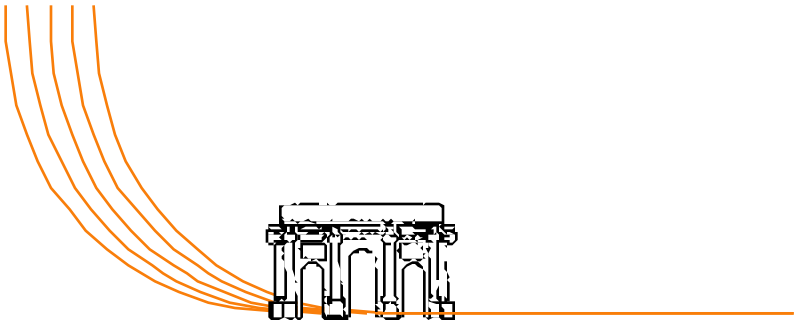
VICOM



User Guide

Changes to Documentation or Software. Vicom Technology Ltd. reserve the right to revise this Guide, and/or the VICOM software and to make any changes without the obligation to notify any person of such changes.

License, Warranty, Limitation of Liability. Details of the software License, Warranty and Limitation of Liability are found in Appendix B of this User Guide. Users of VICOM software are specifically referred to these matters.

Support. Support for VICOM products is provided to registered users through the following contacts.

Contacting Vicom Technology

Support and Product Information

World Wide Web:	http://www.vicomtech.com/appleshare.ip
Email - Information:	info@vicomtech.com

USA & Canada

Email - Support:	as-ip.support.am@vicomtech.com
Email - Sales:	sales_1@vicomtech.com
Address:	465 Fairchild Drive, Suite 202, Mountain View, CA 94043
Telephone:	415 967 5506
Fax :	415 691 9838

UK & International

Email - Support:	as-ip.support.eu@vicomtech.com
Email - Sales:	sales@vicomtech.com
Address:	34/36 Poole Hill, Bournemouth, BH2 5PT, England
Telephone:	+44 (0) 1202 293 233
Fax :	+44 (0) 1202 310 241

Additional User Upgrades

Your VICOM Internet Gateway software license allows you to use it for the licensed number of concurrent users.

Licenses for additional concurrent users are available. Prices and ordering information can be found at the Vicom Technology Web Site at:

http://www.vicomtech.com/

Alternatively, please email **sales@vicomtech.com** or use the other contact information provided at the front of this Guide.

1 Introduction

What is the VICOM Internet Gateway?

The VICOM Internet Gateway is a TCP/IP software router application that runs on a single Macintosh and interconnects local and wide area networks of computers to each other and to the Internet.

The VICOM Internet Gateway uses a Network Address Translation Proxy system to connect a private TCP/IP network to the public Internet. This allows multiple "client" computers to share a single Internet connection, and a single IP address, simultaneously.

A modem or ISDN connection to the Internet using PPP or SLIP protocol is dialed automatically on demand, and disconnected when no longer in use.

The private network can use Ethernet, Token Ring or AppleTalk (via LocalTalk, Apple Remote Access or AppleTalk routing).

Wide area intranet links can be set up to use PPP or SLIP for dial-in or dial-out. The Gateway can be used as a Remote Access Server, with security managed through Macintosh Users & Groups.

The Network Address Translation Proxy feature on the Internet connection ports provides an effective Firewall, preventing any unwanted intrusion into your private network from the public Internet.

For a basic Internet Access configuration, the Gateway configures itself and your Client machines automatically. Comprehensive configuration and monitoring options are accessed using a familiar Macintosh user interface.

Client configuration is achieved using a built-in DHCP Server, supporting multi-subnet fixed and dynamic IP address management for up to 1024 clients.

About this Guide

The VICOM Internet Gateway offers a comprehensive set of TCP/IP routing and network administration facilities. To provide a progressive introduction to these capabilities, the product and this Guide define two levels of complexity, referred to as the Basic and Advanced User Modes.

The first Chapters include information on the following subjects:

- The System and Network Requirements for Gateway configurations.
- Installing and Configuring the Gateway and its Clients for basic Internet access.
- Operating and Customizing the Gateway using its Basic User Mode facilities.

The later Chapters explain how you can use the Gateway to:

- Control user access to the Gateway and to public network locations.
- Manage inbound connections through the Firewall to internal servers.
- Monitor and log user activity.
- Provide secure dial-in remote access to your LAN.
- Customize the built-in DHCP Server to support multiple LAN segments, and fixed addresses.
- Configure manual routing tables to inter work with other Gateways and routers in a multi-segment intranet.

Chapter 2 explains how to install the Gateway, Chapter 3 tells you how to set up local Client computers to access the Gateway, and Chapter 4 shows you how to extend the facilities to remote Clients. By following these Chapters you should be able to build and use a basic configuration for shared Internet access.

Chapters 5 and 6 provide reference material the Gateway's operating and configuration facilities.

Chapters 7 to 12 give more detail on the concepts of TCP/IP addressing, routing and firewalls, and describe the many Advanced Mode features of the software.

Chapter 13 gives guidance on troubleshooting, and describes the diagnostic features of the Gateway software that will assist you in resolving problems.

If you are not familiar with TCP/IP routing concepts, we recommend that you set up the Gateway by following Chapters 2 to 6 on Installation and Operation first. By the end of Chapter 6 you should be able to connect clients on your Local Area Network through the Gateway to your Internet Service, and you will have an understanding of the way the Gateway operates. This will provide a starting point for understanding the later material in the Guide.

What do you need?

To use the VICOM Internet Gateway you need an account with an Internet Service Provider. The equipment and information you require in order to connect will depend on the kind of service you choose. The service may be:

- A dial-up service for which you are responsible for providing a suitable modem and any routing facilities required at your premises. This is the most common type of service at the time of writing.
  In this case you need to obtain, from your Service Provider, all the information specified in the next Chapter.
- A dial-up, leased line or cable service, for which the Service Provider installs connection and routing equipment at your premises. You then connect your Ethernet network directly to the Service Provider's equipment.
  In this case your Service Provider should tell you the IP addresses for your LAN connection, and their Domain Name Server.
  In some cases you may also be expected to provide other items, such as a primary Domain Name Server or a mail server. It is beyond the scope of the Gateway documentation to cover the provision of these functions, but you should refer to Chapter 9 on Inbound Mapping for information on how to make them accessible through the Gateway.

If you are required to provide the connection equipment, you should select the fastest modem or ISDN facility you can, as this will minimize the delays for users accessing web and FTP sites. The Gateway supports modems and external ISDN Terminal Adapters via the Macintosh serial interface ports, using the Apple Modem Tool software which is supplied with the Gateway. You must ensure that the cable you use to connect your Macintosh to the modem is a high speed serial cable supporting hardware handshaking.

Various internal ISDN cards are also supported via the Comms Toolbox connection software provided by the card manufacturers. At the time of writing, Vicom Technology has tested the Gateway with cards made by Sagem, Hermstedt and SCii.

If your Internet service is provided through an ethernet interface, for example via a cable modem or a router, the Gateway machine requires a separate Ethernet interface for this connection. This may be the built-in Ethernet interface on the Macintosh, or a plug-in Ethernet adapter card.

One or more local area network (LAN) connections are required on the Gateway Macintosh for the Client computers. These may use any combination of the built-in Ethernet or LocalTalk interfaces, and plug-in Ethernet or Token Ring adapter cards. You require one network interface for each LAN segment you wish to connect.

The Gateway supports Ethernet and Token Ring adapters on Nubus or PCI machines. PCI Ethernet adapters may operate at the 100 MBit/sec fast Ethernet standard. This enables the Gateway to work as an IP bridge between 10 MBit/sec and 100 MBit/sec cables.

You may use the Gateway as a Remote Access Server, allowing users to dial into your network to access the internal network servers or to connect through to the Internet. For this purpose you can add modems or ISDN adapters, using multi-port serial cards to augment the two Macintosh built-in serial ports if necessary.

The Gateway can be configured with up to eight ports in all. The Gateway Macintosh itself will count as one port if it runs TCP/IP applications, leaving seven ports for any combination of local or remote connections. For complex configurations requiring more ports than this, several Gateway or SoftRouter systems can be set up to partition the functions.

The VICOM Internet Gateway runs on any Macintosh system with the following minimum specification:

- A Macintosh with at least a 68020 processor and a 13" monitor. (See also the notes below)
- At least 2.5 MBytes available memory
- At least 1.5 MByte available disk space
- System Software version 7.0 or later

Notes on CPU requirements:

1. To achieve optimum throughput with an external ISDN terminal adapter, a Macintosh with a high speed serial port is recommended. These are built-in on Quadra AV and PowerPC models. On lower specification systems a high speed port can be provided using a plug-in serial card.
2. If you plan to use LocalTalk cable to connect the clients to the Gateway, the minimum recommended system is a Mac IIci or equivalent.

Please read the notes on Performance Considerations in Chapter 13 for more details.

Information Required from Your Internet Service Provider

To use the Gateway for connection to the Internet, you need an account with an Internet Service Provider. This section lists the information you will need if you choose a dial-up account.

If your Macintosh has previously been set up to dial into your account using MacPPP or FreePPP, the Gateway will read the existing settings during its configuration process. If this is not the case, make sure you obtain the following information from your Internet Service Provider:

- Protocol used for connection (SLIP or PPP)
- Whether the account is configured for static or dynamic IP addressing
- For static addressing, the assigned Internet IP address. An IP address is normally stated as a four-number sequence, such as 198.45.123.25
- The IP address of the Internet Access Provider's Domain Name Server (also known as DNS).
- The telephone number to access the account
- The user name and password for your account
- The login protocol used by the Service Provider. This may be PAP or a scripted sequence of prompts and responses.
- For scripted connection you need to know the prompts and responses. For example:

prompt	**Login:**	respond with account user name
prompt	**Password:**	respond with account password
prompt	**Protocol:**	respond with protocol type, such as SLIP or PPP

2 Installation & Configuration

About this Chapter

This Chapter describes how to Register your Gateway, how to install it on your Macintosh computer, and how to run the Auto-Setup process.

If you are using a modem or ISDN connection to the Internet, driven by the Apple Modem Tool, the Auto-Setup sequence should take you to the stage where you can use the Gateway to connect to the Internet. If you are using another connection method such as cable modem, a Service Provider's router, or an ISDN card Comms Toolbox driver, then this Chapter includes information on making "Manual Additions" to the configuration to handle these cases.

Following the configuration stage, you will be advised how to test the installation. Chapter 3 then describes how you configure Client computers to use the Gateway.

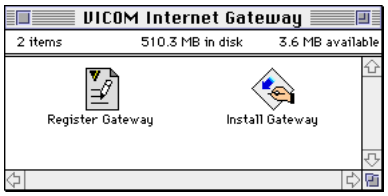
Registering your Gateway

By registering as a VICOM Internet Gateway owner on-line at the VICOM web site below, you will be able to access our Support services, and we can keep you up to date on our product developments.

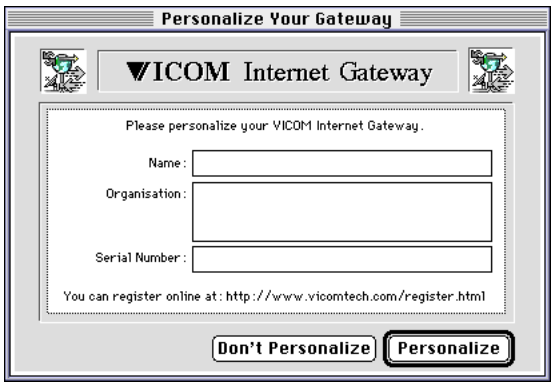
http://www.vicomtech.com/register.html

The Gateway software must also be personalized before it can be installed. Note that you do not need to personalize demonstration versions.

Put the VICOM Internet Gateway diskette into your Macintosh.



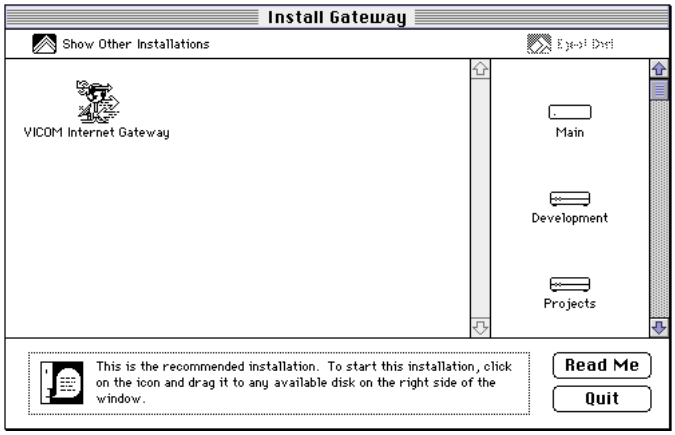
Double-click **Register Gateway** and, the following window is displayed:



Enter your name, organization and the Gateway serial number given in your registration document, and click on the **Personalize** button.

Installing the Gateway

To install the Gateway, double-click on the “Install Gateway” icon. After an introductory screen the following window is displayed:



The PowerPC native version of the software requires Open Transport system software. If you are using MacTCP on a PowerPC then you must install the 680x0 version. Switch to this option by clicking "Show Other Installations" at the top of the screen.

