM field looking for a local address before accepting mail.

System reports to - this is the mail address that MailGate will send administrative messages to. This can be the name of a MailGate mailbox or a full email address (internal or external).

Optional Settings

APOP - MailGate's POP server supports encrypted login using the

APOP command. Select if you wish the POP server to accept or require users to login using APOP authentication. You may have to adjust your email client setting to use APOP. The default for normal POP3 operation is to disable APOP.

Outgoing copy - you can have a copy of all outgoing mail it sent to a specific MailGate mailbox.

Warn After - the number of hours a message can stay in the outgoing queue before a warning message is sent to the originator. The default is 24 hours. The warning can be disabled by entering 0 hours.

Fail After - the number of hours a message can stay in the outgoing queue before a failure message is sent to the originator and MailGate stop trying to send the message. The default is 72 hours.

If you enter 0 hours, MailGate will never fail a message and will keep trying indefinitely.

Send mail immediately if connection open - MailGate will connect to the ISP's SMTP server if the connection is currently open, to send an outgoing mail. If unchecked, outgoing mail will be held until the next scheduled mail exchange.

Reject SMTP messages bigger than - MailGate will reject messages from your users if they are larger than the maximum size in kilobytes. Note - this option is intended to prevent accidental sending of extremely large messages and if triggered it simply cuts the user connection when they try to send the message. This will normally cause an error in the users mail client and should therefore be set with caution. The default setting of 0 disables the option.

SMTP Authentication Details

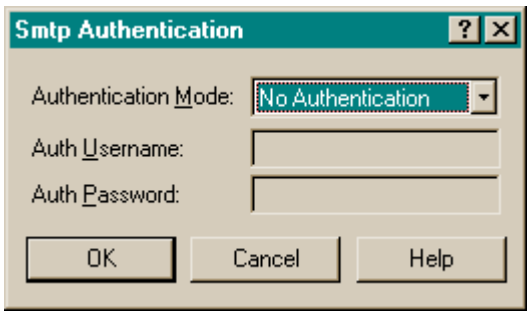

Figure 14 - Smtp Authentication Details

Some ISP's require you to use Authenticated Login to their SMTP server before you can send a mail. This is used to prevent unauthorised relaying of mail through the server.

MailGate provides support for the Auth Login method of authentication which requires a username and password to be sent to the server before sending the mail.

Authentication Mode

Use the dropdown to select the authentication mode to use. Three modes are available:

1. No Authentication - Select this if your ISP does not require authentication
2. Dialin User/Pwd - Use the Dialin username and password specified on the Dialup tab for login to the ISP's server.
3. Specified User/Pwd - Use the username and password specified on this dialog for login to the ISP's server. Use this option if you do not use dialup or you dial into another provider.

Enter the SMTP account username and password to use if you have selected the Specified User/Pwd mode.

LAN Forward Tab

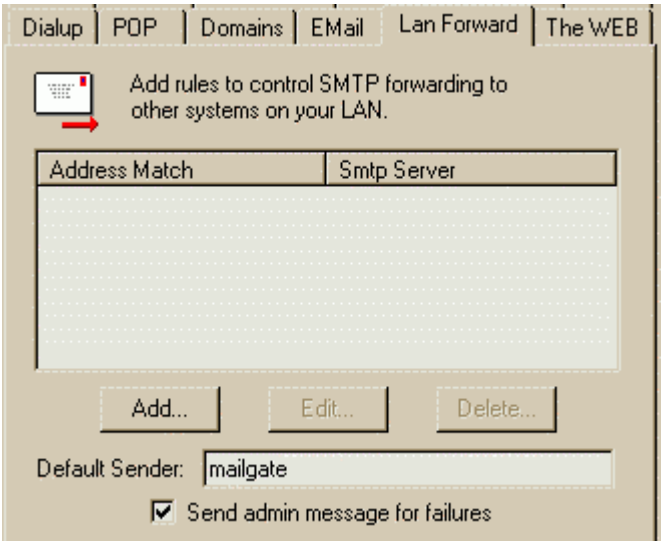

Figure 15 - LAN Forward Tab

The LAN Forward function is used when you have multiple SMTP mail servers on your network or if you wish to use MailGate as a mail collection and delivery agent for another server, for example MS Exchange.

In the LAN Forward tab you specify any number of mail address patterns to look for and decide which messages should be forwarded to another server. Use the Add/Edit buttons to create or change these address patterns, using the **Lan Forward detail** dialog on page 3-15.

Example, if you have two offices and the following setup:

1. All mail to the main office is directed to name@**company1.com**
2. All mail to the remote office is directed to name@**company2.com**
3. The remote server is named "Remote1"

Then the MailGate rule for LAN Forward would be:

*@**company2.com** forward to **Remote1**

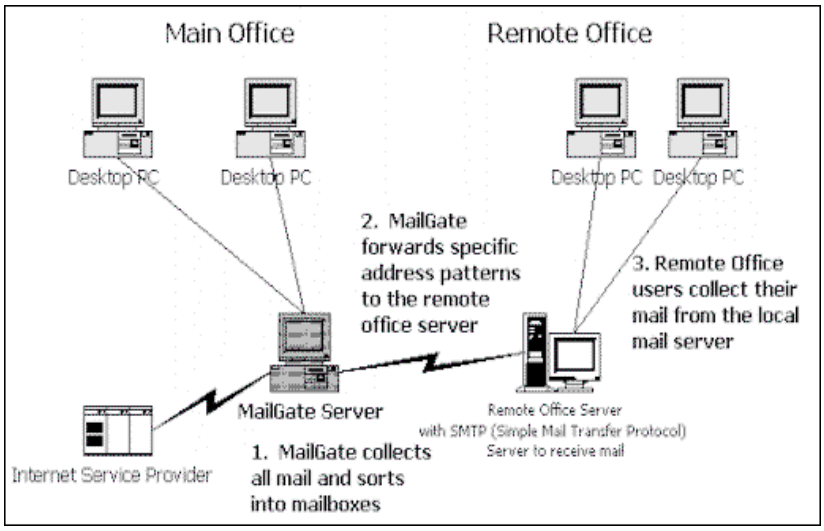

Figure 16 - Lan Forward

Default Sender - Enter the email address you wish to be used if MailGate encounters a problem establishing the From: data when forwarding a message.

Send admin message for failures - If you forward all mail messages to another server, you should uncheck this. If MailGate encounters a problem forwarding mail it will send an advisory message to the *System reports to* address specified on the **Email Tab** on page 3-11. If this address is also forwarded, then a loop can occur in the event of the link between the servers being down.

LAN Forward Detail Screen

In the LAN Forward Detail screen you define the settings for this LAN forward pattern entry.

Address Pattern - Use wildcards (see 9-1) to specify the pattern of addresses to be forwarded. For example *@company2.com.

Smtp Server - the address of the server to forward to.

Smtp Port - the port to use.

Default Recipient - If MailGate encounters a problem establishing the recipient or sending to the extracted address, it will default to using this setting.

The Web Tab

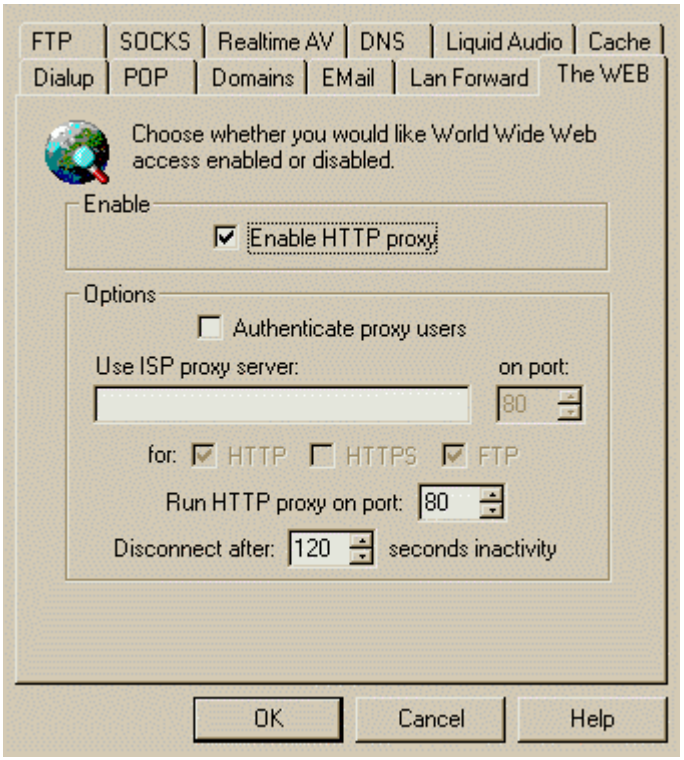

Figure 17 - Web Tab

Check the Enable HTTP Proxy option to enable the MailGate web proxy service.

Optional Settings

Authenticate Proxy Users - If checked, this option requires users to enter a logon and password before they can use the web proxy service. The logon names and passwords available are set by the MailGate mailbox names and their passwords.

ISP Proxy Server - Instead of MailGate connecting directly to a target host web site, you may prefer to use your ISP's Proxy server (if available). You may also select which protocols are passed through this server and which should make a direct connection. Using an ISP's proxy can improve performance but may give some reliability problems.

Run HTTP Proxy on port - If you have a local web server running on the same machine as MailGate, it may be using the standard HTTP port - Port 80. As only one application on a machine can use a port, you will have to run the MailGate Web proxy on a different port. The standard one for this situation is 8080. Ensure you set your client programs to connect to MailGate on your alternative setting.

Disconnect After - Once a connection has been made with your ISP, MailGate will monitor the session activity. If there is no activity for the *Disconnect Time* period then MailGate will request the connection be closed. The default period is 120 seconds.

If MailGate is making frequent connections to your ISP for HTTP requests, you may want to increase the Disconnect After setting. The line will be open a little longer, but MailGate will make fewer phone connections. This should also help response times.

FTP Tab

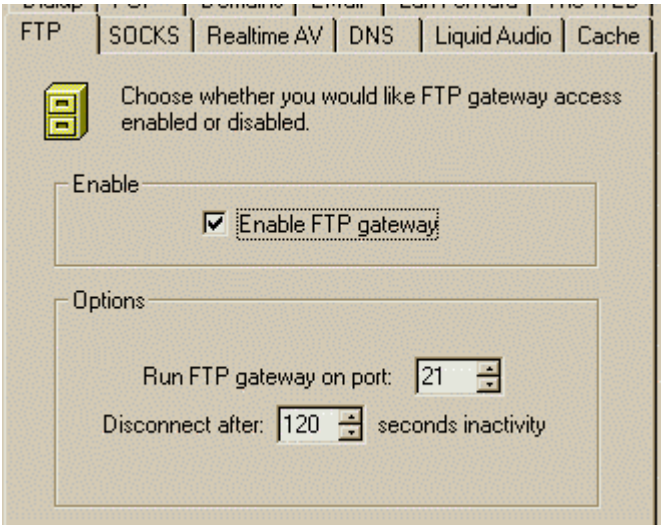

Figure 18 - FTP Tab

Check the Enable FTP Proxy option to enable the MailGate FTP proxy service.

Optional Settings

Run FTP Proxy on port - If you have a local FTP server running on the same machine as MailGate, it may be using the standard FTP port - Port 21. As only one application on a machine can use a port, you will have to run the MailGate Web proxy on a different port. The standard one for this situation is 2121. Ensure you set your client programs to connect to MailGate on your alternative setting.

Disconnect After - Once a connection has been made with your ISP, MailGate will monitor the session activity. If there is no activity for the *Disconnect Time* period then MailGate will request the connection be closed. The default period is 120 seconds.

If MailGate is making frequent connections to your ISP for FTP requests, you may want to increase the Disconnect After setting. The line will be open a little longer, but MailGate will make fewer phone connections. This should also help response times.

Socks Tab

Figure 19 - Socks Tab

MailGate supports both version 4 and version 5 of SOCKS. For more information on Socks, see www.socks.nec.com

Check the Enable options to enable the MailGate SOCKS service you require.

Optional Settings

Pass HTTP request through Web Proxy - Check this option to allow MailGate to check the local web cache.

Run SOCKS gateway on port - The default for this is port 1080. As only one application on a machine can use a port, if you already use this port you will have to run the MailGate proxy on a different port. Ensure you set your client programs to connect to MailGate on your alternative setting.

Disconnect After - Once a connection has been made with your ISP, MailGate will monitor the session activity. If there is no activity for the *Disconnect Time* period then MailGate will request the connection be closed. The default period is 120 seconds.

RealTime AV Tab

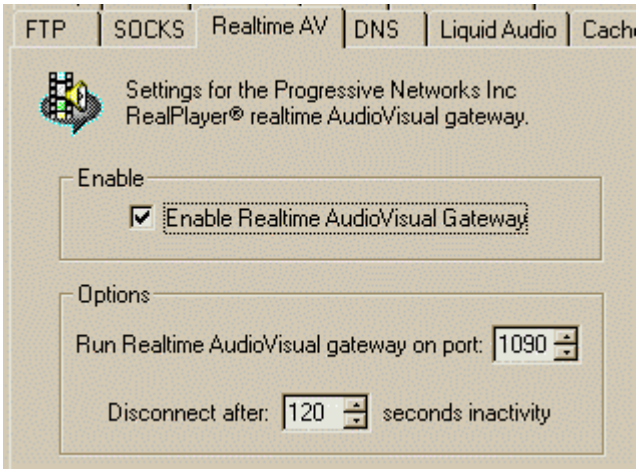

Figure 20 - RealTime AV Tab

Check the Enable Realtime AudioVisual Gateway option to enable the MailGate proxy service.

Optional Settings

Run Realtime AV gateway on port - The default for this is port 1090. As only one application on a machine can use a port, if you already use this port you will have to run the MailGate proxy on a different port. Ensure you set your client programs to connect to MailGate on your alternative setting.

Disconnect After - Once a connection has been made with your ISP, MailGate will monitor the session activity. If there is no activity for the *Disconnect Time* period then MailGate will request the connection be closed. The default period is 120 seconds.

For more information about RealPlayer® see www.realaudio.com

DNS Tab

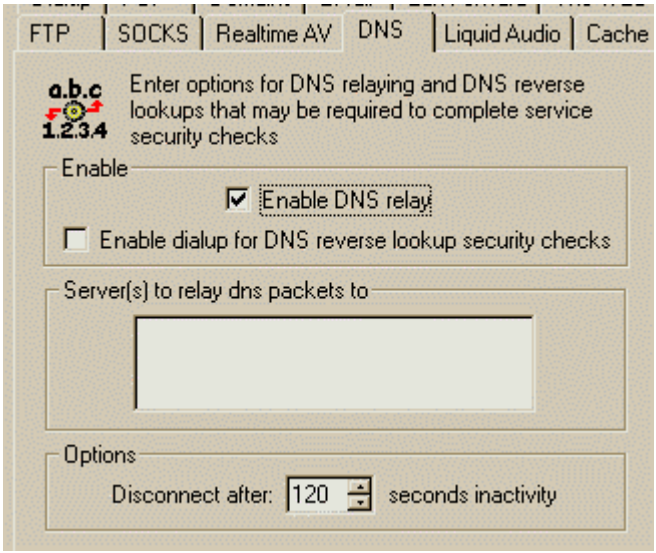

Figure 21 - DNS Tab

Check the Enable DNS relay to enable the MailGate DNS relay service. You will also need to specify at least one DNS server to query. This will normally be your dialin ISP's DNS server.

Optional Settings

Enable dialup for DNS reverse lookup security checks - If you set security settings in the Gateway | Advanced setup using machine names, this option tells MailGate to dialup your ISP to lookup the machine name belonging to an IP address (reverse lookup) for the allow/deny access checks. Normally you will not use this option.

Disconnect After - Once a connection has been made with your ISP, MailGate will monitor the session activity. If there is no activity for the *Disconnect Time* period then MailGate will request the connection be closed. The default period is 120 seconds.

If MailGate is making frequent connections to your ISP for DNS requests, you may want to increase the Disconnect After setting. The line will be open a little longer, but MailGate will make fewer phone connections. This should also help response times.

DNS relay is normally only required if you are running Internet applications on your workstations such as:

- Java applets which need to make a connect by machine name.
- Socks 4 systems if there are any references by machine name.

Enabling DNS relay when it is not required can give rise to spurious connections being made to your ISP for no obvious reason.

To correctly use DNS relay, you will need to specify the MailGate machine address as the DNS server in the network settings on your client workstations.

Liquid Audio Tab

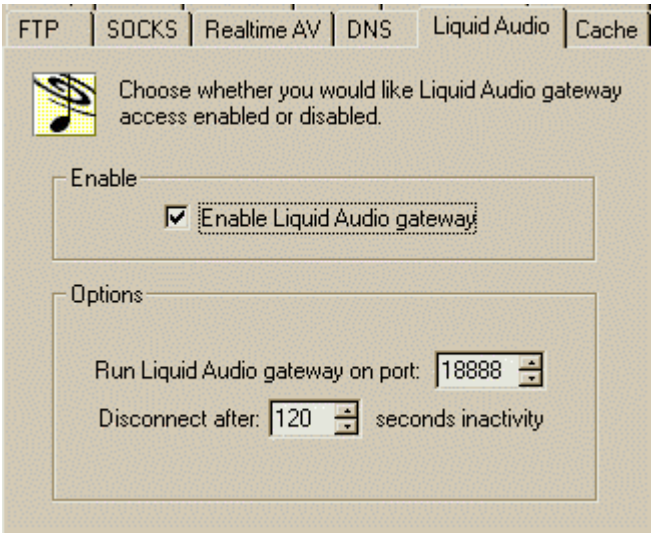

Figure 22 - Liquid Audio Tab

Check the Enable Liquid Audio Gateway option to enable the MailGate proxy service.

Optional Settings

Run Liquid Audio gateway on port - The default for this is port 18888. As only one application on a machine can use a port, if you already use this port you will have to run the MailGate proxy on a different port. Ensure you set your client programs to connect to MailGate on your alternative setting.

Disconnect After - Once a connection has been made with your ISP, MailGate will monitor the session activity. If there is no activity for the *Disconnect Time* period then MailGate will request the connection be closed. The default period is 120 seconds.

For more information about Liquid Audio, see www.liquidaudio.com

Cache Tab

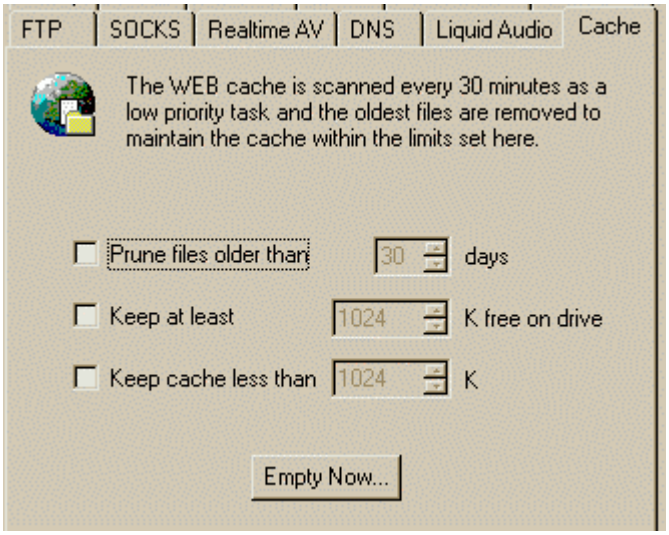

Figure 23 - Cache Tab

The Web Cache stores web page data that is specifies as static. This is determined by the web data header information. Dynamic web pages (for example, forms results)
are not cached.