Drag the “VICOM Internet Gateway” icon to the icon for your Startup Disk on the right. This will create a folder on the disk called “VICOM Internet Gateway”, and install the following files:

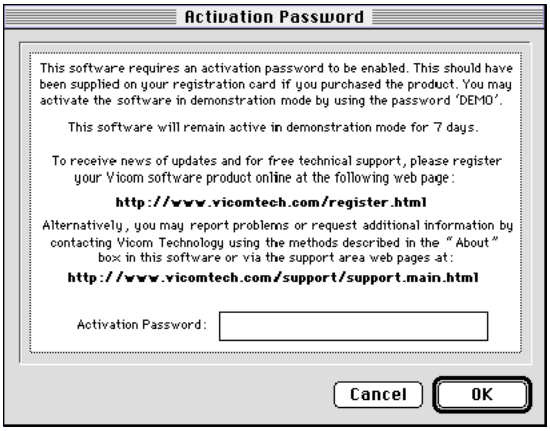
- “VICOM Internet Gateway” - the Gateway application.
- One or more ReadMe files providing supplementary information about the version you have installed.
- An empty "DHCP Clients" file. This is a text file in which you can assign user names to machine addresses.
- “Apple Modem Tool” - this file is put in the Extensions folder in your System Folder, and is used to make Modem PPP and SLIP connections to the Internet or to support dial-in users.
- "-Gateway-" - this file is also put in the “Extensions” folder, and enables TCP/IP client or server applications to be used on the Gateway Macintosh.

Entering the Activation Password

Double-click the VICOM Internet Gateway icon to start the application.

The first time you open the Gateway it will prompt for an activation password. If you are installing a licensed copy of the product the password is printed on your registration document. If you are installing a demonstration version, use “DEMO” as the activation password.

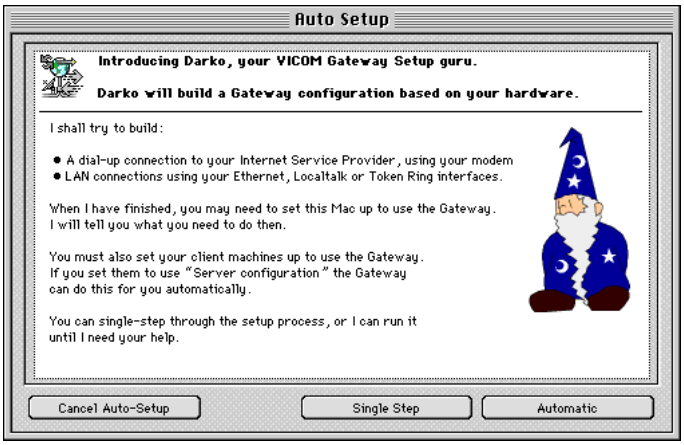
Please note that the password is case sensitive, and ensure that you enter the password exactly as it appears on your registration document.



Configuring the Gateway

When first opened, the Gateway attempts to configure itself automatically, based on the configuration of your computer. You can also run this Auto-Setup sequence manually at any time.

Darko, the Gateway Guru, will guide you through the process.



There are two ways in which you can run the configuration.

'Single Step' will allow you to read and acknowledge each stage of the configuration as it progresses.

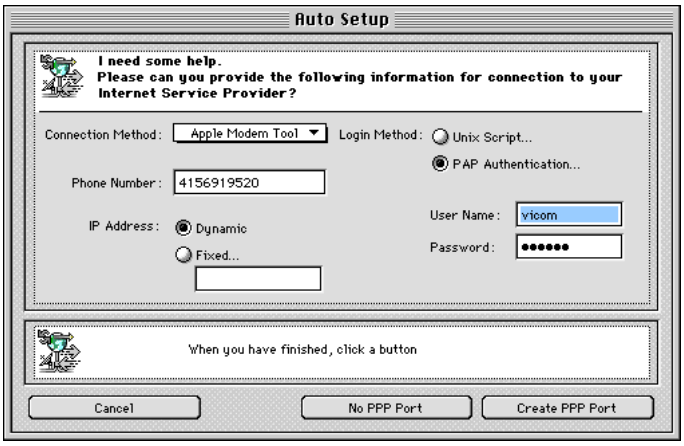
'Automatic' will build the configuration without interaction, only prompting you for key questions, which are explained further in this Guide. We recommend that for first installations the Automatic button is selected. Darko will stop and wait when he needs your answers.

Whenever a 'Cancel' button is displayed you can click on it to leave the automatic setup process, and use the manual editing options instead.

Step 1 - Building a PPP Port

First, Darko will try to build a PPP port. This is used to dial your Internet Service Provider using your modem or ISDN adapter.

Darko will look for a MacPPP or FreePPP Preferences file, and will import the information about its most recently used configuration. If he can't find a suitable preferences file, Darko will ask you to fill in the following screen.



All the information requested should have been supplied to you by your Internet Service provider. Read Chapter 1, "Information Required from Your Internet Service Provider" for more details. When you have completed the above screen select "Create PPP Port" to proceed with the configuration.

If you do not intend to use a PPP dial-up modem connection you should click the "No PPP Port" button at this point. You may want to do this because your Internet connection is via Ethernet, or will use the SLIP protocol, or if you have a plug-in ISDN card. In these cases you can continue the Auto Setup process and then configure your Internet configuration manually. See "Manual Additions" later in this Chapter for more details of this step.

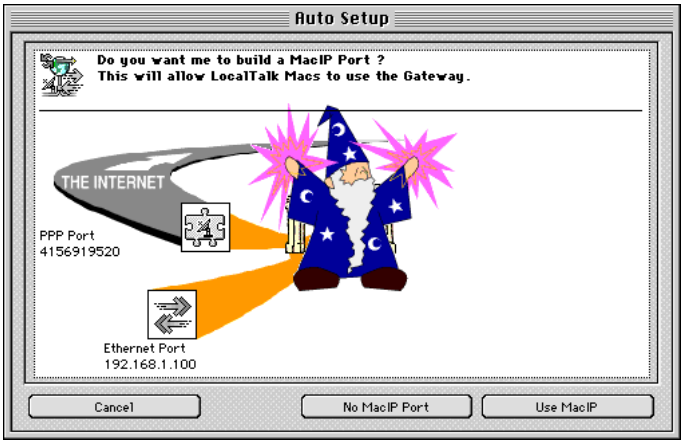
Step 2 - Building an Ethernet Port

Next Darko will try to build an Ethernet port for your local clients. If he finds an Ethernet interface in your computer Darko will assign it a network address. A built-in Ethernet interface will be used if found. Otherwise the first plug-in adapter will be configured.

Step 3 - Building a MacIP Port

Darko will then ask you whether you wish to build a MacIP port.

MacIP allows TCP/IP packets to be carried over an AppleTalk network to reach the Gateway. It can be used if you have clients who are attached to the Gateway using LocalTalk cabling, or for users connecting via Apple Remote Access or through one or more routers which only support AppleTalk.



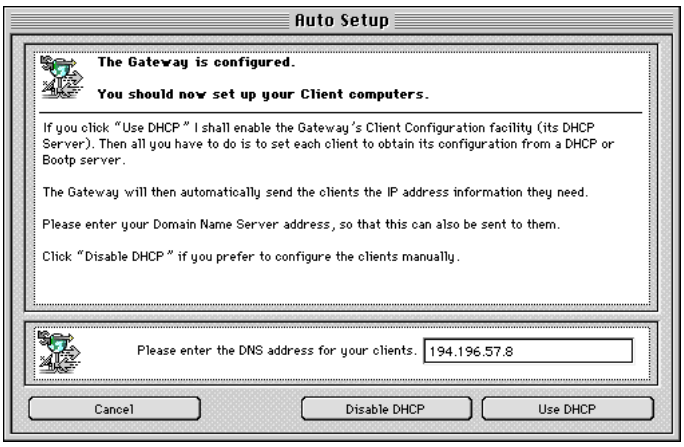
If you have clients who wish to connect to the Gateway using an AppleTalk network, select 'Use MacIP'. If this is not the case select 'No MacIP Port'. A MacIP port uses memory and slows down some Gateway functions, so do not set one up if you don't need it.

Step 4 - Enabling DHCP

The Gateway includes a function called DHCP (Dynamic Host Configuration Protocol) that can send TCP/IP configuration information automatically to the clients on an Ethernet network. This saves having to configure them manually, but the Gateway needs to know what Domain Name Server address to send them.

To use the DHCP function, type the DNS address into the field provided, and select 'Use DHCP'. You should have received the DNS address information from your Internet Service Provider.

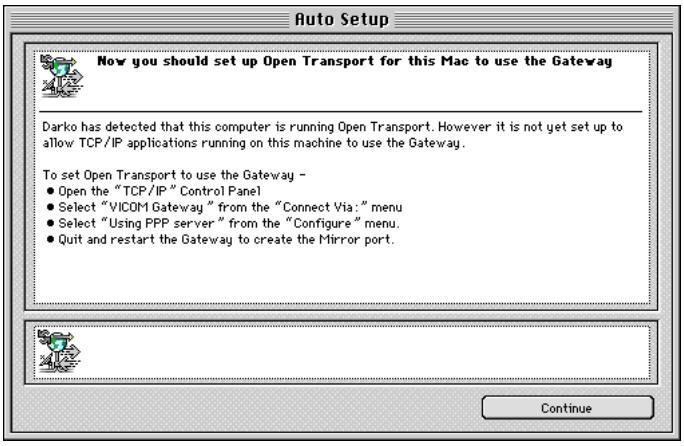
It is strongly recommended that you use DHCP to simplify network address administrayion. However, if you prefer to set up your client machines manually then select "Disable DHCP". You should only select this option if you operate an existing DHCP server in your network, or if the clients are already configured with IP addresses.



Step 5 - Mirroring MacTCP & Open Transport

Next, Darko will build a Mirror port, to enable TCP/IP applications to be used on the Gateway machine. If you are using MacTCP on this machine, this will be done automatically and all you have to do to enable this feature is to restart your machine, which Darko will inform you about.

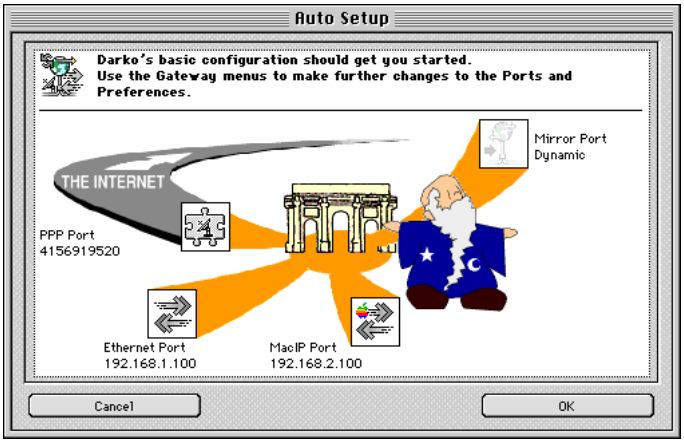
However if you are using Open Transport you will need to change its configuration by using the TCP/IP control panel. The changes are described in the following screen.



In either case you should ensure that the correct DNS address is configured in the Control Panel.

Step 6 Completed Auto-Setup

Darko will now show you the finished configuration.

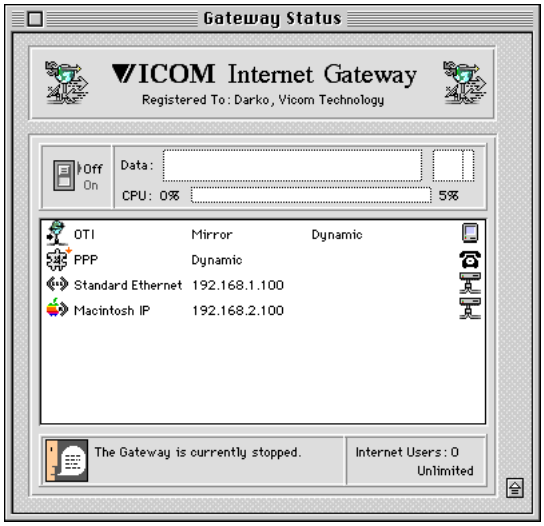


If you click OK, the Gateway Status Window will appear.

If you click Cancel the new configuration will be discarded and the Gateway will revert to its previous state. If this is the first time the Gateway has run then the Status Window will appear, but the Port List will be empty.

You can repeat the Auto-Setup process at any time when the Gateway is operational by selecting "Auto Configure" in the Edit pull-down menu.

The Gateway Status window should look something like this:



The window lists a number of Ports. The first is the Mirror Port which allows applications running on the Gateway Macintosh to use TCP/IP services. The second is the Internet dial-up Port, if it was built. The rest are one or more local network Ports for your Client machines.

Manual Additions

If your Internet connection uses the Apple Modem Tool to control a modem or an external ISDN adapter, then the configuration should now be ready to use. In this case you can skip the next paragraphs and move straight to "Checking your Gateway Setup" on Page 26.

However, you may want to use a method other than the Apple Modem Tool to connect to the Internet. Other connection options include Ethernet, provided by a cable modem or your Service Provider's router, or a plug-in ISDN card with its own Comms Toolbox driver.

In these cases you should manually create and edit an appropriate Port.. The necessary steps are summarized below. Full details of the manual Port configuration options are provided in Chapter 6, "Customizing the Gateway".

For an Ethernet connection:

- If you are using a plug-in Ethernet card for the Internet connection, install the hardware and software, following the manufacturer's instructions.
- Select "New Port" in the "Gateway" pull-down menu to open the Edit Port Settings window.
- Check the Static Address check box and type in the IP address that your Internet Service Provider has given you.
- In the "Method" pop-up menu, select the Ethernet adaptor that you will use to connect to the Internet.
- In the "Type" pop-up menu, select "Internet Proxy - Directly Attached".
- Click "OK" to close the Edit Port Settings window and to save this Port configuration.
- Select "Preferences" in the Edit pull-down menu, and select "Routing" in the Preferences window pop-up menu. Type the IP address of the Service Provider's Internet router in the "Default Gateway" field.
- Close the Preferences window.

For an ISDN plug-in card:

- Install the card and its Comms Toolbox software, following the manufacturer's instructions.
- Select "New Port" in the "Gateway" pull-down menu to open the Edit Port Settings window.
- If your Internet Service Provider has given you a Static IP address, check the "Static Address" box and type in the IP address that your Internet Service Provider has given you.
- Select "PPP" in the "Method" pop-up menu, .
- Select "Internet Proxy - Dial Out" in the "Type" pop-up menu.
- Click on the "Tool Setup" button on the right of the window to open the Comms Toolbox setup window.
- Select the approriate Method in the pop-up menu at the top of this window, which will then change to display the protocol configuration options for your card.
- For a Sagem Planet ISDN card, select "Planet PPP" as the protocol. For other cards select "HDLC". Other settings should be generally in accordance with the guidance provided with your card and the software.
- Close the Comms Toolbox window and then click "OK" to close the Edit Port Settings window and to save this Port configuration.

Checking your Gateway Setup

To test the configuration it is suggested that you now try to connect to the Internet from the Gateway machine.

If your connection to the Internet is via an Ethernet Port you should now be able to access it using a Web browser on the Gateway machine.

If your connection is via a dial-up modem or ISDN Port, use the following procedure to test it:

- Make sure that the modem or terminal adapter is correctly connected to the Gateway Macintosh and to the phone socket, and is switched on.
- Turn the Gateway on by clicking the On / Off switch or by selecting "Start Gateway" in the Gateway menu.
- Select the 'PPP' port by clicking on it once.
- Choose the 'Connect' option from the Gateway menu.
- If all is well the modem will dial and in due course you will see the 'Connected' message appear in the status window.
- If your connection fails, check that the correct entries have been made for your modem or ISDN adapter, telephone number, and login details. Refer to "Tracing Ports" in Chapter 13, Troubleshooting, for help in finding the problem.
- If you discover an incorrect entry you can run the Auto-Setup sequence again by selecting "Auto Configure" in the Edit menu. Alternatively, refer to Chapter 6, Customization, for instructions on making manual modifications.
- Once you have connected to the Internet, launch a Web browser on the Gateway Macintosh, such as Netscape Navigator, Microsoft Internet Explorer or CyberDog, and try to display a Web page. If this fails you may have entered an incorrect DNS address. See "Pinging Hosts" in Chapter 13, Troubleshooting, for help in finding the problem.
- Disconnect from the Internet using the "Disconnect" menu option, and then automatically reconnect by trying to display a new WWW page.
- The final step is to configure the Client computers to use the Gateway, and check that they can also cause it to reconnect and display WWW pages. This procedure is summarised below, with more details in the next Chapter.

Please note that your Gateway license may restrict the number of client computers that can connect to the Internet through the Gateway at any time.

Configuring your Client computers

Each Client computer on your local network should be set up to use the Gateway to connect to the Internet. The simplest way to set up your clients is to enable the DHCP Server function of the Gateway. Then the clients can all be set to obtain their address details from the Server. PCs, UNIX systems and Macintoshes have different set up systems, but all offer a way to use a DHCP or BOOTP server.

Example instructions for the most common Client operating systems are provided in detail in Chapter 3, "Setting Up Gateway Clients".

You may also wish to support dial-in clients. The Gateway can operate as a remote access server, supporting SLIP or PPP connections from other Gateways. To do this you need a separate dial-in Port with a modem or ISDN terminal adapter, and you need to configure the remote clients to connect using their remote access PPP or SLIP software.

For details of how to set up a dial-in facility for clients, see Chapter 4, "Setting Up Remote Access Services".

If your clients are already configured for an existing IP address scheme you must edit the Ethernet Port address on the Gateway to conform with this address range instead.

- Obtain a spare address from the network administrator, or use the one already assigned to the Gateway Macintosh.
- Open the Edit Port Settings window for the Ethernet Port and enter this address in the Edit window.
- Then change the client TCP/IP configurations so that they have this address as a router entry. Appendix A provides guidance on manual client configuration.

Using the VICOM Internet Gateway

Congratulations. You have completed the Installation and Setup of a TCP/IP router, and you can now use your Gateway to save you cost and time as you share your Internet connection.

The default Gateway configuration should meet your basic operating requirements. However, you may wish to adjust or correct these settings. Chapter 6 describes how to customize the Preferences and the Port configurations to your specific needs.

Configuration information is stored in a file called “Vicom TCP Gateway Prefs” in the “Preferences Folder” in the System Folder. You may wish to copy this file using the Macintosh Finder facilities, to provide a backup or to maintain alternative configurations.

The File menu item "Save Config As..." saves the current setup as a Text file which can be viewed or printed using SimpleText or any other text processing application. This can provide a record of your configuration, and may be requested by Vicom Technology if you seek technical assistance.

Later Chapters of this Guide describe how to configure the Advanced Gateway features to support Inbound Mapping to servers, complex routing, and the DHCP facilities.

3 Setting Up Local Gateway Clients

About this Chapter

The Client computers must be set up so that they can use the Gateway when they need to connect to the Internet. This Chapter describes how to do this for a number of common Client systems.

Chapter 4 describes how to set up the Gateway and clients for remote dial-in access to your network.

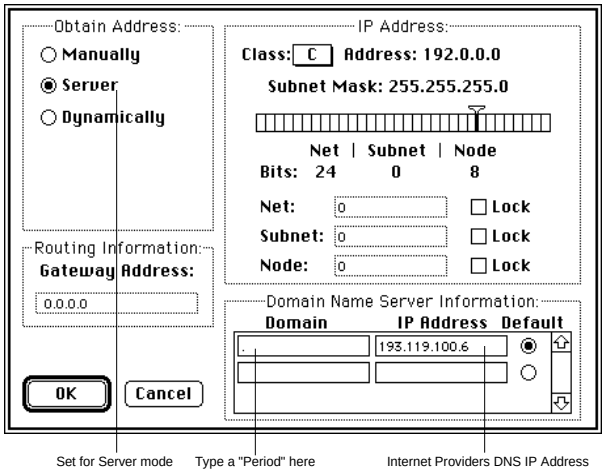
For local clients, these instructions assume that Dynamic Host Configuration Protocol (DHCP) is enabled in the Gateway. DHCP is described in detail in Chapter 11 of this Guide. You may have enabled it during the Auto Setup process, or you can do so at any later stage by selecting "Gateway Preferences" in the Edit pull-down menu, and "Routing" in the pop-up menu.

You should only choose to disable DHCP if your Gateway Macintosh is connected to a network that already has an assigned TCP/IP address range. In this case your Clients should already have been configured, but you will need to change their default router addresses to that of the Gateway's LAN Port on their network segment.

For your convenience, manual client configuration guidelines for some common desktop clients are provided in Appendix A. You are also recommended to refer to the documentation that is provided with your client systems for more complete details.

Setting up MacTCP Clients

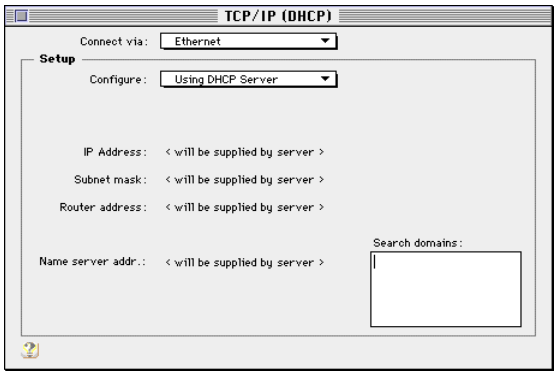
1. Open the MacTCP control panel.
2. Configure the network connection for Ethernet or LocalTalk according to your cabling.
3. Click the More… button, and click the “Server” button under “Obtain Address”.
4. For LocalTalk cabling, enter the DNS IP address supplied by your Internet Service Provider.



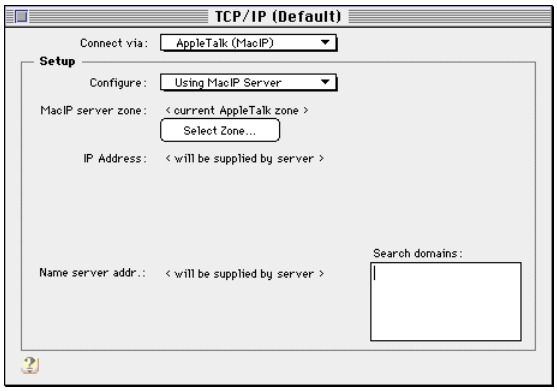
5 Close the MacTCP control panel and restart the Macintosh.

Setting up Open Transport Clients

1. Open the TCP/IP control panel on each client running Open Transport.
2. For Ethernet cabling, select "Connect via: Ethernet" and "Configure: Using DHCP Server" in the pop-up menus.



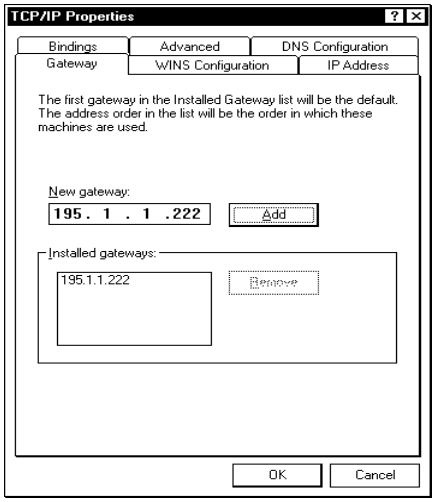
3. For LocalTalk cabling, select "Connect via: AppleTalk (MacIP)"and "Configure: Using MacIP Server" in the pop-up menus.



5. Close the TCP/IP control panel.

Setting up Windows 95 Clients

1. Open the Network control panel.
2. Highlight TCP/IP and click the "Properties" button.



3. Select the "IP Address" Tab and click "Obtain an IP address Automatically".
4. Close the Network control panel.

Setting up Windows 3.x Clients

TCP/IP setup procedures vary according to the software installed. The following is a typical example, based on Netmanage NEWT:

1. Start up the "Custom" application that is installed with NEWT.
2. Select "Configuration" in the Setup Menu and check the box for "Use Dynamic Configuration"
3. Check the box for "DHCP"
4. Close the Custom application

4 Setting Up Remote Access Services

About this Chapter

The Gateway can be set up to permit remote systems to dial in using ISDN or a modem. In this mode, it acts as a PPP Server, or Remote Access Server. This capability can be used on a Gateway that is also providing the other Internet Gateway services.

The PPP Server function can be used to support individual remote users wishing to dial into your TCP/IP network via PPP client software, or it can create a wide area intranetwork.

If a remote Gateway dials into the PPP Server then the two networks can be linked together as a Wide Area Intranet. The Gateways then route traffic via the serial line to allow users at each site to access TCP/IP facilities at the other site. A high speed link such as ISDN is recommended for inter-connecting a wide area Intranet.

This Chapter describes how to configure the Gateway for use as a PPP Server, and gives examples of remote Client configurations for typical desktop machines.

Setting up Dial-In ports

In order to use the Vicom Internet Gateway as a PPP server you need to create one or more new ports to answer incoming calls.

A single dial-in Port can be provided using one of the serial interfaces on the Gateway Macintosh. If all the built-in serial interfaces are in use, or more dial-in ports are required to support simultaneous remote Clients, you can add more by plugging in a multi-port serial card. Cards are available from various manufacturers, including Keyspan, Creative Solutions and Megawolf.

The Gateway can support up to eight Ports of all types. If you are using a Mirror Port, an Internet Proxy Port and a local Ethernet Port then there are up to five available for use as dial-in Ports.

To configure each dial-in Port, open a New Port window using the Gateway pull-down menuand set it up as follows:

Port Name: You may want to give the Port a name such as "Remote Access", to appear in the Port List in the Status Window.

Static Address: check "Static address" for the dial-in Port. An address in the range of 192.168.x.x is recommended by Inter-NIC for private networks. See Chapter 8, Routing, for more information on network addresses.

Method: set to "PPP". SLIP can also be used, but PPP is now the most common protocol for remote access.

Type: choose an Answer option:

- "Dial up - Answer only" sets the port to accept incoming calls.
- "Dial up - Answer and Dial" also enables the Port to initiate outgoing calls.

Dial In Security: There are four options for checking incoming caller identity:

- Open Port (No security): any client can dial in without authentication.
- Users and Groups (PAP): uses Password Authentication Protocol to authenticate the clients' username and password. This is normally the fastest authentication method.
- Users and Groups (Minimal Prompts): uses a login script; prompts are "login:" and "password:".
- Users and Groups (Full Prompts): displays a logon banner with the Gateway name and version before prompting for "login" and "password". The Gateway name can be set in the "General" Preferences.

Timeout: A timeout value may be defined to disconnect inactive connections.

Tool Setup: click to select and configure the appropriate Comms Toolbox tool. For more details,see Chapter 6, "Customizing the Gateway".

Host Access Rights: use these settings to restrict local or remote access through this Port for specific IP addresses. See Chapter 12 for more details.

Dial-in Client Access

Once connected, remote access Clients can access all of the same network facilities as local Clients. These include:

- local network servers
- servers on the Gateway's Mirror Port
- the Internet, via an Internet Proxy Port. This may be on the PPP Server, or on another Gateway.

Dial-In Client Security

The Vicom Internet Gateway provides dial-in password security.

The remote user's name and password are sent to the Gateway by the Client and authenticated by the Gateway during each connection attempt. The Gateway can be configured to require Password Authentication Protocol (PAP) or a Unix-style login to obtain this information.

To use PAP, Dial-In clients enter their username and password into the "Authentication" field of their PPP dialer. To use a Unix login the user or the PPP dialler responds to user name and password prompts.