MailGate runs the low priority cache management job in the background to check the cache parameters and delete old information. MailGate will always delete oldest data first until all criteria are met.

On the Cache Tab you can set the Cache criteria both by age and cache size as well as request the current cache be cleared.

Note - You can exceed limits specified in the Cache tab until the next time the cache management task is run.

Gateway Advanced Setup

Gateway Advanced Setup

The Gateway | Advanced Setup section contains the settings used to set the MailGate security and timeout options. You should review your security settings but generally should not change the timeouts.

Security Tab

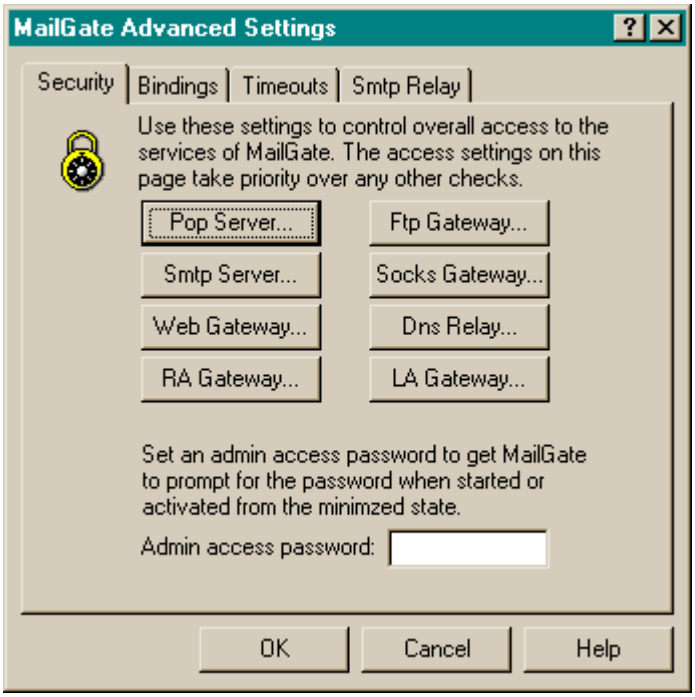

Figure 24 - Security Tab

The security tab allows you to set allow or deny access to each of the standard functions in MailGate. This access check is made before all other checks. You can set similar access rights on any custom proxies, see the Custom Proxy detail page (3-47) for more information.

To set the access rights, select the service you wish to configure and this will display the Allow or Deny access dialog.

You should ensure after installing MailGate you set security options using either these settings or the Bindings (3-28) settings (or a combination of both) to at least prevent unauthorised access to your system by external users.

Admin access password

You can optionally set a password here which will be required to access the **MailGate** administrator program.

Allow or Deny Access

Use this dialog to set the access rights for the current service. You may either explicitly allow or deny access by machine IP address. You can also use wildcards (see 9-1) and set an address pattern.

In addition to the standard wildcards, there are two special notations for specifying IP address ranges for this setting.

To specify all addresses in a subnet range

Enter <any address in the desired subnet range>/<the number of bits used for the subnet>

Example - 192.168.0.1/24

With this example the first three octets form the subnet and the entire last octet is assignable. The range of addresses is therefore similar to 192.168.0.*

Example - 192.168.0.32/27

With this example the first three octets and the first 3 bits of the last octet form the subnet and only the last 5 bits of the last octet are assignable. The range of addresses is therefore 192.168.0.32 to 192.168.0.63, because the range is for the 32 addresses of which 192.168.0.32 is a member.

To specify a specific range of addresses

Enter <starting address in the desired range>/<the number of bits used for the subnet> - <end point of range>

Note - this option is limited to a range defined by using numbers in the last octet.

Example - 192.168.0.4/24-8

With this example the first three octets form the subnet and the entire last octet is assignable. The range of addresses is therefore 192.168.0.4 to 192.168.0.8.

Example - 192.168.0.35/27-38

With this example the first three octets and the first 3 bits of the last

octet form the subnet and only the last 5 bits of the last octet are assignable. The range of addresses is therefore 192.168.0.35 to 192.168.0.38. Note in this case the start and end of the range must both lie in the same subnet range.

If you wish to use machine names, MailGate must be able to reverse look up an IP address to establish the name associated with it. This will require correctly configured HOSTS files, local DNS or a WINS server to be available.

Entering an address in the top box allows access and entering it in the lower box denies access from that machine. MailGate will check for a match to the deny settings first.

Note - See also the SMTP relay tab on page 3-31 to prevent spam mail relay.

 If your network is configured such that your users all access MailGate through a single LAN card in the MailGate machine and your Internet access is through dialup or via a different LAN card, use the Bindings settings to prevent external access to your system.

Bindings Tab

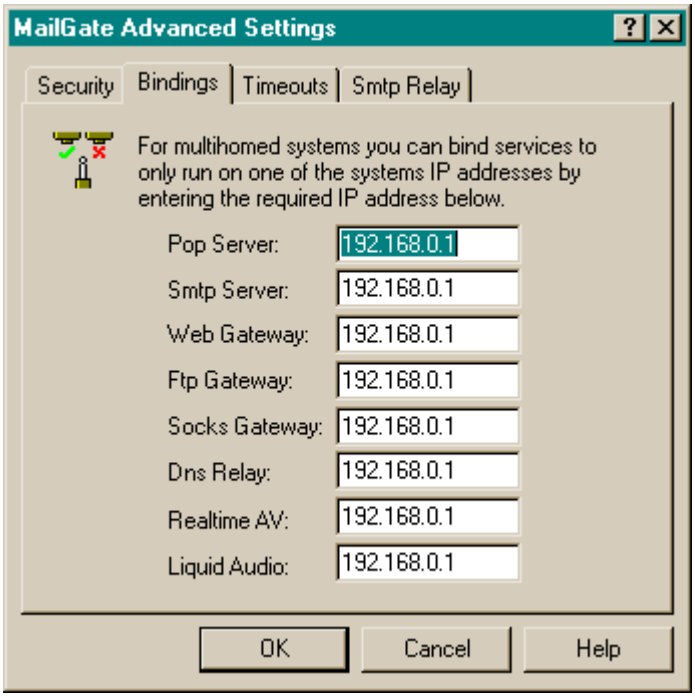

Figure 25 - Bindings Tab

The Bindings Tab is for Multi-homed system (i.e. a system with two or more IP address). It can limit a particular service to be available on only one of the addresses. In a dialup system, the dialup connection will always be on a second IP address.

Although not a Firewall in the strictest sense, MailGate can prevent access to any service by making the service only available to the local LAN, provided all valid users access MailGate through a single IP address.

To do this, put the IP address of the MailGate machine in each entry. You must use numeric IP address. MailGate will ignore any attempt to connect to a service via any other address.

If your network is of a more complex structure, you should use the **Security Tab** on page 3-25 to make the appropriate settings.

Other options within your operating system to further increase the security of your network are outside of the scope of this document. Refer to the operation system documentation.

Timeouts Tab

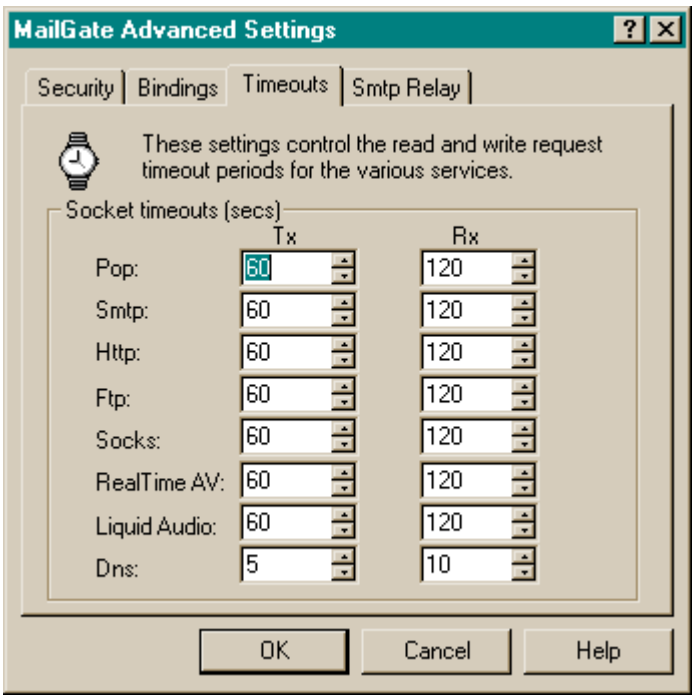

Figure 26 - Timeouts Tab

The Timeout tab sets the timeout for each individual socket operation. Each protocol can have different timeouts. The Timeout tab has the settings to the standard protocols. See the **Custom Proxy Details** on page 3-47 for the settings for each Custom Proxy.

Socket Timeouts and Inactivity Timeouts

MailGate has two types of timeout:

Inactivity Timeouts, which can be set against each service, are managed internally by MailGate. Each time some data is passed using one of the service protocols, the inactivity timer for that service is reset. MailGate will only request a line close once all the inactivity timeouts have expired. See the service setup pages for your current inactivity timeout settings. These are the "Disconnect after XX seconds inactivity" settings for each service.

You can adjust these timeouts to suit your performance requirements. For example, an HTTP request for a web page is much more likely to be followed by another request than an email collection. To save delays at the client workstation, MailGate can keep the line open longer after an HTTP request than when doing an email collection.

Socket Timeouts set the lower level TCP/IP timings.

The TX timeout sets the time to wait for a confirmation after transmitting data.

The RX timeout sets the time to wait for data to arrive after making a request for data.

In general you should only make changes to these settings if you have a poor communications problem. If you need to increase these values, you may also need to increase your inactivity timeouts as your connection may be being cut before the socket timeout period has expired.

SMTP Relay Tab

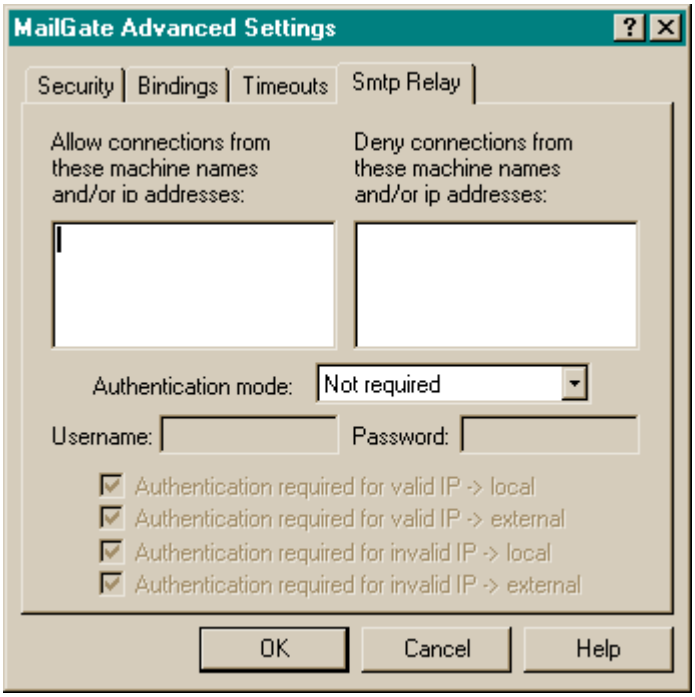

Figure 27 - Smtp Relay Tab

SMTP relaying is the passing of mail messages from one domain to another. This feature of SMTP servers is often exploited by email spammers to hide the original source of their mails.

The standard SMTP protocol does not require a user to provide a username/password before sending mail data. The enhanced protocol, ESMTP, though allows for a number of SMTP authentication methods. MailGate supports the LOGIN method of authentication.

With the SMTP relay tab you can control access to the MailGate SMTP service by using a combination of settings.

Allow/Deny Connections

Use these settings to set the access rights to the SMTP relay service. You may either explicitly allow or deny access by machine IP address. You can use wildcards (9-1) to set an address pattern.

If you wish to use machine names, MailGate must be able to reverse look up an IP address to establish the name associated with it. This will require a correctly configured HOSTS file, local DNS or WINS server to be available.

Entering an address in the left box allows access and entering it in the right box denies access from that machine. MailGate will check for a

match to the deny settings first.

Authentication Mode

Use the dropdown to select what usernames/passwords are acceptable:

- Not Required - Authentication is not required. If used, any username/password will succeed.
- Any MailGate user/pass - The username/password must match a user mailbox
- Specified user/pass - The username/password must match the setting specified here

Authentication Required Checkboxes

These checkboxes provide overrides for the Allow/Deny settings above. The two valid IP settings can be used to turn on the requirement for authentication for machines which could otherwise send mail and the two invalid IP settings can be used to allow mail sending by machines otherwise blocked.

Check the required boxes as follows. In all cases, a local domain is one that is included in the **Domains Tab** (3-9) list otherwise a domain is treated as external :-

Authentication required for valid IP -> local - Check to require SMTP clients with allowed IP addresses to use authentication when sending e-mail to a local domain address.

Authentication required for valid IP -> external - Check to require SMTP clients with allowed IP addresses to use authentication when sending e-mail to an external domain address.

Authentication required for invalid IP -> local - Check to allow SMTP clients with denied IP addresses to send e-mail to a local domain address if the client uses authentication.

Authentication required for invalid IP -> external - Check to allow SMTP clients with denied IP addresses to send e-mail to an external domain address if the client uses authentication.

Note - If full access to the SMTP service is blocked in either the **Security** (3-25) or the **Bindings** (3-28) tabs, these will take precedence over the SMTP relay settings.

NT Users Tab

This tab is only available when MailGate is installed on Windows NT or 2000.

When enabled, MailGate will use the NT user database to obtain the passwords for each mailbox. If using NT domain account validation, make sure that each mailbox you create has a matching Windows NT domain account or that no one will be able to collect the mail from that mailbox.

You must specify the NT Domain to query when checking a mailbox password.

Using Windows NT domain accounts is more secure but less flexible than storing the password within MailGate.

Backup and Restore Configuration

The MailGate configuration information is stored in the Windows registry. You can create a backup file of this information and restore it if needed. You can also use this facility to move MailGate from one machine to another.

Backup Configuration

Backup MailGate configuration

1. Select the Gateway menu and click on Backup Configuration
2. Use the dialog box to select where to place the backup file
3. Enter a filename for the backup and make sure the file ends with .MGB
4. Press the OK button

Restore Configuration

Restore a Configuration

This option will overwrite ALL your current settings with those contained in the backup file.

1. Select the Gateway menu and click on Restore Configuration
2. Use the dialog box to locate the previously saved configuration
3. Press the OK button

Move MailGate to another computer

You can use backup and restore if you need to move MailGate to another computer:

1. Backup the current configuration
2. Install MailGate and any extension modules on the new computer. Do not configure this installation.
3. Copy the configuration file (*.MGB) to the new computer
4. Restore the configuration file on the new computer

Large POP Message Control

Large POP Message Control

MailGate lets you defer collection of messages over a specified size. You can then review the list of large messages and decide whether to collect or delete them.

To specify size and action

1. Select Gateway | Large POP Message Control to open the Large POP message dialog box
2. Set the maximum message size to collect (in kilobytes)
3. Specify whether to notify the administrator and/or the recipient of the large message

The following message is delivered to the recipient or MailGate administrator when a message is deferred:

There is a 0k message for you pending on pop server 'YOUR-SERVER-NAME', account 'YOUR-ACCOUNT-NAME' which is larger than the max download message setting. Your MailGate administrator should be contacted if you require that it is collected and delivered to your account. To help determine the message origins the header and first 25 lines follow:-

---

< Header and text is then displayed from the message >

To Collect or Delete Large Messages

1. Select Gateway | Large POP Message Control to open the Large POP message dialog box
2. Select a message and use the right mouse button to display the menu
3. Select to collect the message or delete it on the next connection

Note - The email address of the MailGate administrator is the *System Reports to* setting in **Email Tab** on page 3-11.

Load Accounts

Load Accounts

If you have a large number of mailboxes to create, you can create a list of them and import that list into MailGate.

Create a text file

First you need to create a file with the name of each mailbox on a separate line, then a comma and the password, like this:

username,password

Save the file with the extension .CSV in any directory

Load Accounts into MailGate

In MailGate, use File | Load Accounts to locate the file. Press OK

MailGate opens a dialog box listing all the accounts and passwords it found in the file. You have the following options:

- Click on any specific account that you want to exclude from the mailbox creation. An x will be placed next to the account name.
- Remove all existing mailboxes before loading the new list
- Don't overwrite any existing accounts

You will need to set any other options for the mailboxes manually.

Load Accounts Detail

If you have a large number of mailboxes to create, you can create a list of them and import that list into MailGate.

Create a text file

First you need to create a file with the name of each mailbox on a separate line, then a comma and the password, like this:

username,password

Save the file with the extension .CSV in any directory

Load Accounts into MailGate

In MailGate, use File | Load Accounts to locate the file. Press OK

MailGate opens a dialog box listing all the accounts and passwords it found in the file. You have the following options:

- Click on any specific account that you want to exclude from the mailbox creation. An x will be placed next to the account name.
- Remove all existing mailboxes before loading the new list
- Don't overwrite any existing accounts

You will need to set any other options for the mailboxes manually.

Logging Information

Purge Logging Files

MailGate can create several log files containing data as specified by the options selected in the Logging Menu.

The length of time log files are retained is defined in the Logging | Purging ... dialog box.

Enable log file purging

Check this to have MailGate purge the log files.

Purge log files older than

Specify the number of days to retain the log files. The default is 30 days.

Logging

The core MailGate system can create two type of log file, General logs and Web Request logs. If you have installed any Extension Modules, then there may be additional logs associated with the module.

The above log files are stored in subdirectory LOG with the filenames:

a) MG<date>.log for general logging
b) RQ<date>.log for web request logging

To view a log, use any text editor. You can also view the general log using the MailGate log viewer, accessed from the Logging | View Logs menu option.

In the Logging menu option, you may select the type of information written to the log files.

General Logging

The Logging menu item allows you to log the following items. If there is a check mark to the left of the item, the logging is turned on.

- Log errors - MailGate system errors
- Log warnings - warnings for potential problems
- Log informationals - general information and activity

Recommend: Enable all three options

Mail Logging

The Logging menu item allows you to log the detail for POP and SMTP traffic. If there is a check mark to the left of the item, the

logging is turned on.

- POP protocol (mail collection and clients)
- SMTP protocol (mail delivery and clients)

Recommend: Enable these when you first install to monitor exactly the processing of your mail and otherwise if there are problems with your mail handling.

Web Logging

The Logging menu item allows you to log each URL requested. If there is a check mark to the left of the item, the logging is turned on. In addition, if you use Authenticate proxy users (see the **Web Tab** on page 3-16) MailGate will log the requesting user name.

- Log Web requests

Recommend: None, depends on site requirements.