Each remote Client has an account defined by a User Name, and a Password. Gateway Client accounts are created and modified using the Macintosh "Users and Groups" facilities

To set up a new remote user:

1. Open the Users and Groups control panel.
2. Go to the "File" pull-down menu and select "New User".
3. Type in the account username.
4. Double-click on the user icon.
5. Type in the account password.
6. Drag the user icon to the "VIP Gateway Group" group icon.

To add an existing user to the Gateway's Group:

1. Open the Users an Groups control panel.
2. Drag the user icon to the "VIP Gateway Group" group icon.

NOTE: If the Gateway is running on the same Macintosh as an AppleShare Server, see pages 57 and 64 for additional information.

Setting Up Remote Access Clients

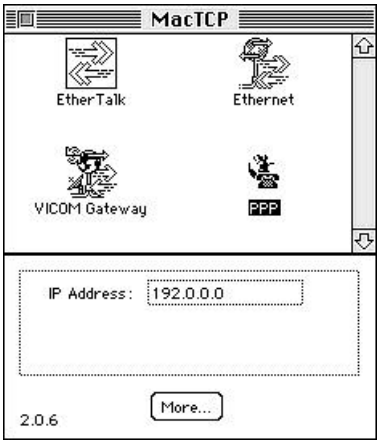
The Client Remote Access service is set up with a combination of a TCP/IP stack and a PPP dialer. The following examples include details on how to set up clients for three common configurations: MacPPP/FreePPP, Open Transport-PPP, and Windows 95 Dial-Up Networking

MacPPP/FreePPP

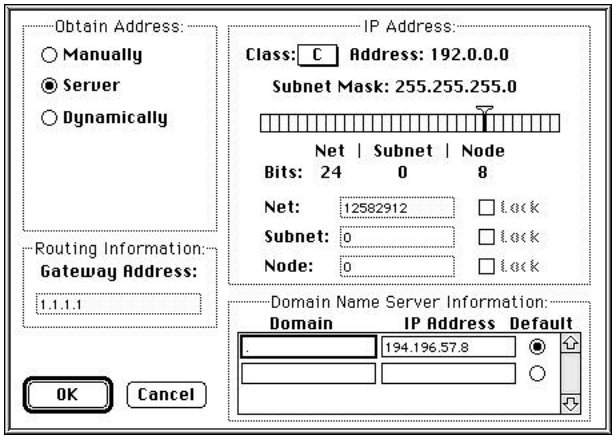
MacPPP configuration consists of setting up the FreePPP or ConfigPPP control panel to dial the PPP connection, and setting up the TCP/IP stack to allow an Internet connection. The TCP/IP stack may be Open Transport or MacTCP.

Setting up MacTCP

1. Open the MacTCP control panel.



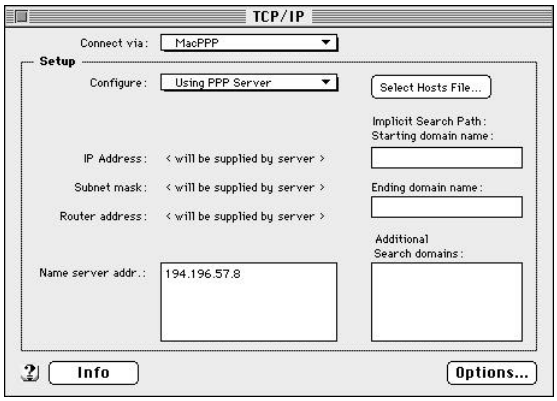
2. Select the "PPP" icon.
3. Click the More... button, and click the "Server" button under "Obtain Address".



4. Enter the DNS IP address supplied by your Internet Service Provider.

Setting up Open Transport

1. Open the TCP/IP control panel.
2. Configure the network connection for "PPP".
3. Select "Using PPP Server" in the configuration pop-up menu.
4. Enter the DNS IP address supplied by your Internet Service Provider.

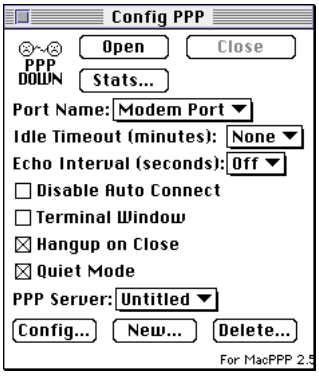


Setting up MacPPP or FreePPP

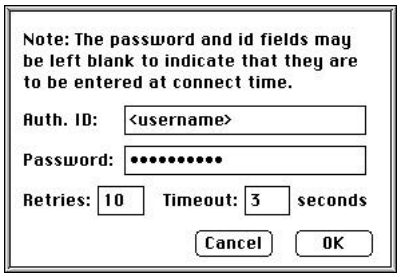
Early versions of FreePPP use the same ConfigPPP control panel as MacPPP. Later versions have their own FreePPP Setup application which can be accessed from a FreePPP pull-down menu.

To set up MacPPP or FreePPP using ConfigPPP:

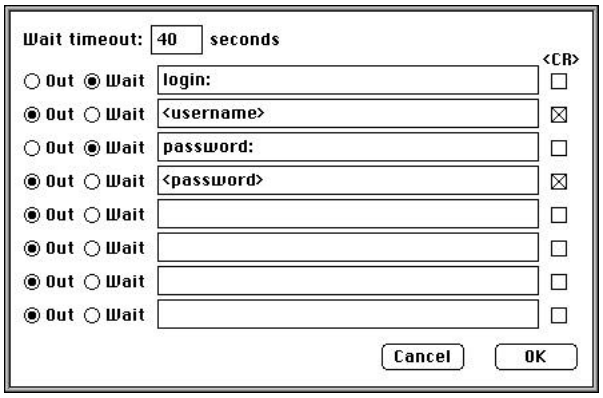
1. Open the ConfigPPP control panel.



2. Click on the New... button and name the service "Remote Access".
3. Set the port speed and the handshake to their appropriate settings.
4. Set the phone number to that of the Vicom Gateway's dial-up line. and the "modem init" field to the string recommended by your hardware manufacturer.
6. If your Gateway has the "Users and Groups (PAP)"option set up click on the Authentication... field and fill in your username and password.

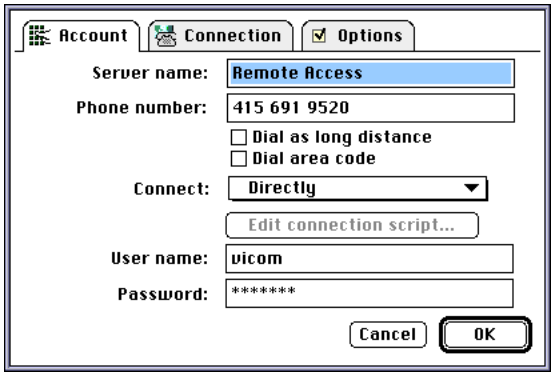


7. If the Gateway uses either "Users and Groups (Full Prompts)" or "Users and Groups (Minimal Prompts)" options then set up your login script.



To set up FreePPP using the FreePPP Setup application:

1. Open FreePPP Setup from the FreePPP pull-down menu. If necessary, ensure that the full window is displayed by clicking the down arrow.
2. Select the "Accounts" tab and click "New" to display this window:



3. Set the Account name and phone number to dial.
4. If the VIG security is set up for "Users and Groups (PAP) then enter your user name and password in this window. Otherwise, select "Using Connection Script" and click "Edit connection script" to enter the prompts and responses.
5. Click the "Connection"tab and set up the port speed, handshake and "modem init" field for your modem.

Open the dialler and click on the "Open" button to test the configuration.

Open Transport PPP

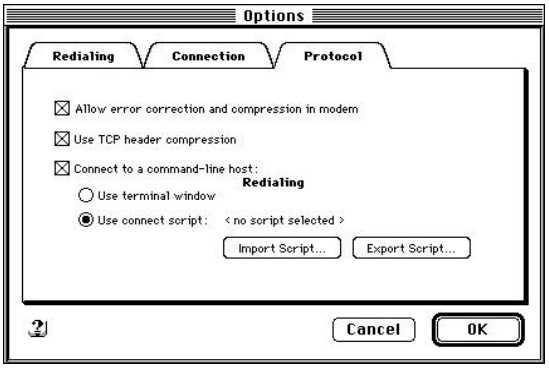
The Open Transport PPP configuration consists of setting up the Modem, PPP, and the TCP/IP control panels.

Setting up Modem

1. Open up the Modem control panel.
2. Select the appropriate serial port and modem settings.

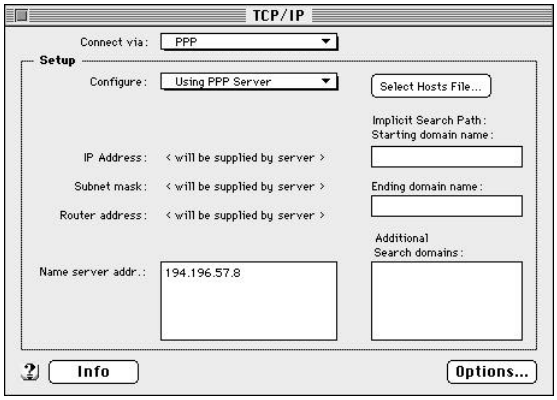
Setting up PPP

1. Open the PPP control panel.
2. Enter the phone number of the Vicom Gateway's dial-up line.
3. If the Gateway security is set to "Users and Groups (PAP)", enter your username and password in the connection settings.
4. Otherwise, click the "option" button and highlight the "Protocol" button. Enable the check-box "Use Connect Script:" and click the button "Import Script" to import a login script.



Setting up TCP/IP

1. Open the TCP/IP control panel.
2. Configure the network connection for "PPP".
3. Select "Using PPP Server" in the configuration pop-up menu.
4. Enter the DNS IP address supplied by your Internet Service Provider.



Once the Modem, PPP, and TCP/IP control panels are set up open the PPP control panel and click on the "Connect" button.

Windows 95 Dial-Up Networking

The Windows 95 operating system has built-in dial-up networking that allows you to establish a PPP connection. The configuration consists of setting up a Dial-Up Networking connection and the Network control panel.

Dial-Up Networking

1. From the Windows 95 desktop click on My Computer | Dial-Up Networking | Make New Connection.
2. Change My Connection to "VIG Dial-Up" and select the appropriate driver for your modem.
3. Click "Next" and enter the correct phone number for the Vicom Gateway's dial-up line.
4. Click "Next" and click "Finish".

Network

1. Open the Network control panel and click "Add".
2. Click "Adapter".
3. Click "Add", select "Microsoft" in the left window, and "Dial-Up Adapter" in the right window.
4. Click "OK".
5. Click "Add", select "Microsoft" in the left window, and "TCP/IP" in the right window.
6. Click "OK".
7. Close the Network control panel.

Dialing Out

1. Double-click on the "VIG Dial-Up" DUN icon.
2. If your Gateway has the "Users and Groups (PAP)"option set up click on fill in your user name and password. Scripted login requires additional software.

Once the Dial Up Network and Network protocols are setup, double-click on your Dial Up Network connection and click on "Connect".

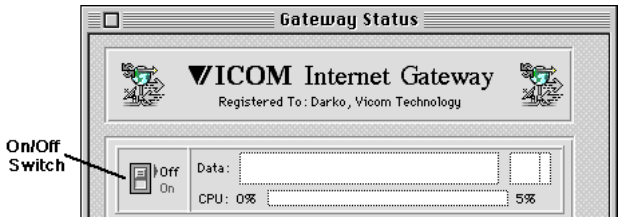
5 Operating the Gateway

About this Chapter

This Chapter describes the facilities for monitoring and controlling the Gateway in normal operation. These include the Menus, and the controls and status displays presented in the Windows.

Starting and Stopping the Gateway

The Gateway is started and stopped by clicking the “On/Off” button in the Gateway Status window, or by choosing “Start Gateway” or “Stop Gateway” from the “Gateway” menu.



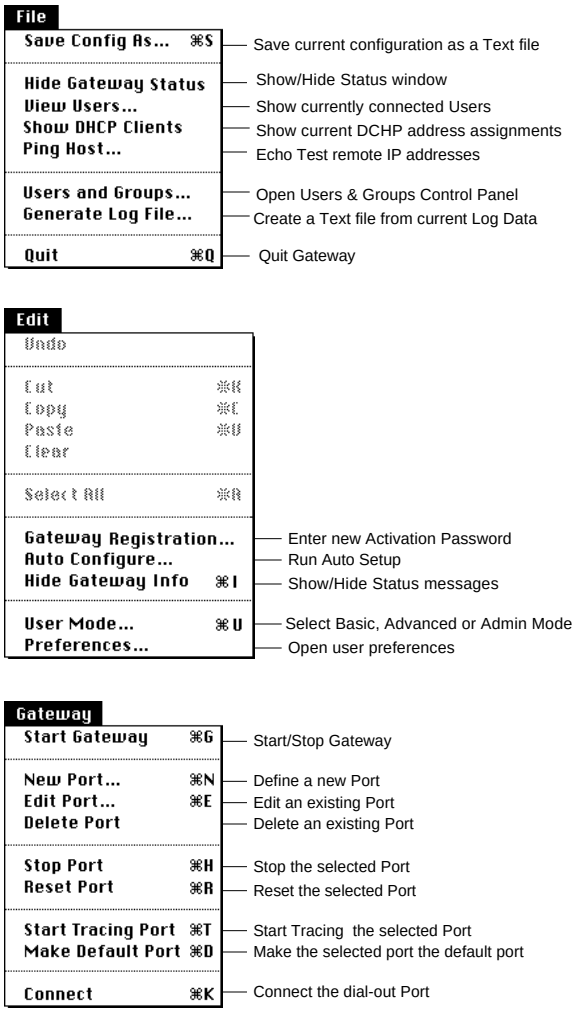
The Gateway's Preferences can be set so that it starts automatically as soon as it is launched. The Gateway can be launched when the machine is switched on by putting an alias of the Gateway in “Startup Items” in the System Folder. If you need to ensure that it starts before other Startup Items, for example mail or web server software, you can rename the Gateway alias to put it first alphabetically.

All ports are reset when the Gateway is started. Directly attached ports will be automatically connected. Open Link and dial-up ports will connect at the appropriate time according to their settings. These ports can also be connected manually.

All ports are disconnected when the Gateway is stopped. This may take some time depending on the connection methods in use. For example, a modem might take up to a minute to hang up.

The Gateway Menus

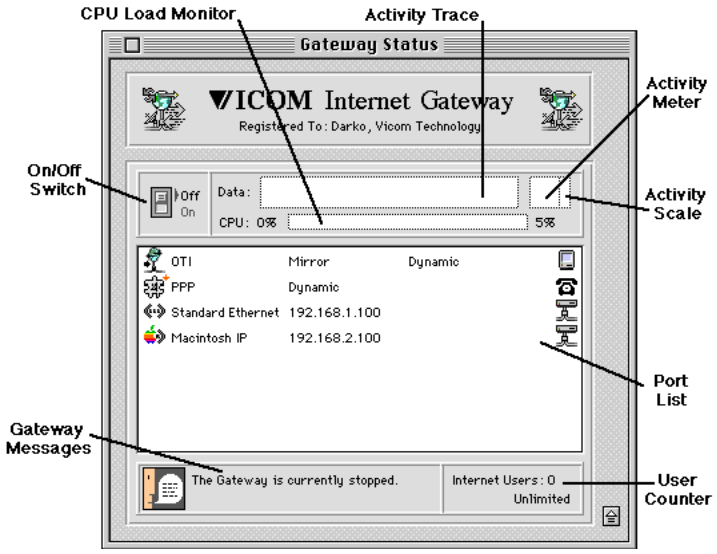
The Gateway's facilities are accessed through its menus. The menus in Basic user mode are shown below.



Additional menu items can be accessed in Advanced User mode. These items are listed in Chapter 7, Advanced Gateway Operations, and explained in the subsequent Chapters.

The Gateway Status Window

The Gateway Status window shows the current activity of the Gateway and the status of all the ports. The window looks like this:



Items in the status window have the following functions:

On/Off Switch: Turns the Gateway on or off.

Activity Trace: Displays packet throughput.

Activity Scale: Shows the activity trace scale.

Activity Meter: Shows the number of packets processed by the Gateway in the previous second.

CPU Load Monitor: The percentage of available processor time used by the Gateway.

Port List: The type, IP address and status of each Gateway port.

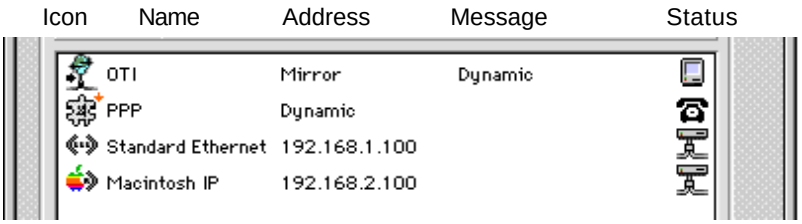
User Counter: The number if current users, and the licensed limit.

Gateway Messages: The current operating state of the Gateway.

The Port List display

The Gateway Status window has two views: a standard view and a condensed view which does not display the port list. The condensed view is activated by clicking on the up arrow symbol in the bottom right corner of the standard view. The standard view is activated by clicking on the down arrow in the bottom right hand corner of the condensed view.

The Port List displays the following information:



If there is a problem with a port, an exclamation mark is displayed next to its icon. A dot is displayed to the lower right of the icon for the Internet Port.

The Port Name is either a default name corresponding to its connection method, or a name you set in the Edit Port Settings Window (Chapter 6).

The IP address of each port is displayed. If the port is set for dynamic addressing and it is not connected, the word “Dynamic” is displayed instead.

The port message indicates connection status, such as “Connected” or “Not connected”. If the port has been disabled for any reason, an error message is displayed here. If the port is connected and port counts are enabled they are shown.

Port status displays an icon showing the current status of the port:

Dial Up port:

Indicates that the port is ready to dial out or receive a call. If this is a dial-out port, and auto-connect is set, the port will attempt to make the connection whenever a packet is routed through this port. If the port is set to dial-in, then the port will answer on incoming calls.

Indicates that a remote user is dialing into this port and that the Gateway is answering the call.

Indicates that the dial up port has connected successfully and is able to transmit and receive packets. It may be disconnected by selecting stop port, reset port or by stopping the Gateway.

Open Link port:

Indicates that the port is not connected. If auto-connect is set, then the port will attempt to make the connection whenever a packet is routed through this port. The port may also become connected if the hardware or driver software are set up to connect automatically.

Indicates that the port is connected and able to send and receive packets. The port will be disconnected if 'Stop port' or 'Reset port' is selected, or if the Gateway is switched off. The port may also be disconnected if the hardware or OS software detects an error.

Directly Attached port:

Indicates that the port is active. Directly attached ports are always connected unless they are disabled, or the Gateway is switched off.

Disabled or Stopped port:

Indicates that the port has been disabled or stopped. If an exclamation mark is shown to the right of the port icon, the port has been disabled by the Gateway and will need to be reset before it will become active again. If there is no exclamation mark the port has been stopped by the user. The port message will indicate why the port was disabled or stopped.

Managing Ports

All Port management functions, except “New Port”, are accessed by selecting a port in the Gateway Status Window and choosing the appropriate command from the “Gateway” menu.

New port: Creates a new port and opens the Port Settings window.

Edit port: Opens the Port Settings window for the selected port.
Short cut - double click the Port in the Status Window.

Delete port: Deletes the selected port.

Stop port: The Gateway disconnects the selected port.
No further traffic will be sent to this port until it is started or reset.

Start port: Starts a stopped port, but does not attempt to open a connection for Open Link and Dial-out ports.

Reset port: Clears the “disabled” status on the port, and then stops and starts the port.

Start tracing: Opens the trace window for this port. This window shows all traffic through the port and is used to diagnose network problems. The trace window should not be left open during normal operation, as it will slow down the Gateway considerably.

Mirror this Port:

Makes the selected port the Mirror port. This is the Port whose address will be used, or "Mirrored" by MacTCP or Open Transport on the Gateway machine.

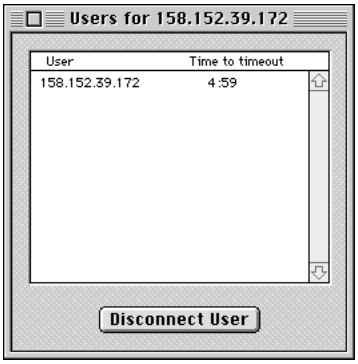
Make default port:

Makes the selected port the default port.
Chapter 8, IP Addressing and Routing, gives more details of the way the Gateway makes its routing decisions.

Connect: Attempts to open the connection for the select port. Changes to "**Disconnect**" when the Port is connected.
This command is usually not necessary as Open Link and Dial-out ports default to connect automatically when necessary.

Managing Local Users

You can list the active users and disconnect them if necessary. Select the Internet port by highlighting it in the Gateway Status Window, select 'View Users' in the File menu and if there are any active users using that port they will be listed in a table like the one below.



The list shows each user's address, and the time remaining before the user's proxy session times out. This value remains at or near the time-out period set in the Internet Proxy Preference until traffic from the user ceases.

To disconnect a user, select the user by highlighting the entry in the table and then click the 'Disconnect User' button. The user will be disconnected from that port until their next attempt to re-connect.

If you assign fixed addresses to users, the numeric addresses can be replaced by names to make the list easier to read. To do this, place a text file called "Gateway Names" in the Gateway's home folder with each user's name and IP address on a separate line. Separate the name and address fields by one or more TAB characters, and do not include spaces or TAB characters in the name.

6 Customizing the Gateway

About this Chapter

This Chapter describes how to change the following default Gateway settings:

Gateway Preferences

- Activity sounds
- Routing and addressing protocols
- Start up the Gateway automatically on launch
- Activity meter settings
- Mirror port settings
- Secure AppleShare interaction
- Logging options
- User time-out
- Name Server information

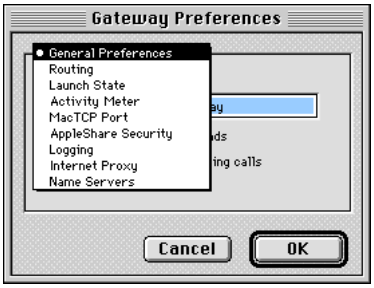
Port Configurations

- Edit the Internet Port settings
- Edit the local network Port settings

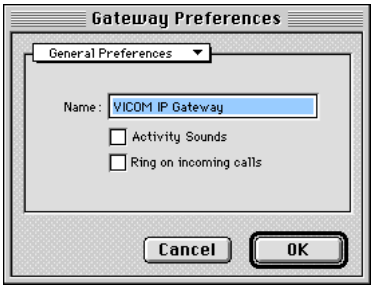
Setting Gateway Preferences

This Chapter describes the facilities for changing the Gateway preferences. The Gateway Preferences window is opened by choosing **Preferences** from the "Edit" pull-down menu.

The Gateway Preferences window provides settings for several parts of the Gateway, accessible through the pull-down menu at the top of the window.



General Preferences

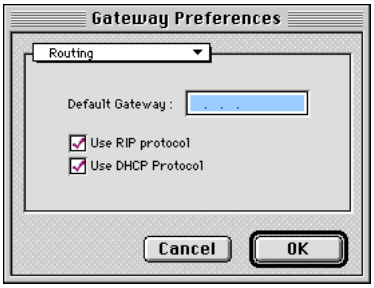


Name: Assign a name to the Gateway. If "Security (Full Prompts)" is used, this name will be displayed in the Login banner when a remote user dials into the Gateway.

Activity Sounds: The Gateway makes sounds during certain activities (such as starting or stopping the Gateway). Unchecking this option disables these sounds.

Ring on incoming calls: If this option is checked the Gateway will make a "telephone ringing" sound when an incoming call is received.

Routing

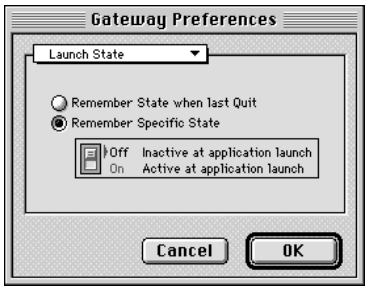


Default Gateway: sets the default gateway. This is the address the Gateway will send packets to when it knows no explicit route to the destination address. If you are connected to the Internet via a router then enter its IP address here.

Use RIP Protocol: When 'checked' the Routing Information Protocol (RIP) is utilized. This allows the Gateway to exchange routing table information with other directly connected TCP/IP routers.

Use DHCP Protocol: When 'checked' DHCP is activated. See Chapter 3, Setting up Gateway Clients for more details.

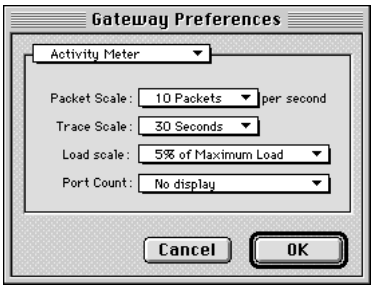
Launch State



Remember State When Last Quit: when selected, the Gateway remembers whether it was on and off and starts in the same state the next time it is launched.

Remember Specific State: when selected, the user can explicitly set the Gateway launch state with the On/Off switch.

Activity Meter



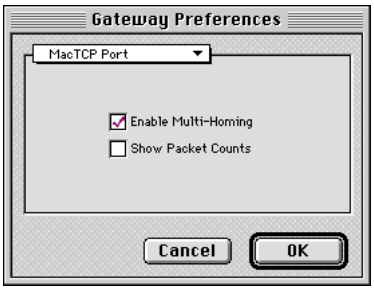
Packet Scale: The packets per second scale changes automatically if throughput increases, but it will not change back to a lower scale than selected here.

Trace Scale: choose from three trace time scales.

Load Scale: the load scale shows how much processor time is consumed by the Gateway .

Port Count: ports can be set to display the number of routed packets, the packets per second, or no traffic information in the Gateway Status Window.

Mirror Port



Enable Multi-Homing: when selected, the Gateway will use several IP addresses for MacTCP / Open Transport clients on this machine. More details on the use of Multi-homing are given in Chapter 10, The Mirror Port.

Show Packet Counts: when selected, the Gateway Status Window's Port List will show the number of packets sent and received through the Mirror Port. If not selected, the Port List will show the address of the mirrored Port.

AppleShare Security

Admin Password: If dial-in security is being used, and the Gateway computer is also running an AppleShare server, enter your AppleShare Admin password here so that the Gateway can access the "Users & Groups" file. Use the Administration program supplied with AppleShare to define and edit Users in the VIP Gateway Users Group.

Chapter 4 provides more details on how to set up and manage remote access for dial-in users.

Logging

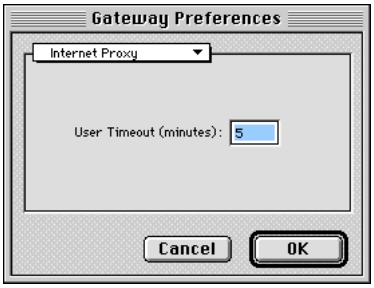
Enable logging: When 'checked' the Gateway will record user events and traffic activity to a binary log file. This file can be processed manually, or automatically each day, to generate a text file listing the information collected.