Maintaining Schedules

Schedule Detail Screen

The scheduler can be used to schedule:

- when mail is exchanged with your ISP. This allows mail to be sent and collected from your ISP during the day on a regular schedule without user intervention.
- when the different proxy gateways are enabled
- to fine tune the use of your Internet connection

To create a new schedule click on the  icon on the tool bar or select Edit | New | Schedule. To edit an existing schedule, highlight the schedule and select Edit | Edit to open the schedule dialog. Then:

1. Check the days of the week the schedule should be active
2. Set the time when the schedule should start and end
3. Check the box to enable the schedule
4. Select the type of schedule from the drop down list

Types of schedules

See **Using the Scheduler** on page 2-25 for more detail on the types of schedule available.

Notes

1. To schedule for the whole day use the start time of 0:0 and the end time of 23:59
2. If MailGate is not running when an event is scheduled (such as mail transfer), it will not happen until the next scheduled time.

Maintaining Mailboxes

Mailbox Detail Screen

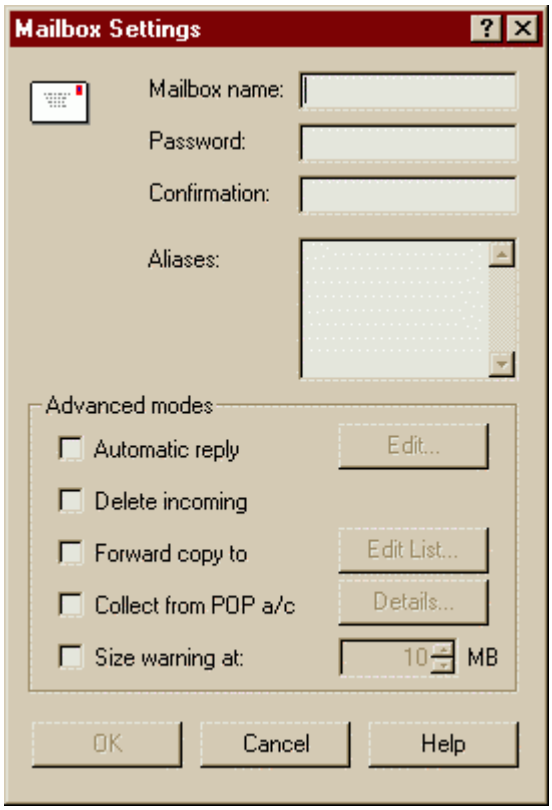

Figure 28 - Mailbox Settings

Each user should be given a mailbox account within MailGate. It is this account from which the mail will be collected by the users mail client.

To create a new mailbox, click on the  icon on the toolbar or select Edit | New | Mailbox. To edit an existing mailbox, highlight it and select Edit | Edit to display the mailbox detail screen.

You must give the mailbox a name and password. The mailbox name can be a full email address or just the user part (part before the @).

Note - if you are using the NT users option in the Gateway | Advanced | NT Users Tab the password will be taken from the NT user database

Mailbox Options

There are a number of optional settings that can be made for each mailbox. Follow the links below for more information on these.

- Aliases - more than one username
- Auto Reply to incoming mail
- Delete Incoming mail to the mailbox
- Forward mail to another account
- Collect mail from specific POP account
- Size warning for this mailbox

 **Tip -** If you have a large number of mailboxes to create, you can use a text file to enter the accounts. See **Load Accounts** on page 3-36 for more information.

Aliases for a Mailbox

An alias allows you to add other names for sorting into a mailbox. This can be useful for people who have nicknames or change their names.

Aliases can be used to put several accounts into one local mailbox. For example, if you setup a SALES mailbox, you could put INFO in as the alias. Then any mail sent to either sales or info would go to the same local mailbox.

Aliases can also be used to put a message into multiple mailboxes. For example, if you want to have mail sent to SUPPORT@yourcompany.com copied to all the technical support people, you can put SUPPORT in as an aliases in the setup for each local mailbox. See **Planning Mailboxes - Advanced Example** on page 2-11 for more information.

Auto Reply to Mail

Auto Reply sends a mail message back to the sender for each message received in the local mailbox. For example this could be used to send a message that you are on vacation

Create the Auto Reply

1. Select the mailbox to send the Auto Reply in the MailGate main window
2. Select the Edit menu and click on Edit
3. Check the Automatic Reply box at the bottom of the Mailbox Settings window
4. Press the Edit button next to Automatic Reply and enter the text to be sent in the reply

Notes

1. The reply text is kept in the MAILBOX sub-directory of the MailGate installation directory in a file called <MAILBOXNAME>.REP
2. Windows 95 has a 64K limit when writing text within the MailGate edit box, but you can edit the file with another editor. Windows NT has no limit to the length of text.

Delete Incoming Mail

This option automatically deletes any mail received into this mailbox.

If you have Forward Copy to or Automatic Reply turned on then these actions will happen before the message is deleted.

Forward Copy To

This option forwards a copy of a mail message to another email address, which can be a local mailbox or an external address.

You can use this to forward mail to another person while you are out of the office or when two people have responsibility for answering a mailbox.

If you are forwarding to another local mailbox, then you only need to specify the mailbox name or alias. To forward to more than one address, enter each on a new line.

Collect from Specific POP Account

This option to collect from a specific POP account directly into this mailbox.

You will need to specify the POP server name, account name and password for the account to collect from. You ISP will supply these details.

You should select the Login Method to use. Most ISP's require the standard User + Pass method. If in doubt you should try this setting first.

NOTE - This method of collection bypasses the normal routing logic specified in **How MailGate Sorts into Mailboxes** on page 2-12 and places all collected mail directly into this mailbox. You should NOT collect mail from a given POP account by this route and by setting the account details in the Gateway | Setup | POP account tab.

Leave Mail on Server for x Days - This option allows mail that you've collected to be retained on your ISP mail server for the specified number of days. This can be used as a backup or

to allow you to collect the mail from different locations, such as at home and the office. This option requires your ISP supports the UIDL command for mail tracking. If it is not working, please consult your ISP.

Size Warning for a Mailbox

A size warning can be set for each MailGate mailbox. This may be useful if you set your users mail clients to leave a copy of mail on the server.

The mailbox sizes are checked daily. When the mailbox reaches this size, the following warning message is sent to the MailGate administrator:

Mailbox '<mailbox name>' exceeds limit of <size limit> mb, currently <current size> bytes

Maintaining the Outgoing Queue

Outgoing Message Details

The Outgoing Queue shows all mail that is waiting to be sent the next time MailGate connects. By double clicking on a queued message or highlighting a message and selecting Edit | Info, MailGate will display the Outgoing Message Details dialog.

With this dialog you can get some additional information that is very useful for tracking errors.

File Details

Both the message file name and size are displayed. There are three files for each message in the queue. The first part of the file name is displayed here. Each outgoing message will have a file with the extension (file type) of .msg, which is the mail message data, a .xdl which contains the sender and recipient addresses and a .ctl which contains the data displayed in this screen.

All outgoing mail is stored in the QUEUE subdirectory under the MailGate system directory.

You may also find files with the extensions of .ldl and .pdl. These are messages that are waiting delivery to local mailboxes or are pending processing.

Address Data

Both the sender and recipient addresses for the message are displayed.

Message Status

Information about the time the message was first placed in the queue and its current status are displayed. If the last error shows an error code, see Winsock Error Codes for a list of the common code meanings.

Delete Message from the Queue

In this dialog you can delete the message by selecting the Delete button.

Requeue if Errors

If there is a problem sending a mail message, MailGate will requeue the message and try on the next connection.

Maintaining URL Filters

URL Filter Details

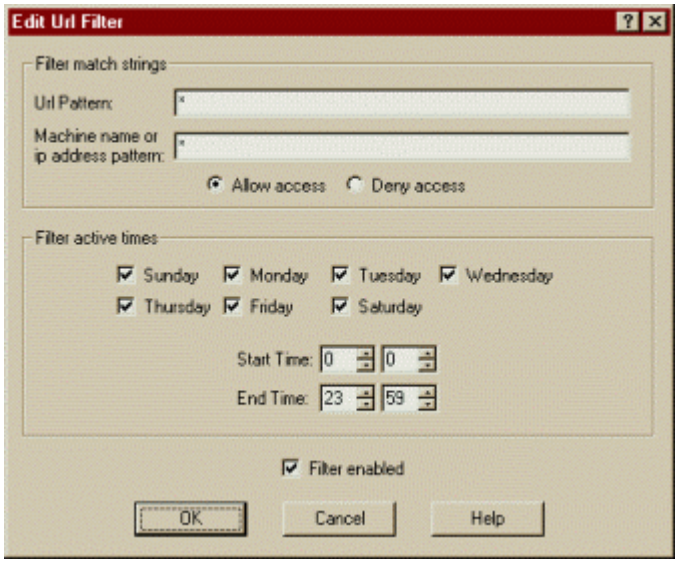

Figure 29 - Edit URL Filter

By creating URL filters you can control which web sites and pages your users can access. You can create as may URL filter checks as you like to build a profile to suit your requirements.

To create a new filter entry, click on the  icon on the toolbar or select Edit | New | URL Filter. To edit an existing entry, highlight it and select Edit | Edit to display the URL filter detail screen.

You must specify a URL pattern and a machine address pattern to which this filter is applicable using wildcards (see 9-1). You then select to either Allow or Deny access for requests that match the pattern settings. If you choose to use machine names. MailGate must be able to reverse lookup the users IP address and find the machine name using a correctly configured HOSTS file, DNS or WINS server.

Optionally you can define both when the filter entry is active and enable or disable this entry in your filter list.

Order of Filter entries

The order of your filter entries is important. You can drag and drop the filters in the main MailGate window or use Move Up/Down on the right mouse button menu to change the order.

When a user makes a request, MailGate checks each filter entry in turn and uses the first match it finds for both the machine name and the URL, acting on the allow or deny

setting. If the end of the list is reached and no match is found, the request will be allowed.

Example:

You want to limit access only to a few specific web sites on all machines, you would list the ones they could access first and the last URL filter would deny access to all other web sites:

- Allow access to www.macromedia.com* by all machines
- Allow access to *.microsoft.com* by all machines
- Allow access to *.mailgate.com* by all machines
- Deny access to * by all machines

For more information, see **Using URL filters** on page 2-18.

Maintaining Custom Proxies

Custom Proxy Details

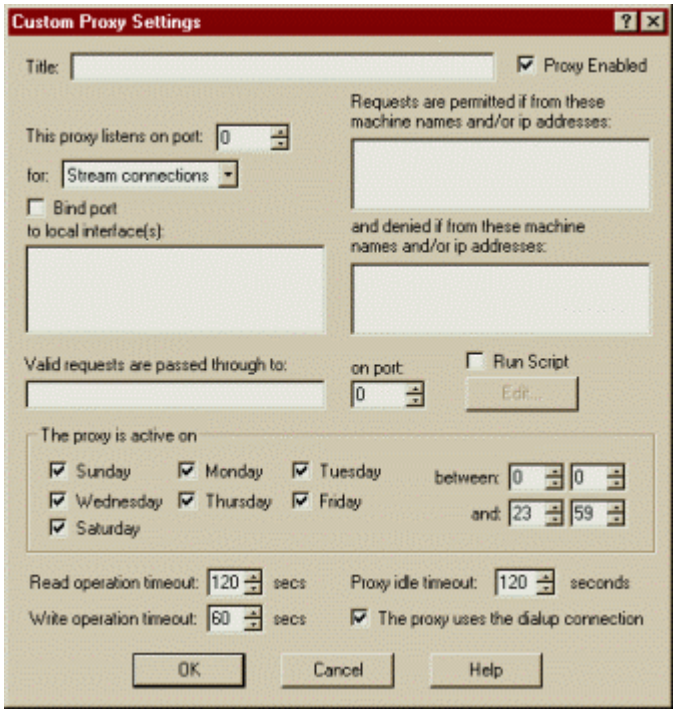

Figure 30 - Custom Proxy Settings

The Custom Proxy facility allows create your own proxy gateways so MailGate can proxy non-standard protocols. MailGate is installed with two examples that you can use to proxy Telnet and NNTP traffic through MailGate. For more details see:

Using Custom Proxies on page 2-22
NNTP Custom Proxy on page 2-23
Telnet Custom Proxy on page 2-23

To create a new Custom Proxy, click on the icon on the toolbar or select Edit | New | Custom Proxy. To edit an existing entry, highlight it and select Edit | Edit to display the Custom Proxy detail screen.

To configure your Custom Proxy, follow these steps:

Required Entries

Title - Give your proxy a title.

Proxy Enabled - Check this box to enable the proxy.

This proxy listens on port - Enter the port number your users will use to connect to the proxy.

For - Select the type of data traffic. Use streams for TCP traffic (like HTTP) and Datagram for IP traffic (like DNS). (Not required if you use a script).

Valid Requests are passed through to - Specify the remote host machine this proxy should connect to. (Not required if you use a script).

On Port - Specify the port number to use when connecting to the remote host. (Not required if you use a script).

Run Script - Check this box if you wish to use a MailGate script. Use the edit button to edit your script. See **Introduction to Scripting** on page 9-3 for more detail on the MailGate scripting language.

Optional Settings

Security:

Use the **Requests are permitted**... **and denied**... boxes to control which machines can access this proxy. This is similar to the settings made in the Security Tab (see 3-25) for the standard proxy gateways.

Use the **Bind Port** setting to bind this proxy to your local lan IP address. This setting can be used in two ways.

1. With the Bind Port box checked, the Local Interfaces entry will change to only allow a single IP address. This is similar to the settings made in the Bindings Tab (see 3-28) for standard proxy gateways. This method is binding in the true sense.
2. With the Bind Port box NOT checked you can enter you can enter more than one IP address (on per line) through which this proxy may be accessed in the Local Interfaces field. This is not binding in the true sense, but access is managed internally by MailGate.

NOTE - You can have both methods configured with addresses. As the true binding IP address is not normally displayed, you should check this setting if you have problems connecting to your Custom Proxy.

Availability:

Use the Proxy is active on settings to define when this proxy may be accessed. This is similar to the settings that may be made using the scheduler (see 2-25).

Timeouts:

Set the required timeouts for this proxy.

Check **The Proxy uses the Dialup Connection** if you want MailGate to connect to your ISP to satisfy requests passed to this proxy.

For your client applications to use a MailGate Custom Proxy you will need to set them to connect to the MailGate machine when making Internet requests. Refer to the supplier of your application to understand how this may be achieved.

4 Registration & Support

Registration

When you first install MailGate you can use the software with up to 10 mailboxes for a full 30 days. At any time during that period you can purchase a license key and after entering this into the Registration dialog your copy of MailGate will become a fully working copy.

To find out how to purchase a key, contact your local reseller or visit our web site - www.mailgate.com.

1. When you receive your 20 character key, use Help | Registration to register your software:
2. Enter your key in the Activation Key field. Note that capital letters must be used.
3. Enter your company or organisation name in the Register to field.
4. Click on OK and you should get a Licence Accepted message if you entered the details above correctly. Click OK to acknowledge this message.
5. You will now be asked if you wish to register your details using an on line email. We advise that you do this as it enables us to keep you updated with product news and events. Our policy is to only use your information for this purpose and we do not disclose your details to an other party. To prevent unauthorised access to your information, the email that is returned by this process to us is encrypted.

Your copy of MailGate will now be registered. Please keep a copy of your key safe!

Email For Support

Free Support for Registered Users

All registered users are eligible for free technical support via Email. All support Emails will be responded to but without guarantee as to the response time. Email your support questions to support@mailgate.com including your serial number and the registered user name.

Chargeable Support Options

Annual Support Contract: A chargeable service that includes telephone support. Please contact your dealer for further information.

Support for Evaluation Versions

Support for evaluation users is freely available on an ad hoc basis by e-mail; response times cannot be guaranteed: eval@mailgate.com

Emailing for Support

MailGate can be used to generate an email message for support:

Select Help | Email for Support to access the Send Support Email dialog. Create your email as follows:

Report Type - Select the type of email you wish to send.

Select Logs to Include - Use you mouse to select the log files that show your problem. Note the log file name is MG<yymmdd>.LOG.

Select other options:

Copy to System Reports Address if you would like to get a copy of your message.

Include Connection History to send a copy of your current connection history data.

Include Configuration to send a copy of your settings so we can replicate your setup.

Reply Address - Enter the email address our support desk should reply to.

Message - Please give as much detail as possible. We would like to know what has happened, what you expect to happen and when the problem occurred if possible.

Click on the send button to transmit your email.

Web Lists on the Help Menu

Our web site www.mailgate.com is the one of the best places to look if you're having problems.

The latest information regarding the program, updates and technical information can be found there. Through Help | MailGate on the Web you will find links both to our web site and other related sites.

This list can be modified to include any web site you might want to visit while using MailGate.

The file URLS.DAT in the directory where MailGate is installed, contains the content of the menu list.

The format for the file is:

<siteaddress><space><description for menu>

You can also insert a line in the menu by placing the word "separator" on a line by itself, without the quote.

For example:

http://www.mailgate.com MailGate home page
separator
http://www.socks.nec.com NEC SOCKS TCP/IP stack home page

5 User Reference

MailGate Customization

Web Proxy Message Customization

When the web proxy returns an error to the user, it uses an internal HTML file to format the error. You can create your own HTML file and optional GIF file to format the error instead for your site requirements, such as internal support telephone line or email address.

MailGate looks for an ERRORS.HTML and LOGO.GIF in the MailGate installation directory. If these files are not found, it uses its own internal file.

Format of ERRORS.HTML

MailGate installs an ERRORS.SAM file as a sample for creating the ERRORS.HTML file.

Errors.html is a standard html page with a couple of comments in it to mark where MailGate adds error specific info. The two tags are:-

<!-- head --> - Immediately after this text string MailGate will put a short message to be used as the title of the web response (i.e. what appears on the browsers window bar). You could put this in the main body of the html as well/instead if you wish.

<!-- error --> - Immediately after this text string MailGate will put the text of the error message.

Referencing an Image

MailGate also supports the insertion of an image into the

page. The image has to be referenced by the GUID string:

/AF00E4B6-C3F0-11d1-86AC-0080C8330493/logo.gif

This is done so the separate request the browser will make for the image can be identified and not proxied like other requests.

The response to this request by MailGate is to send back the image stored in LOGO.GIF file.

6 Solving Problems

Using the Log Files

MailGate logs all activity in a daily log file stored in the LOG folder under the MailGate system directory. The file name used follows the format MG<yymmdd>.LOG.

Using the **Logging** (see 3-37) menu item you can choose what details are written to this log file.

You can view the log file using any text editor or by using the MailGate Log Viewer utility which can be accessed by selecting Logging | View Logs.

The most common use for the log file is to help adjust your POP collection settings. To do this you should ensure you are logging POP Collection Details. When you look at the log file you will see each line of your incoming emails, including the mail header data, and information on how MailGate is routing the mail. Refer to **How MailGate Sorts into Mailboxes** on page 2-12 and adjust your POP collection settings until the routing you require is achieved.

For more complex problems, use the **Email for Support** on page 4-2 facility and send us a copy of your log file with your question.

Winsock Error Codes

MailGate uses TCP/IP to communicate both with your users and the Internet. This communication is processed by passing requests to the IP software loaded on your machine. Sometimes there may be a problem with communications and the IP software will pass an error code back to MailGate. The most common error codes are listed here to help you understand what may be wrong. A full list may be found on our web site www.mailgate.com in the support area.