Start a new log every day: When 'checked' the Gateway will generate a text log file each day, and clear the binary file.

The Gateway logs the following details to the output file:

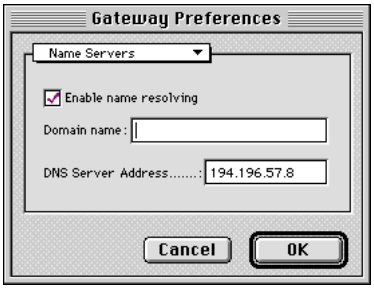
- A header giving the date range for the log.
- A log of Port connection and disconnection events indicating the Instigator, time and duration for each.
- A traffic analysis by Host address, showing the total volume of traffic in bytes, broken down for principal applications, and the total durations for the data transfer activities.

Internet Proxy



User Time-out: The Gateway allows multiple users to connect simultaneously to the Internet, up to the limit of the license purchased. The user time-out defines the idle time after which a user's proxy connection will be closed. This allows new users to connect when previous users have finished their Internet sessions. The number of current users is shown in the Gateway Status window, along with the maximum licensed value. Select 'View Users' in the File menu to see a list of the currently connected users and their remaining times.

Name Servers



Enable name resolving: When 'checked' name resolving will be carried-out on all remote and local addresses when the log is generated. This converts logged IP numbers to host names where possible.

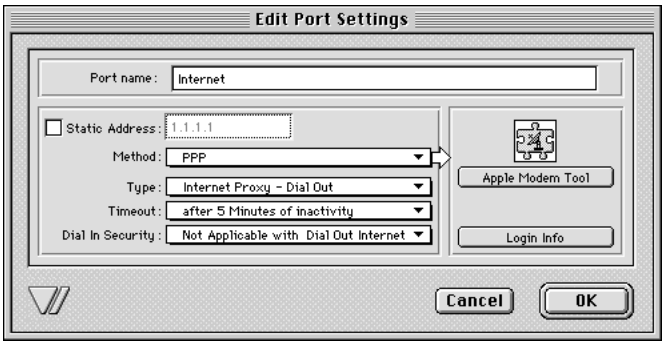
Domain name: Enter your own 'Domain name' here if you wish this information to be sent to Gateway clients by the DHCP Server.

DNS Server Address: Input your Domain Name Server address. This information is given to clients if you are using DHCP. It may be the DNS address supplied by your Internet Service Provider, or a local DNS on your internal network.

Configuring Ports

The Gateway needs a port for each connected network, both directly attached and dial-up. Ports can be created or edited at any time. However, if you edit an existing Port while it is connected, and then enter the changes, the Port will disconnect if it uses a dial connection, and all sessions using the Port will be reset.

You cannot edit or view the Mirror Port configuration. You can manually Edit any other Port by double-clicking it in the Gateway Status Window, or by highlighting it and selecting "Edit Port" in the "Gateway" pull-down menu. The Port Settings window will appear:



This Window has an expanded set of facilities in the Advanced User Mode. These additional items are described in Chapter 7. The following paragraphs describe the controls in the Basic User Mode window.

Port Name: If you type a name into this field it will replace the default name in the Ports List in the Gateway Status Window.

Static address: Each directly connected local area network Port must have a fixed, or Static, address. The Gateway presets each to a Private Network address during Auto Setup. These addresses are reserved by InterNIC, the committee which administers Internet addresses, so that there will be no conflict with public addresses.

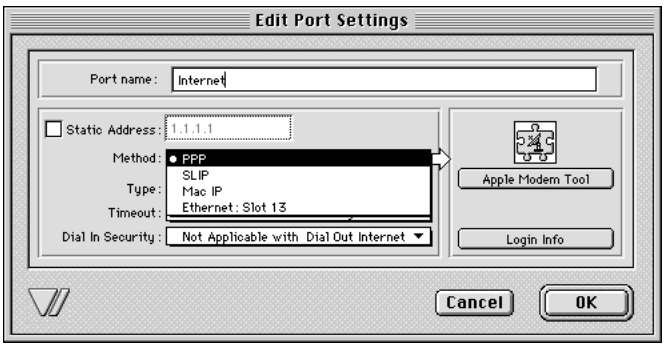
You only need to change the assigned address of a Port if it is connected to an existing local TCP/IP network with a different address range, for example if the Port is connected to the Internet or your private network already has an address structure.

A dial-up Internet Port may have a fixed or dynamic address depending on your Internet Service Provider.

To use a static address, check the box and enter the address in the text field in "xxx.xxx.xxx.xxx" format.

To use a dynamic address, uncheck the box. The Gateway will disable the text field and put “1.1.1.1” in it to indicate that the port has not yet acquired its dynamic address.

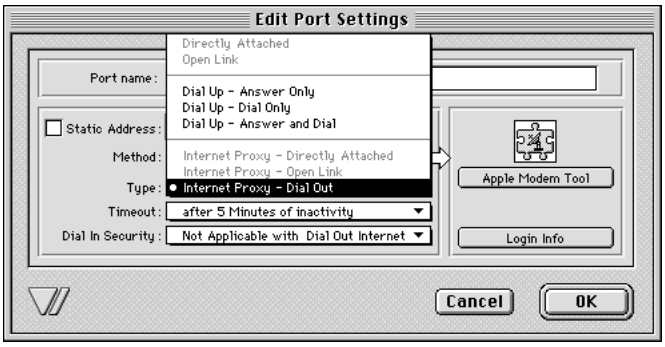
Method: This pop-up menu shows the connection methods and includes a list of all installed interfaces. Only the network interfaces supported by the Gateway can be selected.



The following methods can be selected for Gateway Ports:

- PPP or SLIP: these methods support dial up connection to the Internet, or provide remote dial-in access to the Gateway.
- Mac IP: this method sends TCP/IP packets within AppleTalk packets. It is normally used to connect Macintosh Clients using LocalTalk cabling or Apple Remote Access.
- Ethernet: this method is used to connect Client computers using Ethernet cabling. Each Ethernet interface appears as a separate menu item.
- Token Ring: this method is available if a supported Token Ring adapter is installed. There will be a separate menu item for each Token Ring adapter.
- Other installed PPP drivers, such as supported ISDN adapter software, may also appear in this menu.

Type: this pop-up menu tells the Gateway whether the port is on a directly-attached or remote network, and if Internet proxying should be enabled. The following types are available:



- Directly Attached: the port is on a directly attached network, such as an Ethernet or Token Ring LAN.
- Open Link: this is used when the Gateway is not required to dial the connection, for example with 3rd party ISDN PPP dialers, and leased lines.
- Dial up - Answer only: sets the port to accept incoming calls; used for gateway to gateway and dial-in PPP or SLIP.
- Dial up - Dial only: used for gateway to gateway wide area routing connections.

- Dial up - Answer and Dial: sets the port to accept incoming calls and to dial out when necessary; this is used for gateway to gateway connections and dial-in PPP or SLIP.
- Internet Proxy - Directly Attached: the same as Directly Attached but performs Internet proxying.
- Internet Proxy - Open Link: the same as Open Link but performs Internet Proxying.
- Internet Proxy - Dial Out: the same as Dial up - Dial only performs Internet Proxying.

Time-out: this determines if the Gateway will disconnect if there is no traffic through the port for the specified time.

Dial In Security: this defines the prompts sent to dial-in clients to request their user name and password.

Security works through the Macintosh “Users & Groups” mechanism. Users can be created, viewed and edited using the Users and Groups Control Panel. This can be accessed through the Apple Menu Control Panels item, or using the File menu "Users and Groups" item.

The Gateway creates a group called “VIP Gateway Group”. For authentication, dial-in users must be created as members of this Group. and each user should have a name and password which will be validated during dial-in. There are four levels of security:

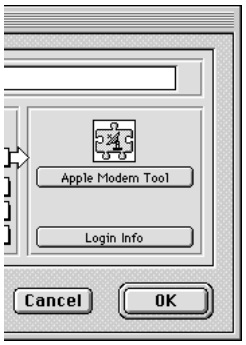
- Open Port (No security): any client can dial-in without authentication.
- Users and Groups (PAP): uses PAP (Password Authentication Protocol) to obtain the client's user ID and password. Clients should set their PPP software to use PAP.
- Users and Groups (Minimal Prompts): the Gateway sends "login:" and "password:" prompts, and validates the responses.
- Users and Groups (Full Prompts): this displays the login banner before sending the "login:" and "password:" prompts. The banner provides a Welcome message including the Gateway Name, if this is set in the General Preferences, and its version number.

Notes For AppleShare Users.

If the Gateway is running on the same Mac as an AppleShare Server, the Administration Password for the AppleShare Server must be entered in the Gateway Preferences so that the Gateway can access its list of Users. In this case the File Menu item "Users and Groups" will not open the Control Panel, and the AppleShare Administration system must be used to edit Gateway Users.

Serial Port Settings Buttons

On the right hand side of the Edit Port Settings window are three buttons which are active if a SLIP or PPP connection method is selected.



Each button opens a window where further information can be entered to define the Port behavior. These buttons are described in more detail in the next sections.

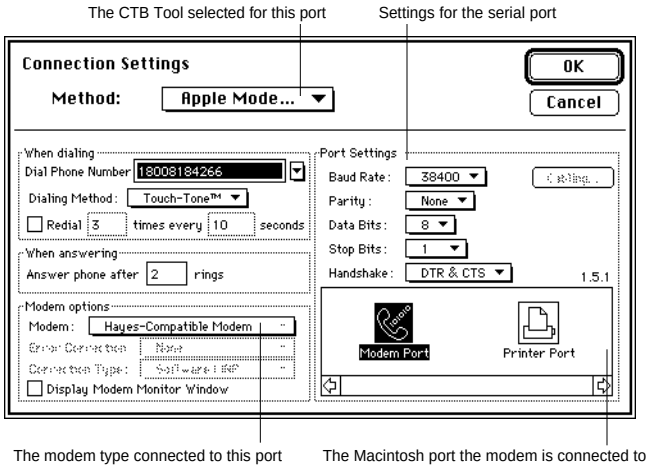
Tool Setup: Click this button to open the Comms Toolbox tool settings window for an Internet Port.

Login Info: Click this button to edit the PPP or SLIP login information.

Tool Setup

This is used to select and configure the Comms Toolbox tool for the Internet port. If a tool is already selected, the name of the button will be set to the name of the tool; if no tool is selected the name of the button will be “Tool Setup”.

When this button is clicked the standard Comms Toolbox “Connection Settings” window is displayed. This example shows the settings for the Apple Modem Tool. The window will be different for other Comms Toolbox tools.



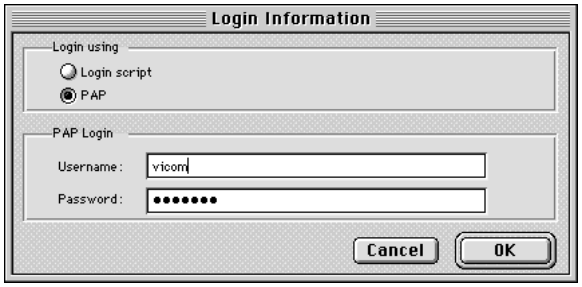
When using a Comms Toolbox connection tool we recommend that the tool’s own re-dialing is turned off so that the Gateway can retry if a login attempt fails.

Hardware handshaking, also known as full flow control, is essential for speeds above 9,600 bps. If you use the Apple Modem Tool then set the Handshake option to “DTR & CTS”, as shown in the example above.

Manufacturers of plug-in ISDN cards and internal modems often supply a special Comms Toolbox driver for their hardware. Once installed, this can be selected in the "Method:" pop-up menu at the top of the Connection Settings window, when the window will change to support the options for this hardware.

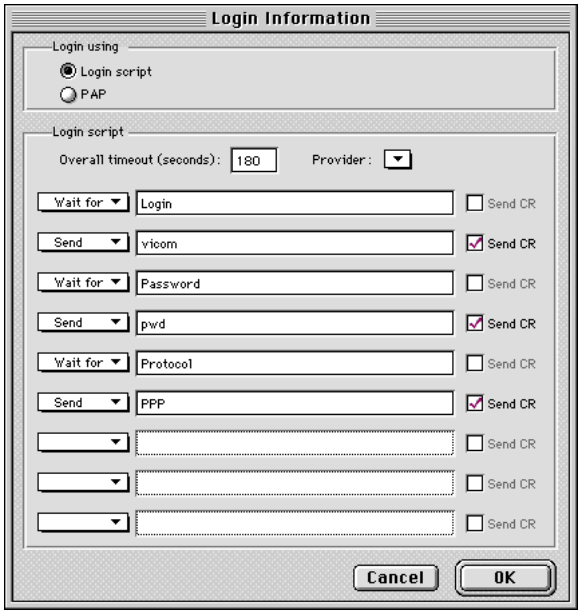
Login Info

The Login Information window allows you to set up the details required to log in to your account at your Service Provider. To open this window, click on the **Login Info** button in the Port Settings window:



If your service provider uses PAP (Password Authentication Protocol) for login, then enter the User name and Password in this window and click OK.

If your service provider uses a Unix-style script for login, then click the "Login Script" radio button to open the Script area of the window.



The Login Information script defines a sequence of host prompts to *wait for* and responses to *send* for each prompt. You can also enter a number of seconds to *delay* between script actions.

Most scripted hosts will prompt for a user name and password, but some Providers may require other prompts, delays or responses before a TCP/IP connection is established. In the above example there are three prompts shown with corresponding responses.

To create a script, type each prompt and response on a separate line in the table. The pop-up menu to the left of each line allows you to define whether the text is a prompt to *wait for*, a response to *send*, or a *delay* in seconds before the next script action. The checkbox at the right of each *send* line indicates whether a Return (CR) character is to be sent after the response.

The table defaults each line function to the reverse of the previous one, and adds a (CR) to each response line. So most scripts can be entered simply by typing each text entry and moving down the table using the TAB key.

The other controls in this window are:

Overall Time-out: this is the maximum time in seconds that a single connection attempt may take before the Gateway aborts the process. The Gateway will try to connect once more, and then will stop until triggered again by a client.

Provider: this pop-up menu presets the prompts sent by several Internet access providers and gateways including the VICOM Internet Gateway. If one of these matches your Service Provider's script then select it to fill in the prompts, and then type in the responses, such as your account name and password.

Click OK to complete the Login Information for the port.

Note: The Login Info window allows you to set up either PAP or scripted access, but not both. If your Internet connection requires a combination of scripted access followed by PAP login, then the Advanced User Mode can be used to set this up. Refer to Chapter 7 for details.

7 Advanced User Mode

About this Chapter

The first Chapters of this Guide have provided details of the Gateway's Basic User Mode facilities, its default User Mode. This Chapter explains the purpose of the Advanced and Administration Modes. The subsequent Chapters then describe the Advanced User Mode facilities and explain how they can be used.

About User Modes

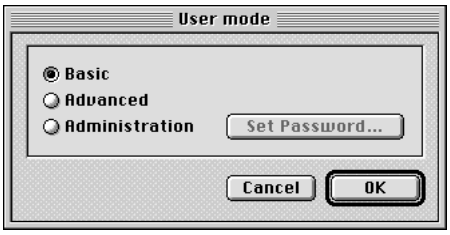
The Gateway can be operated in one of three User Modes:

Basic: this Mode provides the menus and controls you need to configure the Gateway for dial-up Internet access, and to support local and dial-in users.

Advanced: this Mode provides additional set-up facilities for routing, access and firewall control, and DHCP management. These features are accessed through additional items in the "Gateway" pull-down menu, and through extra controls in the Edit Port Settings window.

Administration: this Mode provides access to the same features as Advanced Mode, and adds Password protection to prevent inadvertent or unauthorized modification of the Gateway configuration. When an Administration Password is set any attempt to open a Settings window or the Preferences is intercepted with a password challenge.

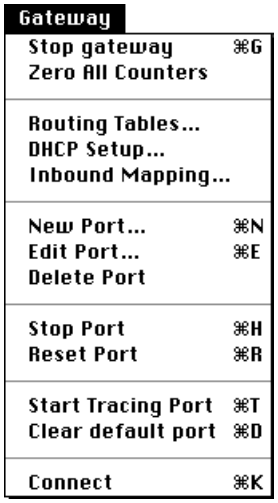
The User Mode can be set by selecting the "User Mode" item in the Edit pop-up menu and clicking the required radio button.



Administration Mode only becomes active if an Administration Password has been entered. Click the "Set Password" button to open the Administration Password window. Type your Password into each of the two fields to activate password protection.

The Advanced Menus

In Advanced User Mode the "Gateway" pull-down menu is extended as shown below.

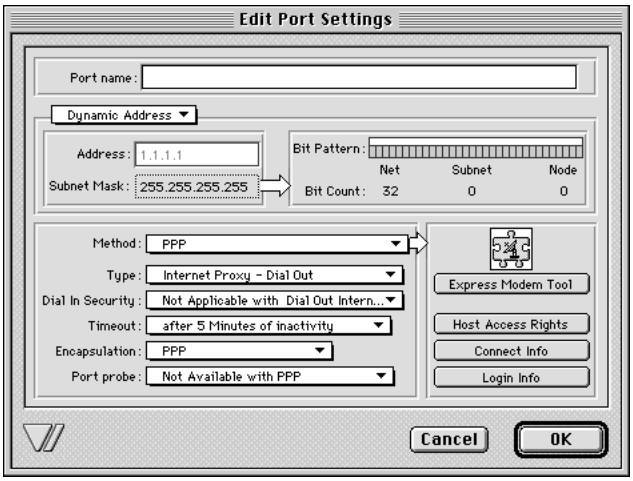


The additional menu items are described in detail in the next Chapters of this Guide, as listed:

- **Routing Tables** see Chapter 8
- **Inbound Mapping** see Chapters 9 and 10
- **DHCP Settings** see Chapter 11
- **Global Host Access Rights** see Chapter 12

Advanced Edit Port Settings Options

In Advanced User Mode the Edit Port Settings Window provides some additional facilities.



The additional controls are:

Address Type: use the pop-up menu to select Class A, B, C or dynamic IP addressing for the Port. See Chapter 8 on Routing for more information.

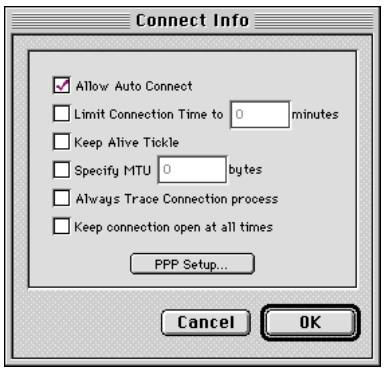
Subnet Mask: a slider control allows you to set the subnet mask for each Port. See Chapter 8 for more information about subnets and routing.

Encapsulation: this item shows the protocol used to transport IP packets for the selected Method.

Port Probe: you can set the Gateway to check Ethernet and Token Ring ports regularly. If one fails this check, the Gateway will stop it. You should then investigate for a network problem before resetting the Port to restart it.

Host Access Rights: click this button to open a window where you can set constraints on which local client addresses can access the Gateway or trigger connections through the Port, and which host addresses can be reached through it. See Chapter 12 for further details.

ConnectInfo: this button opens a window where you can control the detailed attributes of the Internet Port.



The additional facilities in this window are:

Allow Auto Connect: when this is set, the Gateway will automatically try to connect whenever a packet needs to be sent through this port. If it is not set, the only way to establish a connection is to select the port and choose **Connect** from the "Gateway" menu.

Limit Connection Time: this specifies the maximum time the port can remain connected. The Gateway will close the connection after this time expires, even if there is traffic through the port.

Keep Alive Tickle: some Internet Service Providers automatically close the connection if it is idle for a specified time. Set this option to prevent this. The Gateway will then send a "dummy" packet every 30 seconds to prevent the remote end from timing out when there is no real traffic.

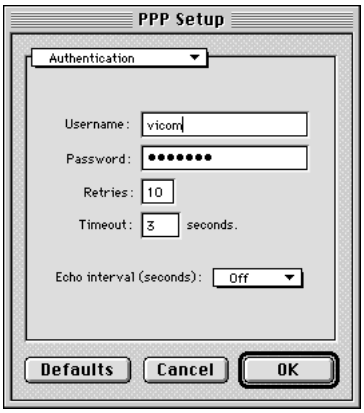
Specify MTU: the default Maximum Transfer Unit (MTU) for the PPP Port is set to 1500 bytes. It is then negotiated with the Service Provider's equipment during connection, so it is very unlikely that you would need to change it here.

Always Trace Connection Process: when activated, the Gateway will display the Trace window while connecting. The window will close once a connection has been established. This is useful for tracking down login problems. Chapter 13 gives details of the Trace window.

Keep connection open at all times: when activated, the Gateway will hold the PPP connection open continuously and attempt to reconnect it if it disconnects for any reason.

PPP Settings: this button opens a further window for setting detailed PPP and PAP protocol options. It opens at the Authentication settings, and the pop-up menu gives access to LCP and IPCP settings.

It is very unlikely that you will find it necessary to make any changes in the LCP or IPCP configurations, as these are negotiated during call establishment.



Normally you should use the Login Information window to set up your PAP or Login Script details for connection to an Internet Service Provider. For ease of use, that window allows you to define either PAP or a script, but not both. If you have used the Login Info window to set up PAP details then they are shown here also.

However, in some situations it may be necessary to use both a script and PAP, for example, if you need to use an X.25 PAD to reach the Service Provider, but the Service Provider then requires PAP for login. In such cases, you should define the script entries in the Login Info window, and enter your User Name and Password in the above Authentication screen.

The retry and time-out settings can be adjusted to achieve successful connections under adverse conditions. The echo interval can be set to send periodic PPP signaling packets to check the link. This may be necessary for a dial-in port. Echo packets are normally initiated by the Internet Service Provider on a dial-up Internet connection

8

IP Addressing and Routing

About this Chapter

This Chapter provides some background on how TCP/IP packets are addressed and routed in the Internet, and describes the way the Gateway makes its routing decisions. It goes on to explain how to configure and monitor the routing information used by the Gateway.

TCP/IP Addressing

Each computer connected to a TCP/IP network has a unique address. The convention is to show the address as four numbers separated with a full stop, for example "192.168.1.100". This address is know as an *IP address*. Each number in the sequence must be between 0 and 255.

The address represents a 32 bit binary number split into four 8 bit octets. It consists of two parts: the *network* number (n) and the *host* number (h). The network number is defined by the first part of the address, 192.168.1 in this example. The host number is the second part.

The first number in the sequence defines the *class* of the network number, which determines how the address is divided into its two parts:

First number range	Network class	Network portion
0	not allowed	
1-126	Class A	n.h.h.h
127	not allowed	
128-191	Class B	n.n.h.h
192-223	Class C	n.n.n.h
224-255	not allowed	

The network number identifies the physical network that the host is connected to. Since the Gateway is connected to several networks, each port must have an IP address with a unique network number.

A Port may have a *Static* or *Dynamic* IP address. A static address is pre-defined and set *before* the computer is connected to the network. A dynamic address is acquired *during* the connection process with the help of a special addressing protocol, and may be different each time it connects.

Network mask

The network mask tells a router how to divide an IP address into its two parts: the network number and the host number. The network mask for any network can be deduced from the Class of the addresses assigned on the network:

Network class	Network mask
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

The network mask is a 32 bit binary number with a **ONE** at each bit in the Network part of the address and a **ZERO** at each Node address bit.

TCP/IP Ports

Since TCP/IP is a multi-session protocol, a computer running TCP/IP might have several connections (sessions) opened at once. In order to distinguish between these sessions, each session is assigned a TCP/IP port number when it opens.

In order to use a TCP/IP service a computer needs to know both the IP address of the host providing the service and the port number the service is located on. Most TCP/IP services use a pre-defined port number referred to as a *well known port*. For example, FTP uses port 21, Telnet uses port 23, SMTP uses 25, and so on.

Subnetting

We've explained than an IP address consists of two parts, the host number and the network number. This notion has been extended by the concept of *subnets*, which are introduced in order to allow organizations to further subdivide their IP networks without computers outside their network (e.g. on the Internet) being aware of it.

Subnetting simply splits a single large address range up into a number of smaller ranges. For example, a Class C network address defines a single network with up to 256 host addresses. By subnetting, this can be structured as, for example, 8 subnets, each with 32 host addresses.

Subnetting divides the host number field into two subfields: a subnet number and a true host number on that subnet. The interconnected LANs within an organization will be given the same network number but a different subnet number. This division will not be visible to routers outside that network.

The division between the subnet part or the host address and the actual host part is specified in local router configurations using a *subnet mask*.

Subnet mask

A subnet mask, taken together with the Network mask, divides an IP address into three parts:

- the network number, defined by binary **ONEs** in both masks
- the subnet number, defined by binary **ONEs** in the subnet mask and binary **ZEROs** in the Network mask
- the host number defined by binary **ZEROs** in both masks.

In the example above, a Class C network was divided up into 8 subnets, each with 32 host addresses. The Network and Subnet masks for this case would be:

Network mask:	255.255.255.0
Subnet mask:	255.255.255.224

A simple rule for calculating the subnet mask for a Class C network is to make the last number in the mask 256 minus the number of addresses per subnet, in this case 256 - 32 = 224.

On simple networks with no subnetting the subnet mask is the same as the network mask. On subnetted networks, local hosts and routers use the extra subnet masked bits to make local routing decisions about which cable a host is on. The public Internet is unaware of these subnet divisions, and simply routes packets to the "boundary" router or routers for the network, based on its Network address only.

The Gateway defaults the subnet mask to be the same as the Network mask, based on the address class of a port. If it is necessary to subnet your internal network, you should select Advanced User Mode, and modify the subnet masks for the affected Gateway Ports in the Edit Port Settings Window. The slider control allows you to position the subnet mask divider at any position in the 32 bit address field. As you adjust it, the window shows the numbers of bits assigned to the Network, Subnet and Host parts of the address.

TCP/IP Routing

Computers communicate over a network using a *network protocol*. The Gateway works only with the IP network protocol. This is the network protocol used on the Internet network, and supports a range of session layer protocols, including TCP and UDP. These, in turn, support the application layer protocols such as HTTP for World Wide Web services, SMTP and POP3 for electronic mail, FTP for file transfer and so on.

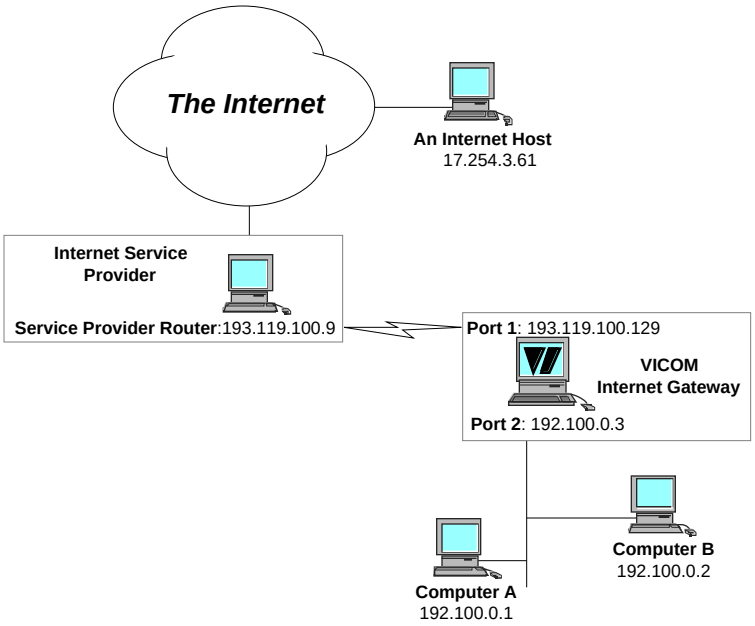
Data is transmitted over a network in a series of *network packets*. A packet contains the IP address of the computer that sent the packet (*source address*) and the address of the computer that is to receive the packet (*destination address*).