Code	Meaning	Likely Cause
10048	The address is already in use	There is a lock or failure to connect. Try again later.
10054	The connection was dropped by the other end	The remote system terminated the connection for some reason. Can also be caused by net overload causing a timeout or a failure in your Internet connection.
10055	Winsock is out of buffer space	Generally caused by a IP address loop. Carefully check your IP configuration. In particular, check you have not set 'Use ISP proxy Server' (Web Tab) or DNS Servers (DNS Tab) to point at MailGate.
10060	Time Out	IP has timed out connecting to or communicating with the host. Check the host IP address is valid and that the service you are trying to use is available. Try again later.
10065	Host Unreachable	The connection to the host machine has failed. Check the host IP address is valid and that the service you are trying to use is available. Try again later.
11001	Name lookup - Authoritative answer: Host not found	A DNS lookup problem. The connection to the host machine has failed. Check the host IP address is valid and that the service you are trying to use is available.
11004	Name lookup - Valid name, no data record.	The DNS server queried does not have data for the request made. Check that the service you are trying to use is available.

7 Network Preparation

Network Requirements

Network Requirements

This section covers the system setup for machines on the network that will connect to the MailGate Server and the machine that will run the MailGate Server program.

- **MailGate Requirements**
  1. Connection to an Internet Service Provider. This can be a direct line or a dial up connection.
  2. TCP/IP installed on all machines in the network that use **MailGate**
  3. Dial-Up Networking installed on the machine running **MailGate**. If you have a leased line connection, you do not need Dial-Up Networking.

- **TCP/IP Networking Requirements**
  1. A unique TCP/IP address for each computer
  2. A unique machine name for each computer (optional)
  3. Network domain name (optional)
  4. Either Domain Name Service (DNS) or LMHOSTS /HOSTS files for name resolution on the network (optional)


The simplest setup for TCP/IP is to use static addresses on your network. With this you give each machine a unique IP number (address) and when you refer to that machine in you software settings you specify only the IP number. **If you use this method you can ignore all references to machine names**.

If you are unfamiliar with TCP/IP, please see **Preparing for TCP/IP Installation** on page 7-2 for more information.

Note - Windows 3.1x and Windows for Workgroup TCP/IP configuration is not covered in this document as there are so many TCP/IP programs with their own requirements.

Get more information

For more information, read the sections for the appropriate operating system.

How can I tell if TCP/IP is installed?	Window 95/98 see 7-4	Windows NT see 7-9
How do I setup the machine address?	Window 95/98 see 7-5	Windows NT see 7-9
How do I enable DNS?	Window 95/98 see 7-5	Windows NT see 7-10
How do I setup the LMHOSTS and HOSTS files?	Window 95/98 see 7-6	Windows NT see 7-10
How do I setup Dial-Up Networking?	Window 95/98 see 7-7	Windows NT see 7-11

Preparing for TCP/IP Installation

Before setting up TCP/IP you will need to obtain some information from your network administrator. If you do not have a network administrator, you will need to make the decisions now for your network.

1. What is the TCP/IP network address for your network and number for each machine?
2. What is the DOMAIN name for your network? (optional)
3. What are the names for each machine in the network? (optional)

TCP/IP Network Address

TCP/IP Networking uses a number broken into four parts and separated by a period.

Part of the IP number is for the network and common to all machines and part is used to address each individual machine.

For example

192.168.0.1 is a TCP/IP network number

192.168.0 is the network part

1 is the individual machine

Other machines in the network would be numbered

192.168.1.2

192.168.1.3 up to 254

What Address Should be Used?

Internet addresses (numbers) are assigned to specific companies or groups by various organizations around the world.

However, many companies connect to the Internet and obtain their Internet address dynamically each time they connect to their Internet Service Provider. This assigned number is only used during the connection and is not the same as the numbers for your local network.

Within your local network, you can use the following network numbers if you do not have an assigned number:

192.168.0.x

10.0.0.x

The x part of the number is used for each individual machine with the range 1-254

Note - When using these addresses, the Subnet Mask is always 255.255.255.0

Domain Name

A domain name groups computers together. If you use static addressing and refer to each machine by IP number this is not required.

For simple networks this can be the same as the Workgroup name and all machines in the network have the same domain name.

For complex networks running NT Server with specific domain setup, consult your network administrator.

Machine Names

In addition to having a unique TCP/IP address, each machine can have it's own name. If you choose to use machine names, you will need to setup a method for your machines to convert these names to IP numbers. This can be done using HOSTS files or a DNS or WINS server. This is the name you will see in the Network Neighborhood display.

Machine names are generally one word with only letters and numbers (alphanumeric) and should be limited to a maximum of 12 characters on Windows machines. Spaces and underscores and hyphens should be avoided in machine names.

Windows 95/98 Network Preparation

Windows 95/98 Network Preparation

The following topics cover network preparation issues for Windows 95.

You will need the following information:

1. The TCP/IP addresses and machine names (optional) for all machines in the network
2. Your domain name (optional)

If you are unfamiliar with TCP/IP, please see **Preparing for TCP/IP Installation** on page 7-2 for more information.

For more information see:

- How can I tell if TCP/IP is installed? (below)
- How do I setup the machine address? (on page 7-5)
- How do I enable DNS? (on page 7-5)
- How do I setup the LMHOSTS and HOSTS files? (on page 7-6)
- How do I setup Dial-Up Networking? (on page 7-7)

TCP/IP Install for Windows 95/98

To check to see if TCP/IP is installed on Windows 95 or 98, do the following

1. Click on the Start Menu and select Settings and from the Settings menu select **Control Panel**.
2. From the Control Panel window, select **Networks**.
3. On the **Configuration tab** TCP/IP should be listed.

- If TCP/IP is **not** listed

1. You will need to obtain the Win 95 Installation CD-ROM.
2. On the Configuration tab, press the ADD button, select protocol and then select Microsoft in the left hand dialog and TCP/IP in the right hand dialog and click OK.
3. Follow the instructions from the setup program.

For detailed information on TCP/IP installation, please consult the Microsoft help files and documentation.

- If TCP/IP is listed

Check the following TCP/IP setup requirements:

- How do I setup the machine address? (on page 7-5)
- How do I enable DNS? (on page 7-5)
- How do I setup the LMHOSTS and HOSTS files? ? (on page 7-6)

Setup machine address for Windows 95/98

To setup the network domain name for Windows 95:

1. Click on the Start Menu and select Settings and from the Settings menu select **Control Panel**.
2. From the Control Panel window, select **Networks**.
3. On the Network dialog, select **TCP/IP -> your network adapter**.
4. Press the **Properties** button and select the **IP Address tab**.
5. Check **Specify an IP Address**
6. Enter a unique IP address

Notes

i. Always check with your network administrator regarding your current TCP/IP setup. Some networks may have a server setup to assign IP address to machines on the network.

ii. The machine where **MailGate** is installed should be setup with a specific IP address and not one obtained by a DHCP server. This is to ensure that it always has the same IP address.

Enable DNS for Win95/98

To setup the network domain name for Windows 95 (Optional):

1. Click on the Start Menu and select Settings and from the Settings menu select **Control Panel**.
2. From the Control Panel window, select **Networks**.
3. On the Network dialog, select **TCP/IP -> your network adapter**.
4. Press the **Properties** button and select the **DNS Configuration tab**.
5. Check the **Enable DNS** button if not already checked.

Notes

i. If you have Windows NT Server and DNS domains already setup, please contact your system administrator for the name you should enter here.

ii. If you enter a domain name here and do not have a DNS Server, Win95 will become confused and often ask to dial-out for local machines. It is recommended that you leave the domain name blank for peer to peer networks.

Setup LMHOSTS and HOSTS files for Windows 95/98

The LMHOSTS and HOSTS files are used to map specific IP addresses to a machine name. In a simple network setup, these contain the same information, but are used by different programs.

If you are using static addressing using just IP numbers, then you can ignore these settings.

LMHOSTS is used by the NetBEUI protocol to map machine names and IP addresses. HOSTS is used by the TCP/IP protocol to map machine names and IP addresses. Note the HOSTS files may have multiple names for the same IP address.

These files are located in the directory where you have installed Windows 95. There are sample files in this directory called LMHOSTS.SAM and HOSTS.SAM for you to refer to.

Setup LMHOSTS and HOSTS

1. Create the LMHOST and HOSTS files on one machine as described below
2. Make sure the HOSTS file has the extra line for localhost and **MailGate** machine as described below
3. Copy the LMHOST and HOSTS file to all other machines in the network

Windows NT - place the file in the \%systemroot%\system32\drivers\etc (%systemroot% is a variable used to describe wherever you have installed NT – this need not be drive C:).

Windows 95/98 and Windows 3.1x - place the file in the directory where Windows 95/98 or 3.1x is installed.

Text for LMHOSTS and HOSTS

The text in both these files is in the form:

ip_address <tab> machinename

ip_address <tab> machinename

You should enter each IP address and machine name in your network, each on a single line.

Additional Requirement for HOSTS file

The HOSTS file should always contain the following entry:

127.0.0.1 localhost

This address is used by many TCP/IP programs.

Requirement for MailGate

For the machine that is running **MailGate**, the HOSTS file can have the name "mailgate" as well as the regular machine name for the IP address. For example:

```
192.168.1.30    sysmachine      mailgate
```

This allows users to enter the word "mailgate" instead of having to know the specific IP address of the MailGate machine.

Note

If you have a Domain Name Server (DNS) setup for your network, please consult your system administrator for details of setting up DNS for your network and these files.

Setup Dial Up Networking for Windows 95/98

Dial-Up Networking must be installed on the machine that will run **MailGate**.

There are two steps with Dial-Up Networking

1. Install the software
2. Configure for connecting to your Internet Service Provider.

Install Software

Check to see if Dial-Up Networking is installed. You can do this by double-clicking on My Computer. If it is installed, you will see a folder called Dial-Up Networking.

If Dial-Up Networking is not installed, do the following:

1. Start Menu, click on Settings and then Control Panel
2. Choose the Add/Remove Programs option.
3. Click on the "Windows Setup" tab
4. Select the "Communications" option and click "Details".
5. Put a check in the box next to the Dial-Up Networking Option.

Configure DUN for your ISP

After Dial-Up Networking is installed, you will need to configure an entry for connecting to your ISP.

1. Select The Internet icon on your desktop
2. Follow the instructions of the Wizard

Tips for Dial-Up Networking Configuration

Check with your ISP for complete information for your connection.

1. You may need to specify the DNS servers for your ISP in the TCP/IP configuration.
2. You will need to select whether you are assigned an address when you logon (most services) or have a specific IP address.
3. You may need a logon script for your ISP. Many service providers already have these scripts written and available.

Windows NT Network Preparation

Windows NT Network Preparation

You will need the following information:

1. The TCP/IP addresses and machine names (optional) for all machines in the network
2. Your domain name (optional)

If you are unfamiliar with TCP/IP, please see **Preparing for TCP/IP Installation** on page 7-2 for more information.

For more information see:

- How can I tell if TCP/IP is installed? (on page 7-9)
- How do I setup the machine address? (on page 7-9)
- How do I enable DNS? (on page 7-10)
- How do I setup the LMHOSTS and HOSTS files? (on page 7-10)
- How do I setup Dial-Up Networking? (on page 7-11)

Note

This section covers only the basic installation and setup for a small network. This section does not cover Windows NT Server setup with Primary Domain Controllers, multiple networks or domains, etc.

For complex network setups, please consult your system network administrator.

TCP/IP Install for Windows NT 4

To check to see if TCP/IP is installed on Windows NT 4.0, do the following:

1. Click on the Start Menu and select Settings and from the Settings menu select **Control Panel**.
2. From the **Control Panel** window, select **Networks**.
3. On the Network dialog, select the **Protocols** tab. TCP/IP should be listed here.

- If TCP/IP is **not** listed

You will need to obtain the NT Installation CD-ROM

1. On the Protocol tab, press the ADD button and select TCP/IP.
2. Follow the instructions from the NT setup program.
3. For detailed information on TCP/IP installation, please consult the Microsoft help files and documentation.

- If TCP/IP is listed

Check the following TCP/IP setup requirements:

 How do I setup the machine address? (below)

 How do I enable DNS? (on page 7-10)

 How do I setup the LMHOSTS and HOSTS files? (on page 7-10)

Setup machine address for Windows NT

To setup the machine address name for Windows NT:

1. Click on the Start Menu and select Settings and from the Settings menu select **Control Panel**.
2. From the Control Panel window, select **Networks**.
3. On the Network dialog, select the **Protocols tab**.
4. **Highlight TCP/IP** and press the **Properties** button.
5. Select the **IP Address tab** on the Properties dialog and check specify an IP address and enter the number.

Notes

i. Always check with your network administrator regarding your current TCP/IP setup. Some networks may have a server setup to assign IP address to machines on the network.

ii. The machine where **MailGate** is installed should be setup with a specific IP address and not one obtained by a DHCP server. This is to ensure that it always has the same IP address.

Enable DNS for Windows NT

To setup the machine name for Windows NT (Optional):

1. Click on the Start Menu and select the Control Panel.
2. From the Control Panel window, select **Networks**.
3. On the Network dialog, select the **Protocols** tab.
4. Highlight **TCP/IP** and press the **Properties** button.
5. Select the **WINS Address** tab on the Properties dialog.
6. Check the "Enable DNS for Windows Resolution".

Note

If you have Windows NT Server and DNS domains already setup, please contact your system administrator.

Setup LMHOSTS and HOSTS files for Windows NT

The LMHOSTS and HOSTS files are used to map specific IP addresses to a machine name. In a simple network setup, these contain the same information, but are used by different programs.

If you use static addressing using IP numbers, then you can ignore these settings.

LMHOSTS is used by the NetBEUI protocol to map machine names and IP addresses. HOSTS is used by the TCP/IP protocol to map machine names and IP addresses. Note the HOSTS files may have multiple names for the same IP address.

These files are located in \%systemroot%\system32\drivers\etc (%systemroot% is a variable used to describe wherever you have installed NT). There are sample files in this directory called LMHOSTS.SAM and HOSTS.SAM for you to refer to.

Setup LMHOSTS and HOSTS

1. Create the LMHOST and HOSTS files on one machine as described below
2. Make sure the HOSTS file has the extra line for localhost and **MailGate** machine as described below
3. Copy the LMHOST and HOSTS file to all other machines in the network

Windows NT - place the file in the \%systemroot%\system32\drivers\etc (%systemroot% is a variable used to describe wherever you have installed NT).

Windows 95 and Windows 3.1x - place the file in the directory where Windows 95/3.x is installed.

Text for LMHOSTS and HOSTS

The text in both these files is in the form:

ip_address <tab> machinename
ip_address <tab> machinename

You should enter each IP address and machine name in your network, each on a single line.

Additional Requirement for HOSTS file

The HOSTS file should always contain the following entry:

127.0.0.1 localhost

This address is used by many TCP/IP programs.

Requirement for MailGate

On the machine that is running **MailGate**, the HOSTS file can have the name "mailgate" as well as the regular machine name for the IP address. For example:

192.168.1.30 sysmachine mailgate

This allows users to enter the word "mailgate" instead of having to know the specific IP address of the mailgate machine.

 The setup instructions in this manual are based on using the machine name "mailgate" setup in the HOSTS file. If you use another name, you will need to remember to use that name instead when configuring **MailGate** and your client programs.

Note

If you have a Domain Name Server (DNS) setup for your network, please consult your system administrator for details of setting up DNS for your network and these files.

Setup Dial Up Networking for Windows NT

Dial-Up Networking must be installed on the machine that will run **MailGate**.

There are two steps with Dial-Up Networking:

1. Install the software
2. Configure for connecting to your Internet Service Provider.

Install Software

You can check to see if Dial-Up Networking is installed by the following:

1. Click on the Start Menu and select Settings and from the Settings menu select Control Panel
2. From the Control Panel window, select Networks

3. On the Network dialog, select the Services tab and look for Remote Access Service. If it is listed, go to Configure your ISP below.

If Remote Access Service is **not** listed:

1. You will need to obtain the NT Installation CD-ROM
2. On the Service tab, press the ADD button and select Remote Access Service.
3. Follow the instructions from the NT setup program.
4. If connecting by a modem to your ISP, you will also need to install a modem if you have not done so previously.

Configure DUN for your ISP

After Remote Access Service (DUN) is installed, you will need to configure an entry for connecting to your ISP.

1. Select the Dial-Up Networking icon on your system (rasphone.exe)
2. Press the New button and follow the instructions of the Wizard

Tips for Dial Up Networking Configuration

Check with your ISP for complete information for your connection.

1. You may need to specify the DNS servers for your ISP in the TCP/IP configuration.
2. You will need to select whether you are assigned an address when you logon (most services) or have a specific IP address.
3. You may need a logon script for your ISP. Many service providers already have these scripts written and available.

Checklist for Simple Network Setup

Checklist for Simple Network Setup

The following checklist is for a simple peer-to-peer network setup. The options when using Windows NT Server and Domain Controllers is beyond the scope of this document.

	All machines in network (including MailGate machine)
	TCP/IP installed
	Have a unique IP address
	Have a unique machine name (optional)
	Have enabled DNS (optional)
	LMHOSTS and HOSTS files setup (optional)
	One machine in the HOSTS file is called mailgate (optional)
	Machine where MailGate is installed
	The TCP/IP address is set explicitly and not by a DHCP server
	Dial-Up Networking is installed
	The HOSTS file has this machine named as mailgate (optional)

Figure 31 - Checklist for Simple Network Setup

Tip

You can quickly check all machines to see if TCP/IP is installed by opening a DOS box and typing PING.

You can test connections to other machines by typing PING IPAddress or PING Machinename.

See the Microsoft help file for more information about PING or type PING /? at the DOS prompt.

8 Configuring Clients for MailGate

Overview of Client Configuration

A client is the program that accesses the MailGate Server from your computer, such as Internet Explorer or Netscape for web browsing; MS Outlook, Eudora or MS Mail for collecting your mail.

For your workstations to be able to access the Internet successfully they need to use the gateways that MailGate has authorised for traffic in and out of the network.

This section contains some simple guidelines on setting up some of the more common client programs to use MailGate. For more detailed and up-to date information, please check our web site www.mailgate.com. The web site is updated more frequently than the help file.

For more information, please choose a client type below:

- Web Browsers on page 8-2
- Mail clients on page 8-4
- FTP clients on page 8-7
- News clients on page 8-9

Web Browser Client Configuration

Web Browser Client Configuration

You use a Web Browser to access and view website pages.

You will need to configure your browser to use a Proxy Server and give it the proxy server address (this will be the MailGate machine address). Your browser will then pass your web requests to the proxy server.

In this section you will find notes on setting up Internet Explorer Versions 3,4 and 5 and Netscape Version 3 and 4 to use the MailGate Server.

» Information on Internet Explorer below
» Information on Netscape on page 8-3

Internet Explorer Proxy Configuration

There are several methods with Internet Explorer 32 bit versions 3,4 and 5 on Windows platform for getting to the browser configuration:

i. In the Control Panel select Internet applet.
ii. In Internet Explorer select the View menu and click on Options.

Whichever method is used, select the Connection tab. This allows you to configure the proxy settings.

Internet Explorer Version 5

If installed on the machine where MailGate is running:

In the Tools | Internet Options | Connections dialog:

1. Select the 'Never Dial a Connection' radio button
2. Select EACH dialup account and open the settings page. Ensure the setting has Use Proxy Server checked and enter the IP address or name and port of the MailGate server.
3. Press the LAN settings button and enter the IP address or name and port of the MailGate server here also.

On all other client machines, you should only have to enter the LAN settings and point to the MailGate server (step 3).

Internet Explorer Versions 3 and 4

In the Connection Tab Configuration:

1. In the HTTP dialog enter the IP address or name of the MailGate server (generally mailgate).
2. Check the "Use the same proxy server for all protocols" box
3. Click OK.

Note

You will usually only need to set exceptions if your network is complex and contains multiple servers and routers, or if you are running a local Intranet web server. Consult your Network Administrator for more information.

Netscape Proxy Configuration

- Configure Netscape Version 4
    1. Select the Edit menu and click on Preferences
    2. Double click on Advanced in the tree on the left
    3. Select Proxies
    4. Select the Manual Proxy Configuration option on the right and press the View button
    5. For each proxy that you will use, enter the IP address or name of the MailGate server (generally mailgate) and the port it uses.

- **Configure Netscape Version 3**
    1. Select the Options menu and click on Network Preferences
    2. Select the Proxies Tab
    3. Select the Manual Proxy Configuration option and press the View button.
    4. For each proxy that you will use, enter the IP address or name of the MailGate server (generally mailgate) and the port it uses.

Note - The following are the standard ports for some common protocols:

Protocol	Port
HTTP	80
FTP	21
Socks	1080

More Information

Check our web site www.mailgate.com for more detailed information on configuring clients.

Mail Client Configuration

Mail Client Configuration

Your mail client is used to collect mail from your personal mailbox in MailGate, allows you to review this mail and create and send mail to other users. To communicate with MailGate you will need to set the server details to use the MailGate IP address or name and the account details to refer to your mailbox in MailGate.

Note - MailGate uses Internet standards to mail communications and any mail client that supports these standards can be used.

This section covers setting up several common mail clients for use with MailGate.

MS Internet Mail on page 8-5
Eudora Mail on page 8-5
Agent/Free Agent on page 8-6
Virtual Access on page 8-6

MS Outlook Express Configuration

Select Tools then Accounts on the menu and click on the Mail tab. Click on Add and choose Mail to activate the new account wizard or change your existing account details to include the following settings:

1. E-mail address - enter your own address.
2. My incoming mail server is - select POP3
3. Incoming Mail Server - enter the IP address or name for the MailGate server machine.
4. Outgoing Mail Server - enter the IP address or name for the MailGate server machine.
5. Account name - enter the name for your mailbox in MailGate.
6. Password - enter the password used for your mailbox in MailGate. If you have chosen to use NT passwords in MailGate, then the password is your NT login password and you should tick Logon using Secure Password Authentication.
7. Connection - Set this to using a Local Area Network (LAN).

You will probably also want to set this account to be the Default account and adjust the Check for new messages setting in the Tools Options screen to a shorter time.

MS Outlook Configuration

Select Tools then Services on the menu. If you already have an Internet E-mail service you can change this, otherwise click on add to add this service. Set or change your existing service details to include the following settings:

1. E-mail address - enter your own address.
2. Outgoing Mail Server - enter the IP address or name for the MailGate server machine.
3. Incoming Mail Server - enter the IP address or name for the MailGate server machine.
4. Account name - enter the name for your mailbox in MailGate.
5. Password - enter the password used for your mailbox in MailGate. If you have chosen to use NT passwords in MailGate, then you should check Logon using Secure Password Authentication.
6. Connection - Set this to using a Local Area Network (LAN).

You will probably also want to adjust the Check for new messages setting in the Tools Options screens to a shorter time.

MS Internet Mail Configuration

1. Select the Mail menu and click on Options.
2. Select Server tab
3. Fill in Name, Organization and email address
4. Under "Servers" fill in the local IP address or host name of the MailGate server, usually "mailgate" in both the outgoing mail and incoming mail slots.
5. Under Logon settings:
   If you configured MailGate to use NT password authentication then select "Logon using secure password authentication" otherwise select "Logon using" and fill in the name of your mailbox and your password on the MailGate server.

Eudora Mail Configuration

1. Select the Tools menu and click on Options
2. Select Getting started, fill in your pop account details. Note Eudora requires a fully qualified mail name – popname@your_ISP will work correctly for machines on workgroups that are not part of a domain. Add Real name and return address.
3. Select Hosts and enter the SMTP address – this is the MailGate server IP address or name.
4. Select Auto Configure and fill in the Server Name: this is the IP address or name of the MailGate Server. Enter the user name and password for the MailGate POP mailbox.
5. Click OK to accept all changes.

Agent/Free Agent Mail Configuration

1. Select the Options menu and click on General Preferences
2. Select User tab and fill in your email and other personal details.
3. Select System Tab and enter the IP address or name of the MailGate server under both the mail and news server.

Virtual Access Mail Configuration

In Version 4.0+ of Virtual Access, do the following:

1. Select the File menu and click on Comms Setting
2. Select the Internet service to configure
3. On the MAIL tab set the outgoing and incoming mail server as mailgate

More Information

Check our web site www.mailgate.com for more detailed information on configuring clients.

FTP Client Configuration

FTP Client Configuration

You use an FTP client to access an FTP server for uploading or downloading files. Often this is the method used to maintain a web site.

FTP via Browsers

If your browser has already been configured to use the MailGate HTTP proxy server then you need do nothing further for FTP under HTTP to work through the browser. For setting the HTTP proxy, see **Web Browser Client Configuration** on page 8-2.

Note - You should NOT set the FTP protocol in your browser proxy settings to use the MailGate FTP port.

FTP Client Configuration

This section covers setting up some common FTP client programs to use the MailGate Server.

If you have a separate FTP program, you must configure it to use the MailGate FTP proxy.

For information see the listings below for how to configure:

- Cute FTP below
- Internet Neighbourhood on page 8-8
- WS_FTP on page 8-8

Cute FTP Configuration

1. Select the FTP Menu and click on Settings
2. Click on Options and select Firewall tab.
3. Set HOST to point to the MailGate machine. Enter either the IP address or the machine name (generally mailgate).
4. Set PORT to point at relevant port [normally port 21].
5. Leave USER ID and PASSWORD blank
6. Set TYPE to USER
7. Tick to enable firewall access.

Internet Neighbourhood Configuration

Set these properties for each site to which you wish to connect to

1. Firewall Access – ticked
2. Firewall Access Type – RAPTOR (USER fw_usrnam)
3. Firewall Host Information
4. Firewall – MailGate Host Machine ID
5. Leave Username & Password Blank.
6. Leave Passive Mode unchecked.

WS_FTP Configuration

Create a Site Entry for each host you wish to connect to. Set the following properties to use the MailGate proxy.

1. Set the Host Name to the required host site address.
2. Set the User ID and Password as required to access the host.
3. Check Use Firewall on the Firewall Tab.
4. Set the Host Name on the Firewall tab to the IP address or name of your MailGate server.
5. Set the Port on the Firewall tab to the port used by the MailGate proxy.
6. Select the 'USER with no logon' firewall type.

More Information

Check our web site www.mailgate.com for more detailed information on configuring clients.

News Client Configuration

News Client Configuration

You use a News client to connect to a news server to make use of Internet Newsgroups.

News Proxy

You will need to setup and enable a new Custom Proxy or modify the NNTP proxy installed with MailGate to be able to connect to your chosen news server first. See **NNTP Proxy** on page 2-23 for more information.

This section covers setting up some common News programs to use the MailGate Server.

See the pages below for more information on how to configure that program:

» Anawave Gravity below
» Forte Agent/Free Agent below
» News Stand below
» Virtual Access on page 8-10

Anawave Gravity Configuration

1. Select the View Menu and click on Options.
2. Select the Setup tab.
3. Enter the IP address or name of your MailGate server (generally mailgate).
4. Enter name of your mail server

Agent/Free Agent News Configuration

1. Select the Options menu and click on General Preferences
2. Select the System tab.
3. Enter the IP address or name of MailGate server (generally mailgate).
4. Enter name of your mail server

More Information

Check our web site www.mailgate.com for more detailed information on configuring clients.

News Stand Configuration

1. Select the Tools menu and click on Options
2. On the Connections tab select "Use a LAN connection"
3. On the Network tab under the "Host News Server" entry enter the MailGate server IP address or name (generally mailgate).

Virtual Access News Configuration

In version 4.0+, configure your main ISP connection:

1. Select the File menu and click on Comms Settings
2. Select your ISP from the service list
3. On the NEWS tab, enter the IP address or name of your MailGate server as the news server.

In MailGate, configure an NNTP proxy to connect to your ISP.

More Information

Check our web site www.mailgate.com for more detailed information on configuring clients.

9 Technical Reference

Using Wildcards

Using Wildcard Expressions

Some entries in MailGate allow the use of wildcard patterns rather than creating long lists. When creating these entries, you can use special characters to control the matching process.

The following can be used within MailGate to create wildcard patterns :-

? Matches any single character. T?m matches Tim, Tom and tam.

* Matches zero or more characters. Hol*d matches holed and hold.

[ ] Matches any single character that appears within the square brackets. For example, [0123456789] will match any single digit from 0 to 9. You can also specify a range using a dash - for example, [0-9].

^ Indicates the start of a new line. For example, *^Received:* will only return a match if the Received: is found at the start of a new line. Used in extension modules which check email contents.

_ Indicates the match must occur on a single line. For example, _*filename*.exe* will only return a match if the strings filename and .exe occur on a single line.

[^] Matches any single character that does not appear within the square brackets. For example, [^abc] will match any single character except "a", "b" and "c".

\ Matches the following character literally. For example, * will match a single asterisk and \\ will match a single backslash.

! Negate - The matching will return true if the negated pattern is NOT matched. Use this option with care in pattern lists.
For example, on the Setup | Domains Tab !username@mydomain.com will cause MailGate to treat this address as an external address as it is NOT a local domain.

MailGate Macros

Using Macro Expressions

The MailGate Macro Facility is available in a number of the MailGate extension modules. When manipulating mail data it is often desirable to access the current mail information. This can be specified in the set-up screens by using the MailGate macro facility.

When making a setting that supports the use of Macros, existing mail header fields and other data may be referenced by specifying the field in macro format. This is done by surrounding the required field name with %% (example %%SUBJECT%%). When processed the macro specifier is replaced by the content of the required field.

Example

The SPAM extension allows you to change the subject of an email that has been identified as SPAM. The setting that defines what the change should be can be configured with :-

```
SPAM - %%SUBJECT%%
```

This setting will cause the extension to write a new subject field in the mail, adding 'SPAM - ' in front of the existing subject.

Generally the Macro facility can reference any existing mail header fields, however when configuring to use macros be aware that not all header fields are always available in your mails. Availability can depend on your ISP's server system which may be subject to change.

The following fields are regularly found in mail headers and are good candidates for use with macros:-

FROM - The originator's email address.

DATE - The original email's date.

SUBJECT - The original subject.

MESSAGE-ID - The original message ID.

There are also a number of Extension Module specific macro identifiers available. Refer to the module help for more information on these.

MailGate Scripting

Introduction to Scripting

The script language was originally developed as a simple, extendable and flexible method of controlling automated processes under Microsoft Windows NT. This language is fully incorporated into MailGate as the MailGate Scripting language.

The language consists of a simple set of BASIC like commands (see 9-3) which provide all the necessary programming constructs for program development. It also allows the addition of application specific functionality via the use of external function libraries. These are standard Windows NT Dynamic Link Libraries (DLLs) which can be developed in any language that can produce DLLs (such as C, C++ or Delphi) to provide addition features to the base script language.

Within MailGate there is a standard set of functions (see 9-9) available to the user. These include some specialist functions used when creating Custom Proxy scripts. Where scripting is used in a MailGate extension, there may be additional functions made available for use with the extension.

Scripting Syntax & Commands

Scripting Syntax & Commands

The MailGate language consists of a simple set of BASIC like commands that provide all the necessary programming constructs for program development.

The script language is not case sensitive.

The following pages give details of these commands and examples of the language syntax:-

- Integer and string variables
- Integer and string assignments
- Integer and string arithmetic statements
- Integer Boolean statements
- If .. then ... else constructs
- Labels and jumps
- Subroutines
- Repeat ... until constructs
- For ... to/downto ... step...next constructs
- Inclusion of external source files
- Definition of external functions
- Using comments

Integer and string variables

Variables are defined when an assignment to them is first made and they then exist for the duration of the script execution. Variables are of two types, either integer or string. They are named with alphanumeric characters, names are non-case sensitive and must start with a alphabetic character. Integer variables are indicated by ending the name with a '%' and strings with a '$'. String and integer variables of the same name are permitted.

Some example variable names:-

a%	Integer variable 'A'
A%	Integer variable 'A', same variable as previous
a$	String variable 'A', exists as a separate entity to integer variable 'A'
test123$	String variable 'TEST123'
123test$	Invalid variable name - names must not start with a digit.

Integer and string assignments

Variables are created when assignments are made to a previously uncreated variable. The following statements would create and initialise some variables:-

```
a%=1

b%=2

test$ = "Hello"
```

You can also initialise new variables to the value of an already existing variable of the same type:-

```
a%=1

b%=a%

a$="hello"

b$=a$
```

You cannot assign integer values to strings or vice versa.

Integer and string arithmetic statements

String variables support the operation '**+**' which acts as 'string' concatenate. The following script segment shows this:-

```
a$="Hello"

b$="there"

c$="folks"

d$=a$+" "+b$+" "+c$
```

The value of **d$** after executing this script would be "Hello there folks". The '**+**' operator is the only one supported by string variables.

Integer variables support the following arithmetic operators:-

```
+  -  /  *  and  or  xor  not
```

The logic operators **and, or, xor** and **not** do bitwise operations between two integer values, for example '**7 and 3**' would result in the value 4. The integer arithmetic evaluator also supports parenthesis and operator precedence as per the standard rules. Some example arithmetic assignments:-

```
a%=1

b%=2

c%=3

result%=a%*(b%+c%) and 121

notres%=not result%

d%=-c%
```

Integer Boolean expressions

Non-zero values are considered true and zero values false. Two constants exist, TRUE and FALSE which have the value -1 and 0 respectively. Boolean expressions can only exist in if...then...else and repeat...until statements. The following comparison operators are supported:-

```
=     <     >     <=    >=    <>
```

These will evaluate to either the TRUE or FALSE (-1 or 0). The Boolean operators and, or, xor and not work as logic statements on these values. For example:-

```
(a%=1) and (b%=2)
```

would evaluate to TRUE if a% was equal to 1 and b% was equal to 2.

If ... then ... else ... endif

The if statement comes in two forms, the single line form and the multiple line form. If the whole if..then..statement is on one line the '**endif**' is not needed. If the statement is split of a number of lines the statement must be terminated with '**endif**'. For example:-

```
if a%=1 then b%=2
```

or

```
if a%=1 then
   b%=2
endif
```

The else section of the statement is optional. You can separate

statements with the '&' character which acts as a statement separator. You may also use this statement separator anywhere in a script. You can join lines of a script to be treated as a single line with the '_' character, again this can be used anywhere in a script.

Some more example if statements:-

```
if a% < 3 then b%=1 & c%=2 else b%=2 & c%=1

if a% < 3 then b%=1 _
   c% = 2

if a% < 3 then
   b%=1
   c%=2
else
   b%=2
   c%=1
endif

if a%=1 then
   if b%=2 then
      c%=1
   endif
   d%=1
endif
```

Notice that nesting of statements is supported.

Labels and jumps

Unlike BASIC the script language does not have line numbers. It supports jumps but you do this by defining labels in the script. A label is given a text value and is defined by proceeding it with a '**:**'. For example:-

:testlabel

would define the label '**testlabel**' at the particular point in the script. You can jump to labels with the '**goto**' statement. The '**goto**' statement is followed by the label name terminated by a '**:**'. For example:-

goto testlabel:

would jump to the above defined label. Think of the '**:**' symbols joining up to remember where to put the ':'. It is in fact not necessary to use the '**goto**' command and this can be omitted but was included for clarity. The following would be equivalent to the above '**goto**' statement.

testlabel:

The most common use of jumps is in '**if**' statements. For example:-

```
if a%=1 then goto testlabel:
```

```
if a%=2 then testlabel:
```

Both of the above statements would jump to the label if the condition evaluated to true.

Subroutines

Labels can also be used to mark the start of a subroutine. Subroutines are called by the '**gosub'** statement and control returns to the calling point when the '**return**' statement is encountered, for example:-

```
gosub test:
```

```
end
```

```
:test
```

```
a%=1
```

```
b%=2
```

```
return
```

Notice the use of '**end'** to stop the program execution 'dropping through' to the subroutine. All variables are considered global and so subroutine script code can access variables created outside the subroutine and vice versa.

Repeat ... until constructs

The repeat ... until construct repeats the enclosed statements until the logical expression evaluates to true. For example:-

```
count%=1
repeat
   a%=1
   b%=a%*2
   count%=count%+1
until count%=10
```

You can nest repeat ... until statements if desired.

For ... to/downto ... step ... next

This statement offers the familiar BASIC looping construct, some examples:-

```
for i%=1 to 10
   a%=i%*2
```

```
next
for i%=a%*2 to a%*3 step 2
   j%=2
next i%
for i%=10 downto 1 step 2
   j%=2
next
```

Notice that the inclusion of the loop variable after the 'next' is optional.

Inclusion of external source files

The '**#include**' directive includes a source file into the current script at the current point. This is for including lists of external functions or script code for previously written useful subroutines. Include directives can be nested across files up to a limit of 32. Example of include statement:-

```
#include "external.inc"
```

External function definitions

The external function definition directive is the key to the scripting systems power and flexibility. It defines the call interface to routines in a DLL file which have been developed in a suitable language. Once defined the functions can be used as part of the script language. The external definition statement has the following form:-

```
#external <name> ([<parameters>]) [as [async ]<type>] in
<library>
```

where

<name> is the name of the function in the external library.

<parameters> lists the parameters expected. Parameters can be either **string** or **integer** and there may be up to 20. These are listed in the **<parameters>** section separated by commas, for example **string,integer,integer**.

async indicates that the function completes asynchronously. Details of this mechanism will be provided in the developers guide to the scripting language.

<**type**> give the return type of the function which can be **string** or **integer**. Functions that don't return a value can be defined by omitting the **as <type>** section of the statement.

<library> gives the filename of the external function library.

Thus some example external function definitions would be:-

```
#external OpenFile(string) as integer in
"c:\external\external.dll"
```

```
#external CloseFile(integer) in
"c:\external\external.dll"

#external Output(string) in
"c:\external\external.dll"

#external IntToStr(integer) as string in
"c:\external\external.dll"
```

Functions that return integers can be used in integer expressions and those that return strings in string expressions. For example:-

```
file%=OpenFile("test.txt")

a$=IntToStr(32)
```

Comments in Scripts

Comments can be added to scripts by preceding them with '//' as per the C++ convention. This turns the rest of the current line into a comment. Comments do not effect the execution speed of the script. For example:-

```
// This is a comment

// So is this

a%=1 // Set a% to the value 1
```

Scripting Functions

Functions for Scripting

There are a number of standard functions available when using the MailGate scripting language. These are listed below with full details on the following pages.

The MailGate Custom Proxy facility can make use of the script language. An example of this is supplied for use with the Telnet Custom Proxy. There are some functions that are only available to the Custom Proxy usage. These are also listed below.

Some of the MailGate optional extensions, like the Spam Mail Filter, also make use of the scripting language. In this case documentation of the module specific functions can be found in the module help.

Standard MailGate Script Functions

String Functions

length(<string>)
left(<string>,<count>)
right(<string>,<count>)
mid(<string>,<start>,<count>)
pos(<string>,<substring>)
ascii(<string>)
chr(<integer>)
value(<string>)
str(<value>)
hex(<value>)

IP Communications Functions

inet_ntoa(<address>)
inet_addr(<address>)
gethostname()
gethostbyname(<host>)
gethostbyaddr(<addr>)
getnumhosts()
getnumaddrs()
gethost(<index>)
getaddr(<index>)

File I/O Functions

fopen(<filename>,<mode>,<sharing>)
fclose(<handle>)
feof(<handle>)
ftell(<handle>)
ferror(<handle>)
fread(<handle>,<count>)
fwrite(<handle>,<message>)
fseek(<handle>,<offset>,<from>)

Windows Registry Functions

regqueryval(<hive>,<key>,<value>)
regquerystr(<hive>,<key>,<value>)
regsetval(<hive>,<key>,<valuename>,<value>)
regsetstr(<hive>,<key>,<valuename>,<value>)

Event Log Functions

logevent(<message>)
debug(<string>)

Custom Proxy Script Functions

Control Functions

connect(<server>,<port>)
proxy()

Client Communication Functions

write(<message>)
readch()
readln(<termination>)
read(<count>)

Proxy Communication Functions

pwrite(<message>)
preadch()
preadln(<termination>)
pread(<count>)

Function Length(<String>)

Parameters -

Value	Type	Description
<String>	string	String to get length of

Return Type - Integer

Operation

Returns the length of the passed string expression as an integer value.

Function Left(<String>,<Count>)

Parameters -

Value	Type	Description
<String>	string	String to extract left portion from
<Count>	integer	Number of characters of <string> to return

Return Type - String

Operation

Returns a string of the <count> leftmost characters from <string>. If the length of <string> is less than <count> the whole of <string> is returned.

Function Right(<String>,<Count>)

Parameters -

Value	Type	Description
<string>	string	String to extract right portion from
<Count>	integer	Number of characters of <string> to return

Return Type - String

Operation

Returns a string of the <count> rightmost characters from <string>. If the length of <string> is less than <count> the whole of <string> is returned.

Function Mid(<String>,<Start>,<Count>)

Parameters -

Value	Type	Description
<String>	string	String to extract portion from
<Start>	integer	Start position to extract portion
<Count>	integer	Number of characters of <string> to return

Return Type - String

Operation

Returns a string of <count> characters starting from position <start> from <string>. If there are less than <count> characters after position <start> in <string> a string of the available characters after <start> is returned. If <start> is a position after then end of <string> a blank string is returned.

Function Pos(<String>,<Substring>)

Parameters -

Value	Type	Description
<String>	string	String to search
<Substring>	string	Seach string

Return Type - Integer

Operation

Returns the position of the first occurrence of <substring> in <string>. If <substring> does not exist in <string> returns zero.

Function Ascii(<String>)

Parameters -

Value	Type	Description
<String>	string	String to get code for

Return Type - Integer

Operation

Returns the ASCII code for the first character of the passed string expression as an integer value.

Function Chr(<Integer>)

Parameters -

Value	Type	Description
<Integer>	integer	ASCII code to convert to string

Return Type - String

Operation

Returns a string containing the single character for the passed ASCII code.

Function

Parameters -

Value	Type	Description
<String>	string	String to convert

Return Type - Integer

Operation

Returns the integer value represented by the passed string. If the string does not represent an integer value zero is returned.

Function Str(<Value>)

Parameters -

Value	Type	Description
<Value>	integer	Value to convert to string

Return Type - String

Operation

Returns a string of digits representing <value>.

Function Hex(<Value>)

Parameters -

Value	Type	Description
<Value>	integer	Value to convert to string

Return Type - String

Operation

Returns a string of hex digits representing <value>.

Function Inet_ntoa(<Address>)

Parameters -

Value	Type	Description
<Address>	integer	IP address as 32bit network byte ordered value

Return Type - String

Operation

Returns a string representing the passed IP address in dotted octet form. Uses Winsock inet_ntoa function internally.

Function Inet_addr(<Address>)

Parameters -

Value	Type	Description
<Address>	string	IP address as dotted octet string

Return Type - See Below

Operation

Returns a 32 bit network byte ordered value representing the string passed. Uses Winsock inet_addr function internally.

Function Gethostname()

Parameters - None

Return Type - String

Operation

Returns a string giving the hostname of the computer that MailGate is running on. Uses Winsock gethostname function internally.

Function Gethostbyname(<Host>)

Parameters -

Value	Type	Description
<Host>	string	Host to obtain information about

Return Type - Integer

Operation

Gets host information available for the passed hostname and stores it in an internal buffer. The getnumhosts, getnumaddrs, gethost, and getaddr functions can then be used to access the information. Returns zero if successful or socket error code if not.

Function Gethostbyaddr(<Addr>)

Parameters -

Value	Type	Description
<Addr>	integer	IP address as 32bit network byte ordered value to obtain information about

Return Type - Integer

Operation

Gets host information available for the passed address and stores it in an internal buffer. The getnumhosts, getnumaddrs, gethost, and getaddr functions can then be used to access the information. Returns zero if successful or socket error code if not.

Function Getnumhosts()

Parameters - None

Return Type - Integer

Operation

Returns an integer value giving the number of hostnames available in the internal buffer filled by the last call to gethostbyname or gethostbyaddr. Returns zero if no information is available because gethostbyname or gethostbyaddr has not been called yet or the last call returned an error.

Function Getnumaddrs()

Parameters - None

Return Type - Integer

Operation

Returns an integer value giving the number of addresses available in the internal buffer filled by the last call to gethostbyname or gethostbyaddr. Returns zero if no information is available because gethostbyname or gethostbyaddr has not been called yet or the last call returned an error.

Function Gethost(<Index>)

Parameters -

Value	Type	Description
<Index>	integer	Index position to read hostname from internal structure

Return Type - String

Operation

Returns a string value giving the hostname at the <index> position in the internal buffer. Returns a blank string if no hostname available at the requested position or no data in the internal buffer. Note that gethost(1) will return the primary name of the host and gethost(2..n) will return any aliases the host has.

Function Getaddr(<Index>)

Parameters -

Value	Type	Description
<Index>	integer	Index position to read address from internal structure

Return Type - See Below

Operation

Returns the IP address as 32bit network byte ordered value at the <index> position in the internal buffer. Returns zero if no address available at the requested position or no data in the internal buffer.

Function Fopen(<Filename>,<Mode>,<Sharing>)

Parameters -

Value	Type	Description
<Filename>	string	Name of file to be opened
<Mode>	string	The string class=pmode specifies the type of access requested for the file, as follows:- class=op"r" Opens for reading. If the file does not exist or cannot be found, the class=op>fopen call fails. class=op"w" Opens an empty file for writing. If the given file exists, its contents are destroyed. class=op"a" Opens for writing at the end of the file (appending) without removing the EOF marker before writing new data to the file; creates the file first if it doesn't exist. class=op"r+" Opens for both reading and writing. (The file must exist.) class=op"w+" Opens an empty file for both reading and writing. If the given file exists, its contents are destroyed. class=op"a+" Opens for reading and appending; the appending operation includes the removal of the EOF marker before new data is written to the file and the EOF marker is restored after writing is complete; creates the file first if it doesn't exist. class=opt Open in text (translated) mode. In this mode, class=kn CTRL+Z is interpreted as an end-of-file character on input. In files opened for reading/writing with class=op "a+", class=op fopen checks for a class=kn CTRL+Z at the end of the file and removes it, if possible. This is done because using class=op>fseek and class=op ftell to move within a file that ends with a class=kn CTRL+Z, may cause class=op>fseek to behave improperly near the end of the file. Also, in text mode, carriage return-linefeed combinations are translated into single linefeeds on input, and linefeed characters are translated to carriage return-linefeed combinations on output. When a Unicode stream-I/O function operates in text mode (the default), the source or destination stream is assumed to be a sequence of multibyte characters. Therefore, the Unicode stream-input functions convert multibyte characters to wide characters (as if by a call to the class=op>mbtowc function). For the same reason, the Unicode stream-output functions convert wide characters to multibyte characters (as if by a call to the class=op>wctomb function). class=op b Open in binary (untranslated) mode; translations involving carriage-return and linefeed characters are suppressed.
<Sharing>	integer	Controls sharing of the file with other processes whilst open by the calling process. Can be one of the following values:- 0 or 16 - deny read and write access 32 - deny write access 48 - deny read access 64 - deny none

Return Type - Integer

Operation

Opens the file and returns a value to be used as the file handle in the other file functions. Returns zero if error.

Function Fclose(<Handle>)

Parameters -

Value	Type	Description
<Handle>	integer	A file handle value returned by the fopen function

Return Type - Logical Integer

Operation

Closes the file. Note that all files opened by a script will automatically be closed when the script session terminates.

Function Feof(<Handle>)

Parameters -

Value	Type	Description
<Handle>	integer	A file handle value returned by the fopen function

Return Type - Logical Integer

Operation

Checks if at the end of the passed file. Returns -1 (TRUE) if position is end of file or zero if not.

Function Ftell(<Handle>)

Parameters -

Value	Type	Description
<Handle>	integer	A file handle value returned by the fopen function

Return Type - Integer

Operation

Returns the current position in the passed file. Returns -1 if error occurs.

Function Ferror(<Handle>)

Parameters -

Value	Type	Description
<Handle>	integer	A file handle value returned by the fopen function

Return Type - Integer

Operation

Returns the current error state of the passed file. Returns zero if no error.

Function Fread(<Handle>,<Count>)

Parameters -

Value	Type	Description
<Handle>	integer	A file handle value returned by the fopen function
<Count>	integer	Number of bytes to read from file

Return Type - String

Operation

Returns a string buffer containing the requested number of bytes from the passed file. If an error occurs or there are not enough bytes available in the file the returned string may be shorted than the requested count. Use feof and ferror to determine further information if this occurs.

Function Fwrite(<Handle>,<Message>)

Parameters -

Value	Type	Description
Handle	Integer	A file handle value returned by the fopen function
<Message>	string	Buffer to write to file

Re**turn Type** - Integer

Operation

Writes the passed buffer to the passed file. Returns the number of bytes written which if write successful will be the length of the passed string. If an error occurs the returned value may be less than the length of the passed string.

Function Fseek(<Handle>,<Offset>,<From>)

Parameters -

Value	Type	Description
<Handle>	integer	A file handle value returned by the fopen function
<Offset>	integer	Number of bytes to move in file
<From>	integer	Indicates the type of move to make as follows:- 0 = move to <offset> bytes from start of file 1 = move to <offset> bytes from current location in file 2 = move to <offset> bytes from end of file

Return Type - Integer

Operation

Moves the current file position as indicated by the parameters. Returns zero if successful or non-zero if error.

Function Regqueryval(<Hive>,<Key>,<Value>)

Parameters -

Value	Type	Description
<Hive>	integer	Value indicating the registry hive to read from as follows:- 0 = HKEY_LOCAL_MACHINE 1 = HKEY_CURRENT_USER 2 = HKEY_CLASSES_ROOT 3 = HKEY_USERS
<Key>	string	Full path giving key to read from, e.g. "software\IDSL\MailGate"
<Value>	string	Name of value to read

Return Type - See Below

Operation

Returns a 32bit integer value giving the DWORD value at the given registry location. Returns zero if error occurs.

Function Regquerystr(<Hive>,<Key>,<Value>)

Parameters -

Value	Type	Description
<Hive>	integer	Value indicating the registry hive to read from as follows:- 0 = HKEY_LOCAL_MACHINE 1 = HKEY_CURRENT_USER 2 = HKEY_CLASSES_ROOT 3 = HKEY_USERS
<Key>	string	Full path giving key to read from, e.g. "software\IDSL\MailGate"
<Value>	string	Name of value to read

Return Type - String

Operation

Returns a string giving the REG_SZ value at the given registry location. Returns zero length string if error occurs.

Function Regsetval(<Hive>,<Key>,<Valuename>,<Value>)

Parameters -

Value	Type	Description
<Hive>	integer	Value indicating the registry hive to read from as follows:- 0 = HKEY_LOCAL_MACHINE 1 = HKEY_CURRENT_USER 2 = HKEY_CLASSES_ROOT 3 = HKEY_USERS
<Key>	string	Full path giving key to write to, e.g. "software\IDSL\MailGate"
<Valuename>	string	Name of value to write
<Value>	integer	32bit value to write to registry as REG_DWORD data

Return Type - Integer

Operation

Writes the given data value to the registry as a REG_DWORD item. Returns zero if successful or Win32 error code if not.

Function Regsetstr(<Hive>,<Key>,<Valuename>,<Value>)

Parameters -

Value	Type	Description
<Hive>	integer	Value indicating the registry hive to read from as follows:- 0 = HKEY_LOCAL_MACHINE 1 = HKEY_CURRENT_USER 2 = HKEY_CLASSES_ROOT 3 = HKEY_USERS
<Key>	string	Full path giving key to read from, e.g. "software\IDSL\MailGate"
<Valuename>	string	Name of value to write to
<Value>	string	String to write to registry as REG_SZ data

Return Type - Integer

Operation

Writes the given data value to the registry as a REG_SZ item. Returns zero if successful or Win32 error code if not.

Function Logevent(<Message>)

Parameters -

Value	Type	Description
<Message>	string	string to write to MailGate event log

Return Type- None

Operation

Writes the given string to the MailGate event log as a script event (type column '~').

Function Debug(<String>)

Parameters -

Value	Type	Description
<String>	string	String to write to debug

Return Type - None

Operation

Write <message> to the system debug console. If MailGate is being run under a debugger the debugger will display <message>.

Function Connect(<Server>,<Port>)

Parameters -

Value	Type	Description
<Server>	string	Hostname or IP address as dotted octet string to connect to
<Port>	integer	Port number to connect to

Return Type - Integer

Operation

Connects the proxy side socket to the given server and port. Return value is zero if successful or socket error code if not.

Note - This function is only applicable to Custom Proxy scripts.

Function Proxy()

Parameters - None

Return Type - Integer

Operation

Proxies data in both directions between the client socket connection that initiated the script and a connection established using the connect function until one or other side closes their connection or a socket error occurs. Returns zero if one side closed the connection gracefully or socket error code if socket error occurred.

Note - This function is only applicable to Custom Proxy scripts.

Function Write(<Message>)

Parameters -

Value	Type	Description
<Message>	string	Message to write to lan client

Return Type - Integer

Operation

Writes the passed string to the client socket connection that initiated the script. Return value is zero if successful or socket error code if failure.

Note - This function is only applicable to Custom Proxy scripts.

Function Readch()

Parameters - None

Return Type - String

Operation

Reads a single character from the client socket connection that initiated the script and returns it as a single character string. If an error occurs the returned string will have zero length.

Note - This function is only applicable to Custom Proxy scripts.

Function Readln(<Termination>)

Parameters -

Value	Type	Description
<Termination>	string	Sequence of characters to look for as the termination of a line

Return Type - String

Operation

Reads a line of text from the client socket connection that initiated the script and returns it as a string. A line is considered all text up to and including the sequence **<termination>**. Normally termination would be passed as **chr(13)+chr(10).**

Note - This function is only applicable to Custom Proxy scripts.

Function Read(<Count>)

Parameters -

Value	Type	Description
<Count>	integer	Number of bytes to read

Return Type - String

Operation

Reads <count> bytes from the client socket connection that initiated the script and returns it as a string. If a socket error occurs before the requested number of bytes has been read then the function returns a string of the bytes that were available. Thus to check for error or socket closure compare the length of the returned string with the requested number of bytes.

Note - This function is only applicable to Custom Proxy scripts.

Function Pwrite(<Message>)

Parameters -

Value	Type	Description
<Message>	string	Message to write to lan client

Return Type - Integer

Operation

Writes the passed string to the proxy socket connection established with the connect function. Return value is zero if successful or socket error code if failure.

Note - This function is only applicable to Custom Proxy scripts.

Function Preadch()

Parameters - None

Return Type - String

Operation

Reads a single character from the proxy socket connection established with the connect function and returns it as a single character string. If an error occurs the returned string will have zero length.

Note - This function is only applicable to Custom Proxy scripts.

Function Preadln(<Termination>)

Parameters -

Value	Type	Description
<Termination>	string	Sequence of characters to look for as the termination of a line

Return Type - String

Operation

Reads a line of text from the proxy socket connection established with the connect function and returns it as a string. A line is considered all text up to and including the sequence **<termination>**. Normally termination would be passed as **chr(13)+chr(10).**

Note - This function is only applicable to Custom Proxy scripts.

Function Pread(<Count>)

Parameters -

Value	Type	Description
<Count>	integer	Number of bytes to read

Return Type - String

Operation

Reads <count> bytes from the proxy socket connection established with the connect function and returns it as a string. If a socket error occurs before the requested number of bytes has been read then the function returns a string of the bytes that were available. Thus to check for error or socket closure compare the length of the returned string with the requested number of bytes.

Note - This function is only applicable to Custom Proxy scripts.

Function

Parameters -

Value	Type	Description
None	None	
<string>	string	
<integer1>	integer	

Return Type - None

Operation

Calling this function

Windows Registry

Windows Registry

MailGate stores its configuration in the registry. All settings are stored under the section:-

HKEY_LOCAL_MACHINE

Software

IDSL

Mailgate

Within this key there is one string value '**InstallPath**' which the install script writes to enable it to easily find the installation for future upgrade installs. There are also number of registry key sections under this location discussed in the following sections.

Parameters

Most of the MailGate general settings are stored in this key. The values and purpose are as follows:-

Value Name (Data Type)	Description
AlwaysCheckMail (DWORD)	Controls whether Mailgate checks for new email at the start of any new connection or only when a connection is established by a mail collection schedule. 1 = always collect, 0 = only for mail collection schedules.
CopyOutgoing (String)	Name of local account to receive copies of all outgoing email or blank string if no copies to be made.
DebugIt (DWORD)	When set to non zero value each time mgatesvc is started it will create a log file debugit.log in the mailgate root directory. This log will received detailed protocol and i/o information that can be used by the developers to diagnose problems. Default is 0 and this value should not be altered unless under the direction of MailGate support staff.
DefaultMailbox (String)	Name of local account to receive messages that can't be delivered to a local account by the routing rules and automatically generated admin messages.

(Registry Parameters – cont.)

DisconnectMode (DWORD)	Option selected on the disconnect dialog when last used. 0 = disconnect when all activity ceases, 1 = disconnect immediately.
DnsAlternativeDelay (DWORD)	Time Mailgate waits for a response from a Dns server given in the DnsServers list before re-issuing the packet to the next server in the list. This value is not normally present and defaults to 1000. If you wish to change this setting manually add this value using the registry editor. The value gives the delay in milliseconds.
DnsBinding (DWORD)	Binding setting for DNS service. 0 = no interface binding, any other value stores the interface address as a 32 bit binary value.
DnsDenied (Multi-String)	List of name or ip address pattern match strings indicating which clients are denied access to the dns relay.
DnsDialupEnabled (DWORD)	Controls whether a new connection is established to do a dns reverse lookup for checking security settings of a service. 0 = don't connect, 1 = do connect.
DnsEnable (DWORD)	Controls whether Mailgate runs the DNS relay. 0 = don't run, 1 = run.
DnsPermitted (Multi-String)	List of name or ip address pattern match strings indicating which clients are permitted access to the pop service.
DnsReadTimeout (DWORD)	Socket timeout setting for read operations by the DNS relay, value given in seconds.
DnsServers (Multi-String)	List of dns servers dns relay relays dns packets to. Servers may be specified by the IP address as a string or by the dns servers name.
DnsTimeout (DWORD)	Idle disconnect time for the dns relay, value in seconds.
DnsWriteTimeout	Socket timeout setting for write operations by the DNS relay, value given in seconds.
EmailConnectFailure (DWORD)	Controls whether or not Mailgate generates an error email message in the default mailbox when there is a failure to connect to a pop server for email collection. This value is not normally present and defaults to 1. If you wish to change the setting add the setting using the registry editor. 0 = don't report errors, 1 = report errors.

(Registry Parameters – cont.)

EnablePurgeDays (DWORD)	Controls whether the web cache purge system checks number of days pages have been in the cache when deciding whether or not to purge pages from the cache. 0 = don't check, 1 = check.
EnablePurgeSize (DWORD)	Controls whether the web cache purge system checks the cache size when deciding whether or not to purge pages from the cache. 0 = don't check, 1 = check.
EnablePurgeSpace (DWORD)	Controls whether the web cache purge system checks the available disk space when deciding whether or not to purge pages from the cache, 0 = don't check, 1 = check.
ErrorImageFile (String)	Can be used to set an alternative file an image for the web proxy error page. This value is not normally present and defaults to 'logo.gif'. If you wish to change the setting add the setting using the registry editor.
ErrorTemplateFile (String)	Can be used to set an alternative file for the web proxy error template file. This value is not normally present and defaults to 'errors.html'. If you wish to change the setting add the setting using the registry editor.
ExpandCustom (DWORD)	Indicates whether or not the Custom Proxy branch of the main display window is expanded or not. Used by Mailgate to re=establish the display at startup to the same state it was in when last run. 0 = not expanded, 1 = expanded.
ExpandFilters (DWORD)	As ExpandCustom for the Url filters branch.
ExpandHistory (DWORD)	As ExpandCustom for the History branch.
ExpandMailboxes (DWORD)	As ExpandCustom for the Mailboxes branch.
ExpandQueue (DWORD)	As ExpandCustom for the Queue branch.
ExpandRoot (DWORD)	As ExpandCustom for the root of the tree.
ExpandScheduling (DWORD)	As ExpandCustom for the Schedules branch.
Extensions (Multi String)	Array of strings giving names of extensions currently present. The first character is either a 1 or 0 indicating whether the extension has been enabled or disabled. This information is generated automatically.
Forwards (Multi String)	An array of wildcard pattern strings and server to forward to. Each email received is compared against these strings and if match the email is queued for SMTP forwarding to the corresponding server address.

(Registry Parameters – cont.)

FtpBinding (DWORD)	Binding setting for Ftp gateway service. 0 = no interface binding, any other value stores the interface address as a 32 bit binary value.
FtpDenied (Multi-String)	List of name or ip address pattern match strings indicating which clients are denied access to the ftp gateway.
FtpEnable (DWORD)	Controls whether the Ftp gateway is enabled or not, 0 = disabled, 1 = enabled.
FtpPermitted (Multi-String)	List of name or ip address pattern match strings indicating which clients are permitted access to the ftp gateway.
FtpProxyPort (DWORD)	Socket port number that the Ftp gateway listens on, normally 21.
FtpReadTimeout (DWORD)	Timeout for socket read operations by the Ftp gateway service, value given in seconds.
FtpTimeoutEx (DWORD)	Idle disconnect time for the Ftp gateway, value in seconds.
FtpWriteTimeout	Timeout for socket write operations by the Ftp gateway service, value given in seconds.
HistorySize (DWORD)	Number of connections Mailgate keeps in the History list display. Value not normally present and defaults to 25. If you wish to change the size of the history list manually add this value using the registry editor and set the value to the required number of entries.
HttpBinding (DWORD)	Binding setting for Http proxy service. 0 = no interface binding, any other value stores the interface address as a 32 bit binary value.
HttpDenied (Multi-String)	List of name or ip address pattern match strings indicating which clients are denied access to the http proxy.
HttpEnable (DWORD)	Controls whether the Http proxy is enabled or not, 0 = disabled, 1 = enabled.
HttpKeepAlive (DWORD)	Controls whether the MailGate http proxy honours keep alive requests. Default value is 1 (do keep alive), 0 = don't do keep alive.
HttpPermitted (Multi-String)	List of name or ip address pattern match strings indicating which clients are permitted access to the http proxy.

(Registry Parameters – cont.)

HttpProxyIgnore (Multi String)	An array of wildcard strings for matching against url requests. Any match will stop that request being sent through a remote proxy if you have enabled this feature in MailGate.
HttpProxyPort (DWORD)	Socket port number that the Http proxy listens on, normally 80.
HttpProxyServer (String)	Name or ip address of a proxy server for Mailgate to pass all web requests through.
HttpProxyServerPort (DWORD)	Port number the proxy server given in the HttpProxyServer setting is running on.
HttpReadTimeout (DWORD)	Timeout for socket read operations by the Http proxy service, value given in seconds.
HttpTimeoutEx (DWORD)	Idle disconnect time for the Http proxy, value in seconds.
HttpUseFtpProxy (DWORD)	Controls whether ftp:// url requests made to the Mailgate web proxy are routed through the proxy server given in the HttpProxyServer setting or the request is made direct to the requested ftp server. 0 = direct, 1 = pass to proxy.
HttpUseProxy (DWORD)	Controls whether http:// url requests made to the Mailgate web proxy are routed through the proxy server given in the HttpProxyServer setting or the request is made direct to the requested web server. 0 = direct, 1 = pass to proxy.
HttpUseSecureProxy (DWORD)	Controls whether https:// url requests made to the Mailgate web proxy are routed through the proxy server given in the HttpProxyServer setting or the request is made direct to the requested web server. 0 = direct, 1 = pass to proxy.
HttpWriteTimeout (DWORD)	Timeout for socket write operations by the Http proxy service, value given in seconds.
IsIconic (DWORD)	Indicates whether Mailgate is currently in the iconic (minimized) state or not. Used at startup to restore Mailgate to the same state as when last used. 0 = not iconic, 1 = iconic.
IsZoomed (DWORD)	Indicates whether Mailgate is currently in the zoomed (maximized) state or not. Used at startup to restore Mailgate to the same state as when last used. 0 = not zoomed, 1 = zoomed.

(Registry Parameters – cont.)

KeepAliveMaxRequests (DWORD)	Sets the maximum number of requests that a http socket session will allow using keep alive. Default value is 5.
LastId (DWORD)	Last message id used for internally generated email messages. Value is incremented after each auto generated message.
LicenseString (String)	The license key for this installation of Mailgate
LiquidAudioBinding (DWORD)	Binding setting for Liquid Audio proxy service. 0 = no interface binding, any other value stores the interface address as a 32 bit binary value.
LiquidAudioDenied (Multi-String)	List of name or ip address pattern match strings indicating which clients are denied access to the Liquid Audio service.
LiquidAudioPermitted (Multi-String)	List of name or ip address pattern match strings indicating which clients are permitted access to the Liquid Audio service.
LiquidAudioReadTimeout (DWORD)	Timeout for socket read operations by the Liquid Audio proxy service, value given in seconds.
LiquidAudioTimeoutEx (DWORD)	Idle disconnect time for the Liquid Audio proxy, value in seconds.
LiquidAudioWriteTimeout (DWORD	Timeout for socket write operations by the Liquid Audio proxy service, value given in seconds.
LocalDomainsEx (Multi-String)	List of email domains to be treated as local.
LogFilePurgeDays	Indicates the number of days log files remain in the log directory before being auto-deleted.
LogFilePurgeEnabled	Indicates whether log file purging option is enabled or disabled. 0 = disabled, non-zero = enabled.
Logging (DWORD)	Set of bit flags indicating what information is to be written to the log file. 1 = Errors 2 = Warnings 4 = Information 64 = Pop email collection protocol 128 = Pop client session protocol 256 = Smtp email transmission protocol 512 = Smtp client session protocol 1024 = Debugging messages 2048 = Web access log

(Registry Parameters – cont.)

MaxWorkstations (DWORD)	Indicates the maximum number of workstations (remote IP addresses) that are permitted to use the MailGate system at any one time. Default is 99999. If the 'NT workstation licencing constraint' was enabled during installation this value will be 10.
MbReportDay (DWORD)	Indicates the day of the month that the last oversized mailbox report was generated for the mailboxes with this feature enabled. Used so that MailGate can know if it has already produced a report during the current day.
Minimize (DWORD)	Controls whether Mailgate automatically minimizes itself on startup. 0 = don't minimize, 1 = minimize.
NtAccountDomain (String)	Name of NT server domain that is to be used for Pop account password validation. Only available with Nt version.
Platform (String)	Platform that Mailgate is running on, will be 'Windows95' or 'WindowsNT'.
PoolThreadsPerProcessor (DWORD)	Indicates the number of worker threads to create in the thread pool for each processor in the computer system. This value is not normally present and defaults to 4. If you wish to change the setting manually add the value using the registry editor and set to the required value.
PopBinding (DWORD)	Binding setting for Pop service. 0 = no interface binding, any other value stores the interface address as a 32 bit binary value.
PopCheckInterval (DWORD)	If repeated checking of Pop accounts during a connection is enabled this value controls how often checks occur. Default value is zero (disabled), other values set interval of checks in seconds.
PopDenied (Multi-String)	List of name or ip address pattern match strings indicating which clients are denied access to the pop service.
PopEnable (DWORD)	Controls whether the Pop service is enabled or not, 0 = disabled, 1 = enabled.
PopOversizeCheck (DWORD)	Maximum size of pop message allowed before deferment takes place. Setting to zero disables oversized checking. Default value is zero.
PopOversizeNotifyAdmin (DWORD)	Indicates whether the administrator account should be notified by email of oversized message deferments. 1 = notify, 0 = do not notify, default value is 1.

(Registry Parameters – cont.)

PopOversizeNotifyUser (DWORD)	Indicates whether the account (s) that would have received a deferred message should be notified by email of the message deferment. 1 = notify, 0 = do not notify, default value is 1.
PopPermitted (Multi-String)	List of name or ip address pattern match strings indicating which clients are permitted access to the pop service.
PopReadTimeout (DWORD)	Timeout for socket read operations by the Pop service, value given in seconds.
PopServerPort (DWORD)	Port Mailgate runs the Pop service on. Normally this registry value will not be present and the service defaults to the standard Pop port of 110. If it is required to modify this manually add the value using the registry editor and set it to the required port number.
PopTimeoutEx (DWORD)	Idle disconnect time for the Pop service, value in seconds.
PopWriteTimeout (DWORD)	Timeout for socket write operations by the Pop service, value given in seconds.
PurgeDays (DWORD)	Number of days cached web pages are kept on disk before being purged by Mailgate. Only used if the EnablePurgeDays setting is enabled.
PurgeSize (DWORD)	Size in KB that the web cache is allowed to grow to before pages are purged from the cache. Only used if the EnablePurgeSize setting is enabled.
PurgeSpace (DWORD)	Size in KB of free disk space that must exist on the web cache drive. If space becomes less than this value pages are purged from the cache. Only used if the EnablePurgeSize setting is enabled.
RasAccountEx (String)	Login account for RAS dialup. Stored as an encrypted string.
RasAlertActions (DWoRD)	Bitmap indicating actions to take on connection timeout. 1 = sound beeps, 2 = Email admin, 3 = Force disconnection.
RasAlertTimeout (DWORD)	This sets the maximum connected session time before MailGate starts its alarm process. Default is zero (disabled), other values give timeout in minutes.
RasBackupAccount (String)	Login account for the backup RAS configuration. Stored as an encrypted string.

(Registry Parameters – cont.)

RasBackupEntry (String)	Name of the Ras phonebook entry to be used for establishing a dialup connection if the primary entry is unavailable.
RasBackupPassword (String)	Backup login account password for dialup. Stored as an encrypted string.
RasEmailFailure (DWORD)	Controls whether or not Mailgate generates an error email message in the default mailbox when there is a failure to connect to the ISP using RAS. This value is not normally present and defaults to 1. If you wish to change the setting add the setting using the registry editor. 0 = don't report errors, 1 = report errors.
RasEntry (String)	Name of the Ras phonebook entry to used for establishing a dialup connection. If blank no RAS dialup is undertaken and Mailgate assumes there is a permanent routed Internet connection.
RasPasswordEx (String)	Login account password for RAS dialup. Stored as an encrypted string.
RasPopAccessCheck (DWORD)	Controls whether Mailgate checks to see if a pop client session has connected to the Ras tcp/ip interface rather than the lan one. If it has Mailgate will keep the Ras connection open until the session ends. This setting is not normally present and defaults to 1. If you wish to change the setting manually add the value using the registry editor. 0 = don't check, 1 = check.
RasPostDialCmd (String)	Command to be executed immediately after to a RAS dialup session ends.
RasPostDialTerminate (DWORD)	Indicates whether the post-dial command process should be terminated if it runs for longer than the timeout value. 1= terminated, 0 = don't. Default 1.
RasPostDialTimeout (DWORD)	Amount of time in seconds that the post-dial command is allowed to complete execution. Default 300.
RasPostDialWait (DWORD)	Indicates whether the dialing process will wait for the completion of the post-dial command. 1 = wait, 0 = don't. Default 1.
RasPreDialCmd (String)	Command to be executed immediately prior to a RAS dialup.
RasPreDialTerminate (DWORD)	Indicates whether the pre-dial command process should be terminated if it runs for longer than the timeout value. 1= terminated, 0 = don't. Default 1.

(Registry Parameters – cont.)

RasPreDialTimeout (DWORD)	Amount of time in seconds that the pre-dial command is allowed to complete execution. Default 300.
RasPreDialWait (DWORD)	Indicates whether the dialing process will wait for the completion of the pre-dial command. 1 = wait, 0 = don't. Default 1.
RasSmtpAccessCheck (DWORD)	Controls whether Mailgate checks to see if a smtp client session has connected to the Ras tcp/ip interface rather than the lan one. If it has Mailgate will keep the Ras connection open until the session ends. This setting is not normally present and defaults to 1. If you wish to change the setting manually add the value using the registry editor. 0 = don't check, 1 = check.
RasUseExisting (DWORD)	Indicates whether RAS should utilise an already existing connection or fail. Default 0. Should only be changed if you realise the conflict this can cause with the dialup connection and other apps using it.
RealAudioBinding (DWORD)	Binding setting for RealAudio proxy service. 0 = no interface binding, any other value stores the interface address as a 32 bit binary value.
RealAudioDenied (Multi-String)	List of name or ip address pattern match strings indicating which clients are denied access to the RealAudio proxy service.
RealAudioPermitted (Multi-String)	List of name or ip address pattern match strings indicating which clients are permitted access to the RealAudio proxy service.
RealAudioProxyPort (DWORD)	Socket port number that the RealAudio proxy listens on, normally 1090.
RealAudioReadTimeout (DWORD)	Timeout for socket read operations by the RealAudio proxy service, value given in seconds.
RealAudioTimeout (DWORD)	Idle disconnect time for the RealAudio proxy service, value in seconds.
RealAudioReadTimeout (DWORD)	Timeout for socket read operations by the RealAudio proxy service, value given in seconds.
RegisteredTo (String)	Name of company or individual this install of Mailgate is licensed to.

(Registry Parameters – cont.)

RemoveEnvelopeFields (DWORD)	Controls whether Mailgate strips out the envelope address fields from collected email headers or not. This value is not normally present and defaults to 0. If you wish to strip out the fields manually add the setting using the registry editor. The default value is 0, 0 = do not strip, 1 = strip.
ReportEmailAddress (String)	Email address that system report emails are sent to. May be an internal or external address.
RootPath (String)	String giving path to root of data storage area to be used by Mailgate. Default is to the location the Mailgate executables have been installed.
ScriptEditWindow (String)	Contains the size and position of the script editor window. The X Y W H values appear as a string of 4 space separated numbers.
SendImmediately (DWORD)	Controls whether Mailgate senses external email as soon as it is received by the smtp server if a connection exists or waits until the next scheduled email transfer. 0 = wait for schedule, 1 = send immediately.
SmtpBinding (DWORD)	Binding setting for Smtp service. 0 = no interface binding, any other value stores the interface address as a 32 bit binary value.
SmtpDenied (Multi-String)	List of name or ip address pattern match strings indicating which clients are denied access to the Smtp service.
SmtpEnable (DWORD)	Controls whether the Smtp service is enabled or not, 0 = disabled, 1 = enabled.
SmtpGateway (String)	Name or ipaddress of Smtp server at ISP to be used for passing all outgoing email to.
SmtpNoFromCheck (DWORD)	Controls if MailGate should check for a From: address. Some email clients responding to a Read Receipt send an acknowledgement with no From address. As many ISP servers will not accept these messages, MailGate by default will not accept them. Use this setting to bypass the check. 0 = check enabled, 1 = check disabled.
SmtpPermitted (Multi-String)	List of name or ip address pattern match strings indicating which clients are permitted access to the Smtp service.
SmtpReadTimeout (DWORD)	Timeout for socket read operations by the Smtp service, value given in seconds.
SmtpRelayDenied (Multi String)	List of name or ip address pattern match strings indicating which clients are denied access to use the smtp server to relay email to external addresses.
SmtpRelayPermitted (Multi String)	List of name or ip address pattern match strings indicating which clients are permitted access to use the smtp server to relay email to external addresses.

(Registry Parameters – cont.)

SmtpSendDelay (DWORD)	Delay in seconds before smtp transmission of outgoing email starts following a dialup connection. Default is zero.
SmtpSendPort (DWORD)	Port to connect to for sending outgoing email during dialup connections. Default is the standard SMTP port 25.
SmtpServerPort (DWORD)	Port Mailgate runs the Smtp service on. Normally this registry value will not be present and the service defaults to the standard Smtp port of 25. If it is required to modify this manually add the value using the registry editor and set it to the required port number.
SmtpWriteTimeout (DWORD)	Timeout for socket write operations by the Smtp service, value given in seconds.
SocksBinding (DWORD)	Binding setting for Socks proxy service. 0 = no interface binding, any other value stores the interface address as a 32 bit binary value.
SocksDenied (Multi-String)	List of name or ip address pattern match strings indicating which clients are denied access to the Socks proxy service.
SocksEnable (DWORD)	Controls whether the Socks proxy service is enabled or not, 0 = disabled, 1 = Socks V4 enabled, 2 = Socks V5 enabled, 3 = both Socks V4 and V5 enabled.
SocksHttpDivert (DWORD)	Controls whether Socks requests for port 80 (http) are passed to the Mailgate http proxy server so that the web cache can be checked for the request. 0 = don't divert, 1 = divert.
SocksPermitted (Multi-String)	List of name or ip address pattern match strings indicating which clients are permitted access to the Socks proxy service.
SocksProxyPort (DWORD)	Socket port number that the Http proxy listens on, normally 1080.
SocksReadTimeout (DWORD)	Timeout for socket read operations by the Socks proxy service, value given in seconds.
SocksTimeout (DWORD)	Idle disconnect time for the Socks proxy service, value in seconds.
SocksWriteTimeout (DWORD)	Timeout for socket write operations by the Socks proxy service, value given in seconds.

(Registry Parameters – cont.)

StatusBarCounter (DWORD)	Indicates which counter to show on the status bar. 0 = cycle through counters, +ve number indexes counter in the order of the popup list.
SupportEmail (String)	Domain to send support email to. This value is not usually present and defaults to 'mailgate.com' If you wish to change the setting add the value using the registry editor. Mailgate pre-pends support@, bugs@ or wishlist@ to the string to get the address to email the support request. Suppliers providing their own support services for their Mailgate customers should use this facility to get support messages sent to them.
SupportRepyAddress (String)	Email address the user has entered on the support dialog.
UnknownHandling (DWORD)	Controls the handling of email that is received but does not have a mailbox for delivery. If this value is zero the message will be bounced to the originator. If it is non-zero it will be delivered to the email address indicated by the UnknownReceipient setting.
UnknownRecipient (String)	Email address for messages collected that don't have a local mailbox. Address my be local or external.
UseNtAccounts (DWORD)	Indicates whether the pop server checks passwords against Mailgate registry or Nt accounts database in the domain set in the NtAccountDomain setting. 0 = use Mailgate password database, 1 = use Nt domain database. Only present in Nt version of Mailgate.
Version (String)	Always contains the last version of Mailgate run on the system
WindowH (DWORD)	Height of the Mailgate main window. Used at Mailgate startup to restore Mailgate to the same size and position as when last run.
WindowW (DWORD)	Width of the Mailgate main window. Used at Mailgate startup to restore Mailgate to the same size and position as when last run.
WindowX (DWORD)	Screen X position of the Mailgate main window. Used at Mailgate startup to restore Mailgate to the same size and position as when last run.
WindowY (DWORD)	Screen Y position of the Mailgate main window. Used at Mailgate startup to restore Mailgate to the same size and position as when last run.

Schedules

The schedules key is used to store the schedules setup in Mailgate. Under the schedules key Mailgate creates a key for each schedule entered. These keys are named Schedule0, Schedule1 and so on for the required number of schedules. The data stored in each of these keys is the same as follows:

Value Name (Data Type)	Description
Days (DWORD)	Flag value indicating days of week that the schedule is active on with flag values as follows:- 1 = Sunday 2 = Monday 4 = Tuesday 8 = Wednesday 16 = Thursday 32 = Friday 64 = Saturday
Enabled (DWORD)	Indicates whether the schedule is enabled or not. 0 = disabled, 1 = enabled.
EndTime (DWORD)	Time the schedules active period ends, value given as minutes from midnight.
Every (DWORD)	Number of minutes between email collection sessions during the active period of the schedule.
MinRedial (DWORD)	Minimum time between redials in seconds.
StartTime (DWORD)	Time the schedules active period starts, value given as minutes from midnight.
Type (DWORD)	Type of schedule, as follows:- 0 = Email transfer 1 = Enable web proxy 3 = Enable ftp gateway 4 = Enable priority email trigger 5 = Enable socks gateway 6 = Enable RealAudio proxy 7 = Outgoing email trigger 8 = Liquid audio proxy 9 = Connect permanently 10 = Transfer email if present 11 = Timeout override

Collection

The collection key is used to store the list of pop servers to collect email from. Under the schedules key Mailgate creates a key for each Pop collection entered. These keys are named Collection0, Collection1 and so on for the required number of pop collection. The data stored in each of these keys is the same as follows:

Value Name (Data Type)	Description
Account (String)	Pop account to collect from, stored as an encrypted string.
Command (String)	External command to run during collection process or blank string if no command to run.
CmdMode	When the command is to run, values as follows:- 0 = Run before starting pop collection 1 = Run after pop collection 2 = Run instead of pop collection
CmdWait	Controls whether or not Mailgate waits for the external command to complete before continuing with collection process. 0 = Don't wait, 1 = wait.
Field (String)	Custom routing field in message headers to search for or blank if standard Mailgate routing logic to be used.
FilterEx (String Array)	List of wildcard pattern match strings to filter email addresses against. Email addresses that don't match any of the pattern strings are dropped.
LeaveDays (DWORD)	Number of days to leave collected email on the pop server before deleting it.
Mapping (String)	String to map email address or domain part of address to the given string.
Password (String)	Password for the pop account to collect from. Stored as an encrypted string.
RemoveString (String)	String to be removed from the email addresses extracted during collection.
Server (String)	Ip address or name of the pop server to collect email from.

Proxies

The proxies key is used to store the list of custom proxies configured in Mailgate. Under the proxies key Mailgate creates a key for each custom proxy configured. These keys are named Proxy0, Proxy1 and so on for the required number of proxies. The data stored in each of these keys is the same as follows:

Value Name (Data Type)	Description
Binding (DWORD)	Binding setting for the custom proxy. 0 = no interface binding, any other value stores the interface address as a 32 bit binary value.
ConnectPort (DWORD)	Port number that proxy connects or forwards datagram packets to.
ConnectServer (String)	Ip address or name of system that proxy connects to or forwards datagram packets to.
Days (DWORD)	Flag value indicating days of week that the custom proxy is active on with flag values as follows:- 1 = Sunday 2 = Monday 4 = Tuesday 8 = Wednesday 16 = Thursday 32 = Friday 64 = Saturday
Denied (Multi-String)	List of name or ip address pattern match strings indicating which clients are denied access to the custom proxy.
Description (String)	String describing the purpose of the custom proxy.
Enabled (DWORD)	Indicates whether the custom proxy is enabled or not. 0 = not enabled, 1 = enabled.
EndTime (DWORD)	Time the proxy's active period ends, value given as minutes from midnight.
Interfaces (Multi-String)	List of interface ip addresses that the custom proxy listens on.

ListenPort (DWORD)	Socket port number the custom proxy listens on.
Permitted (Multi-String)	List of name or ip address pattern match strings indicating which clients are permitted access to the custom proxy.
ReadTimeout (DWORD)	Timeout for socket read operations by the custom proxy, value given in seconds.
Script (DWORD)	Indicates whether or not the custom proxy has a script. 0 = no script, 1 = script present.
ScriptFile (String)	Name of the file that the script is stored in. Scripts are stored in the Script directory that is created in the Mailgate install directory.
StartTime (DWORD)	Time the proxy's active period starts, value given as minutes from midnight.
Timeout (DWORD)	Idle disconnect time for the custom proxy, value in seconds.
Type (DWORD)	Type of custom proxy, 0 = Stream proxy, 1 = Datagram proxy.
UsesRas (DWORD)	Indicates whether the custom proxy requires a Ras connection or not. If not the custom proxy won't cause a dialup to occur. 0 = doesn't use Ras, 1 = does use Ras.
WriteTimeout (DWORD)	Timeout for socket write operations by the custom proxy, value given in seconds.

Mailboxes

The mailboxes key is used to store details of the pop accounts setup in Mailgate. Each account has a number of entries of the form '<accountname> <setting>' as follows:

Value Name (Data Type)	Description
<account> flags (DWORD)	Set of flags indicating mailbox options selected, flags as follows:- 1 = Auto reply 2 = Delete incoming 4 = Forward 8 = Pop collection
<account> forwardex (Multi-String)	List of addresses to forward copy of email delivered to the account to.
<account> password (String)	Password for the account stored as an encrypted string.
<account> popaccount (String)	Account to collect email from direct into account, stored as an encrypted string. Only used if the flags value has the pop collection flag set.
<account> popleavedays (DWORD)	Number of days to leave email on the pop server after collection before deleting. Only used if the flags value has the pop collection flag set.
<account> poppassword	Password to account to collect email from direct into account, stored as an encrypted string. Only used if the flags value has the pop collection flag set.
<account> popserver	Ip address or name of pop server to collect email from direct into account, stored as an encrypted string. Only used if the flags value has the pop collection flag set.

Counters

This key is used to store the number of active sessions of each type of facility in Mailgate. It is a volatile key and the values contained within are not user changeable.

10 The Log File Viewer

Introduction to the Log File Viewer

The Log Viewer is a utility program supplied with MailGate to make the task of monitoring and reviewing the MailGate log files easier.

The Log File Viewer is installed as part of your MailGate installation process and is ready for use with the local MailGate system.

The Log Viewer can be accessed either through the *View Logs* option on the Logging menu item or by running the program Mglogvwr.exe which is installed in the MailGate folder. You may also wish to create a shortcut to this program that can be placed on your desktop.

With the Log Viewer you can :-

- Select the logfile to review from a simple dropdown list.
- Find text within the selected file.
- Use the powerful filter option to limit the entries displayed. Filtering can be by entry type or by specifying a filter text string.
- '*Lock*' the viewer to the current log file for a continuous display of logged activity.
- Install a copy of the viewer on a remote PC and monitor your MailGate systems activity remotely.

Using the Log File Viewer

Using the Log Viewer

When first started the Log File Viewer will display a screen similar to the one below.

All the Viewer functions may be accessed using either the Menus or the Tool bar.

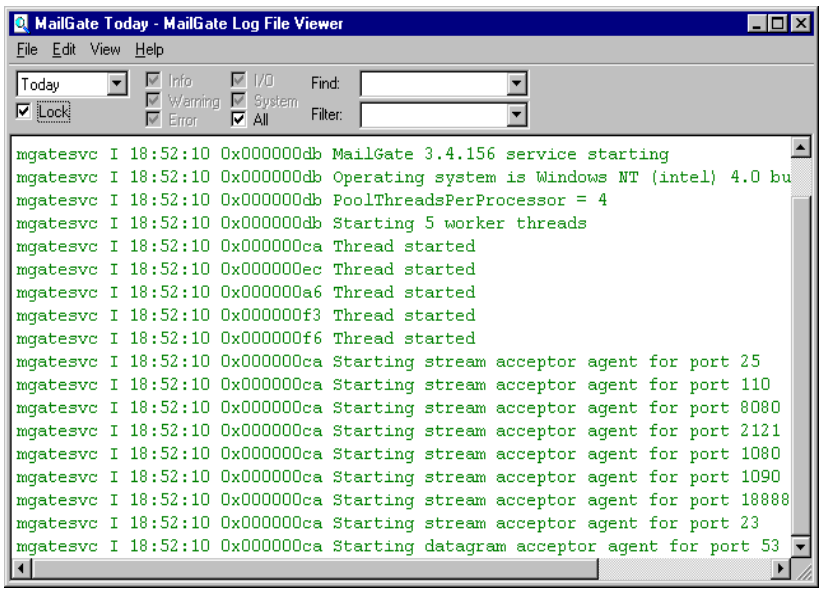

Figure 32 - Log File Viewer

When you exit from the Log Viewer your current settings will be saved.

The Menu Bar

The Log File Viewer menu option give access to all the options available on the Tool bar.

Using the File menu, you can select the log file (see 10-3) to view.

The Find (see 10-3) and Filter (see 10-3) options can be found on the Edit menu.

Using the View menu you can turn off the Menu and Tool bars by unchecking the respective options. This reduces the window size and may be useful if you wish to use the viewer in *locked* mode for a

continuous display (see 10-4) of logged activity. Checking the Always on Top option will make the Viewer window stay visible in the foreground. When the Menu bar is hidden, you can move the entire window by holding down the Control key and then dragging the window using the mouse by clicking anywhere in the display window.

 If the Menu bar is hidden all the menu options are still available by right-clicking in the file display window.

Selecting the File to View

Use the drop down on the Tool bar or the File/Recent Logs item to select the log file to review. The selected file will now be displayed in the display window.

If you select the file *Today*, the *Lock* option for continuous activity display (see 10-4) will also be available.

Using Find

The Find option in the Log File Viewer is a quick way to find a particular text string in the current selected log file.

Find can be accessed either directly from the Tool bar or from the popup screen displayed when you choose the *Find* menu item.

To use the Find option, enter the string to find in the field displayed. If you are accessing Find using the Tool bar press F3 to find the next occurrence or Shift-F3 to find the previous occurrence of the string. If you are using the popup screen, use the radio button to select Up or Down and click OK.

Using 'Find Selected'

Find may be activated by using the Find Selected item available on the Edit menu. To use this, highlight the required string in the File Display Window then select the Find Selected option. The highlighted string will be passed into the Find setting and the find activated.

Using Filters

The Filter options in the Log File Viewer are a powerful way of selecting specified information in the log file to view.

Filter settings can be accessed either directly from the Tool bar or from the popup screen displayed when you choose the *Filter* menu item.

There are two methods for filtering the data -

1. Line Type Filtering

Each line in the log file has a line type. This is indicated by the character in the second column of the log. By using the check boxes in the line type filter, only lines of the chosen type(s) will be displayed.

The line type characters used are :-

I	- Informational Lines
W	- Warnings
E	- Errors
*	- I/O Lines (< indicates inbound data, > is data sent)
!	- System messages

2. String Filtering

By typing a text string into the *Filter* field the viewer will only display log lines which contain a matching string. The last few entries made are saved and may be selected by using the dropdown in this field.

Using 'Filter Selected'

The string filter method may be activated by using the Filter Selected item available on the menu. To use this, highlight the required filtering string in the File Display Window then select the Filter Selected option. The highlighted string will be passed into the Filter setting and the filter activated.

The File Display Window

The File Display window displays the contents of the current selected log file. You can scroll up and down the file using the scroll bar to the right of the window.

The Log Viewer menu may be accessed by right-clicking anywhere in the display window. This is useful if you have turned off the Menu and Tool bars.

You can also move the entire window by holding down the Control key and then dragging the window using the mouse by clicking anywhere in the display window.

Continuous Monitoring

Continuous monitoring of log file activity can be enabled by using the *Lock* option. The display window will update automatically with new logged events as they occur.

To activate continuous monitoring, you must select the file *Today*, then select the *Lock* option on the tool bar or from the menu. The lock can be released by either deselecting the option above or by moving the vertical scroll bar to the right of the display window.

You can set a filter (see 10-3) to only display matching logged items.

 If you use the view menu you can turn off the Menu and Tool bars as well as set the viewer to be 'always on top'. The display window may now be re-sized to suit and will always be visible. Remember the viewer menu can be accessed by a right-click anywhere in the display window.

Installing a Remote Viewer

To use the Remote Log File Viewing capability you must first complete two install steps -

1. Install the Remote Admin Extension

The Remote Admin Extension provides remote access to the MailGate log files. You must install, configure and enable this module on your MailGate server to use the Remote Logfile Viewing facility. Please refer to the Module Help for more information on how to do this.

2. Install a remote copy of the Log File Viewer

To be able to remotely view MailGate log files you need to install a copy of the Log File Viewer onto the remote workstation. To do this you should run the install program on the remote machine and select the option to only install the Log File Viewer utility.

There is no configuration required in the viewer so you will now be able run the program and connect to your remote system. See **Using a Remote Viewer** below for more information.

Using a Remote Viewer

The Remote File Viewing option allows you to connect with and monitor in real time your MailGate system log file, all from a remote workstation.

Once you have completed the required installation steps, you can connect to your remote server either by selecting *Remote MailGate System* on the File Menu item or by using the shortcut Ctrl-R. This will display the connection dialog.

In the **Connect to Remote Server** dialog you should enter or select the address of the remote MailGate system you wish to connect to, enter the appropriate password and ensure the port is set the same as the setting used on the remote system. You should also consider which event types you wish to view (see below). Click OK and a connection will be established with your remote system.

Once a remote connection is in use, all the normal facilities of the Log File Viewer are available for use.

About Event Types.

To reduce the bandwidth requirement when remote viewing you should take care to only view those event types you need to see. The event filtering is performed at the remote system so network traffic is kept at a minimum. This may be particularly important if viewing across a remote TCP/IP link.

Using Command Line Parameters

The Log File Viewer utility may be started from a command line or shortcut with a number of parameters which will establish the remote connection on startup. These parameters are :-

-remote:<server>[:<port>]

-pwd:<password>

-flags:[A][I][W][E][O][S]

where

A = All

I = Info

W = Warning

E = Error

O = I/O

S = System

event types.

Note - If no flags parameter is specified the flags used for the last remote connection are assumed.

Example command line:

mglogvwr -remote:192.168.1.1 -pwd:secret -flags:WES

11 Glossary of Terms

Glossary of Terms

ASCII

American Standard Code for Information Interchange. The set of 255 characters recognized by most computers. These characters are plain text with no formatting information.

Browser (or Web Browser)

A software program that receives and displays information from the World Wide Web (WWW).

Cache

A local store of information used to speed performance by servicing a request rather than having to contact the true source of the data.

Client

The workstation or PC in a Client/Server environment. The Client is the end recipient.

DHCP

Dynamic Host Configuration Protocol. Software included in the operating system that automatically assigns IP addresses to stations on a network.

DNS

Domain Name System is a distributed database system for translating computer names into numeric Internet addresses used when transferring your messages and commands across the Internet.

Domain Name

The part of an Internet address that identifies the address group. Example: in sales@mailgate.com, mailgate.com is the Domain Name.

DUN

Dial-Up Networking. The software that provides the Winsock connection between your computer and your Internet Service Provider.

FTP

The file transfer protocol often used to send files around the Internet. There are public ftp sites where you can download public domain and shareware programs, updated drivers for your PC's graphics card and many other useful files.

Gateway

A link between two systems. Gateways are also used between systems that may otherwise be incompatible.

HTTP

HyperText Transfer Protocol, the mechanism and standards underlying the world wide web. Sometimes also used to refer to a web server. Sometimes used in the form SHTTP or HTTPS to refer to a high security web server.

ISDN

Integrated Services Digital Network. An international standard for transmission over digital lines running at 64 Kbps.

ISP

Internet Service Provider. The company that provides you with your connection to the Internet.

LAN

Local Area Network is a system connecting multiple computers together.

Localhost

A special TCP/IP address which refers to the current machine. Also known as the Loopback address. Uses the reserved IP address of 127.0.0.1.

NNTP

The mechanism and underlying standard for processing News in Internet newsgroups.

POP3

Post Office Protocol 3 is an advanced Internet mail service that allows your ISP to store your mail for you until you dial in. You may also be able to store collected mail for reference for a certain time. With this protocol the 'Recipient' contacts the 'Sender' and requests the data.

PSTN

Public Switched Telephone Network. The worldwide voice telephone network.

RAS

Remote Access Server. The Microsoft Windows software application for managing dialup connections.

Router

A computer system that stores and forwards data packets - using network addresses - from one network to another.

Server

A computer that holds applications or data shared by users on a network.

SMTP

Simple Mail Transfer Protocol is used to send e-mail across the Internet. With this protocol the 'Sender' contacts the 'Recipient' and transmits the data.

SOCKS

SOCKS is a network proxy system equipped with security, auditing, management, fault tolerance, and alarm notification. SOCKS is often used for a firewall.

TCP/IP

Transmission Control Protocol/Internet Protocol is the protocol used for sending information between computers connected to the Internet.

URL

Uniform Resource Locator. A consistent and structured way of writing machine names or addresses of specific types that is used and understood by most internet software.

World Wide Web addresses take the form http://address or http://ip_address

FTP addresses take the form ftp://address