The need often arises to connect several computer networks. The Internet is itself a series of joined networks. A router connecting an office LAN to the Internet will have at least two networks: the local network, such as Ethernet, and the Internet network. The purpose of the *router* (also known as a *gateway*) is to transfer packets between these networks.

Two computers on the same IP network communicate with each other directly, and do not involve a router. When they need to communicate with a computer on a different network, they must pass the packets to an appropriate router or gateway.

Computers and routers maintain *routing tables* to help choose the next router for some destination subnets or groups of subnets. To avoid having to remember the appropriate gateway for every possible network number, most computers and routers have a *default gateway*. This is the address of a router to which all packets destined for unknown networks are sent.

Suppose we have a network like this:



Computers A and B are on a class C network with no subnetting, and a network (and subnet) number of 192.100.0. They have host numbers of 1 and 2. They are accessing the Internet through an Internet provider with an address of 193.119.100.9 (class C network, subnet number 193.119.100, host number 9). We also assume that computers A and B have their default gateway set to 192.100.0.3.

Computer A talks to computer B directly since they are on the same subnet (192.100.0). Computer A cannot talk directly to the service provider's host, because they are on a different subnets. In this case it will send the packet to the Gateway, which receives it on port 1. The Gateway will see that the packet's destination subnet number is the same as for port 2 (193.119.100) and will forward the packet to that port.

Responses from the service provider's host are received on port 2. If they are addressed to computer A or B, the router will notice that the packet's destination subnet number is the same as for port 1 (192.100.0) and forward the packet to that port.

Default port

Most destination addresses on the Internet will not have the same subnet number as any Port on the local router, so a router has to be able to forward packets to other routers if it cannot deliver them itself. The Default Gateway mentioned above provides this function if the router is permanently connected to networks with fixed addresses.

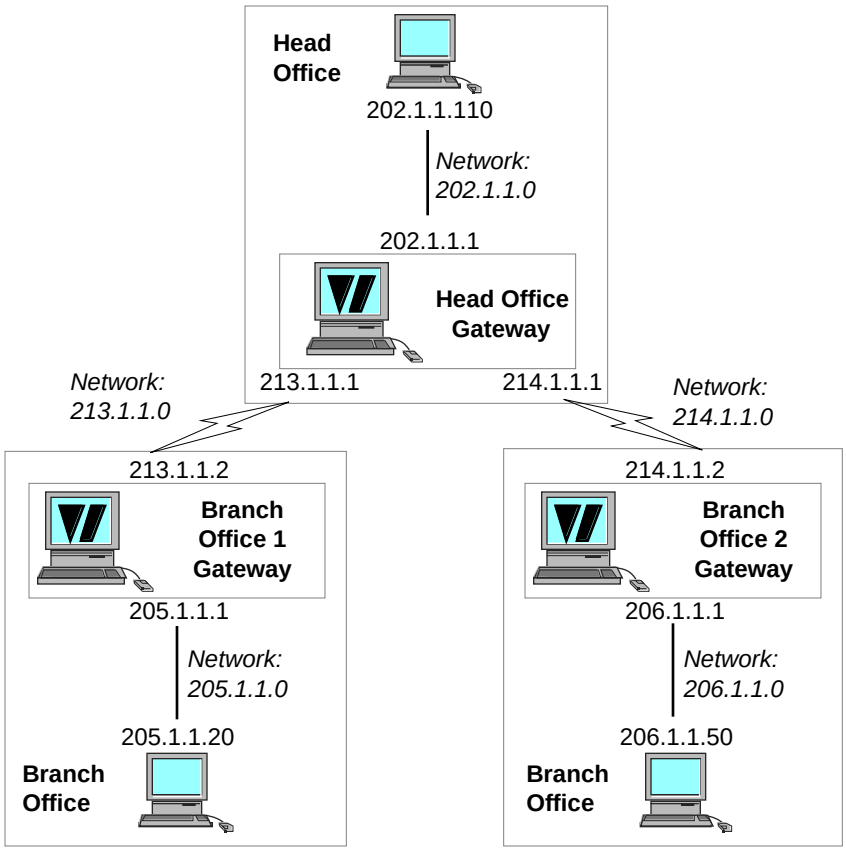
An example of this is illustrated in Figure 1 on the previous page. When computer A wants to talk to Internet host at 17.254.3.61 it finds that the destination has a different network number, and is therefore on a different network, and sends the packet to the Gateway. The Gateway looks for a port with the same network number (17) and fails to find one, so it should send the packet to its Default Gateway, 193.119.100.9.

However, in the case of the VICOM Internet Gateway, it may be disconnected from the Internet when it receives a packet for delivery, and it may not know the router address it will connect to when it dials up the Internet Service.

To solve this, the VICOM Internet Gateway automatically makes the first Internet port the *default port*. All packets with unknown destination network numbers are forwarded to this port. Returning to the example above, network 17 is an unknown network as none of the ports have this network number. The packet for host 17.254.3.61 will therefore be sent through port 2 as it is the default port.

About routing tables

A *routing table* tells a router which path to use to reach a network not attached to it directly. These tables may be necessary when more than one router is used, and a router is connected to more than one network. In this case a default port or default gateway may not provide an effective or efficient solution. Here is an example:



Example 1

This example uses the standard notation of showing the host number as 0 to denote the entire network. For example, “202.1.1.0” represents the class C network with network/subnet number “202.1.1”, while “202.1.1.222” would be a host on that network.

In order for a host on the 202.1.1.0 network to reach a host on the 205.1.1.0 network, the packet must be routed through the head office Gateway and through the branch office 1 Gateway. The 202.1.1.0 host would have its default gateway set to the head office Gateway, so it would send the packet to it. The head office Gateway does not have the 205.1.1.0 subnet attached to it, so it needs to know that 205.1.1.0 network is reached via the branch office 1 Gateway on its 213.1.1.0 network. This could be achieved using default routing, but since we have a similar problem for the 206.1.1.0 network, we need to tell the head office Gateway which specific route to use for each network.

In this example each of the Gateways could have a routing table with two entries:

Gateway	Destination Network	Route
Head Office	205.1.1.0	213.1.1.0
Head Office	206.1.1.0	214.1.1.0
Branch Office 1	202.1.1.0	213.1.1.0
Branch Office 1	206.1.1.0	213.1.1.0
Branch Office 2	202.1.1.0	214.1.1.0
Branch Office 2	205.1.1.0	214.1.1.0

In practice, since both branch office Gateways use only one route, it is possible to mark the 213.1.1.0 and 214.1.1.0 as default ports and the Gateways would then not need a routing table. However, since the head office gateway has two different routes, it must have a routing table. Such a table can be created automatically or manually in the Gateway. The next parts of this Chapter describe these options.

The Gateway Routing Process

The Gateway routes all packets by carrying out the following steps in order. The Gateway executes the next step only if a route has not already been found.

- The Gateway compares the network number of the packet with the network number of each of its ports. The ports are searched in order from top to bottom as they appear in the port list in the “Gateway Status” window. If a port with the same network number is found the packet is forwarded through that port.
- The Gateway searches the routing table for the network the packet is destined for. If the network is found the packet is forwarded to the gateway specified in the routing table. There can be multiple routing table entries for a network and the process by which a route is selected is described in the following Chapter.
- If a default port has been set the Gateway forwards the packet through that port.
- If a default gateway has been set the Gateway forwards the packet to that Gateway.
- If all of the above steps fail the packet is discarded.

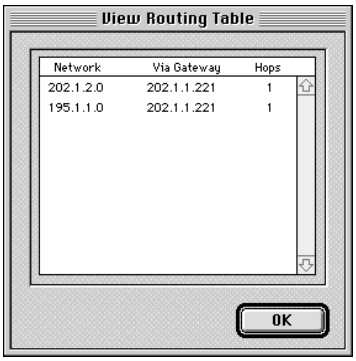
Managing Gateway Routing Information

Routing tables in the VICOM Internet Gateway are only required if the Gateway is running in a network in which it is connected to at least one other IP router. They can be built in two ways.

The simplest way to build routing tables is to set the Gateway to use RIP (Routing Information Protocol) to build and maintain them automatically. This is a standard protocol supported by most routers and used to exchange information about the networks they are connected to.

Manual routing entries can also be set up. If there are manual entries, the Gateway will used these as well as, or instead of, any entries discovered by the RIP process. This may be necessary in a network where other routers do not use RIP.

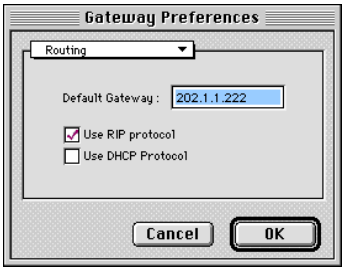
While the Gateway is running, the current routing tables can be viewed by selecting "Routing Tables..." in the Gateway pull-down menu. The routes in use are listed, showing the next router address for each network or subnet in the table, and the Hop Count which is known for that destination network. If the Hop Count is shown as 16 or more, the route has been marked as unusable as a result of RIP communications.



Routing Information Protocol (RIP)

The RIP protocol enables routing tables to be built and maintained automatically using information received from other routing devices. The Gateway can receive and use RIP information, and transmit it to other routers. RIP is needed only if you are operating a Gateway in a multi-router inter-network.

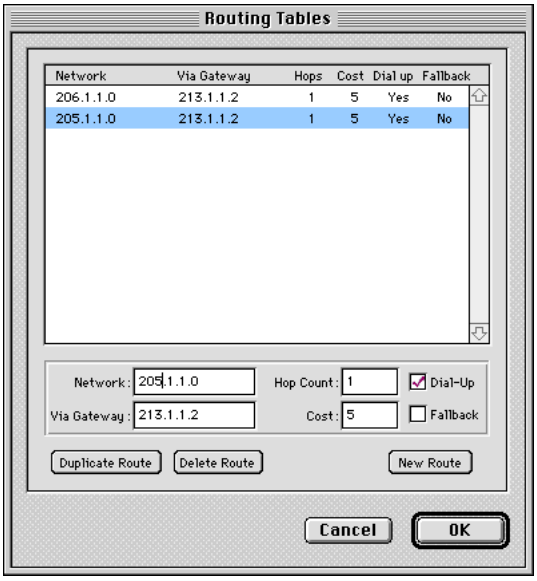
To enable RIP, choose "Gateway Preferences" in the Edit pull-down menu, and select 'Routing' in the pop-up menu in the window. This starts the RIP transmit and receive processes whenever the Gateway is running.



If 'Use RIP protocol' check box is checked, and there are other RIP compliant devices on the network, the Gateway will build a routing table automatically.

Manual Routing Entries

Routing entries can be configured by choosing “Routing Tables…” in the “Gateway” pull-down menu when the Gateway is Stopped. The following window will appear:



Network: the address of the network that is reached via this route. The host number of the address should always be 0.

Via Gateway: the address of the router or gateway to which packets destined for this entry’s network will be forwarded.

Hop Count: the number of gateways the packet of data will travel through to get to the destination network. This figure does not include the Gateway itself.

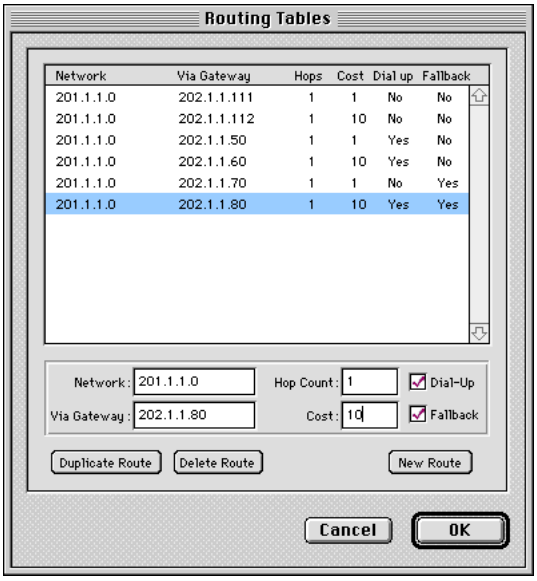
Cost: an arbitrary number between 0 and 65535 which represents the relative cost of using this particular route.

Dial-Up: this checkbox should be set if any portion of the route to the destination network is a dial-up link.

Fallback: this marks the route as a fallback route which will be used only if no other route to the same network is available.

Manual Routing Example

This example shows how the Gateway selects a route to the network 201.1.1.0 using the following manually configured routing table:



Since this Gateway does not have a port with network number 201.1.1 it will search the routing table as described below. The first routing option in the list that succeeds is used and the rest are not executed. The routes in each category are scanned in increasing order of cost.

- Try the direct connection routes (entries 1 and 2).
- Try the dial-up routes (entries 3 and 4).
- Try the direct connection fallback routes (entry 5).
- Try the dial-up fallback routes (entry 6).

If all of the above fails, the Gateway forwards the packet through the default port. If no default port is available, the Gateway forwards the packet to the default gateway. If neither the default port nor the default gateway is available, the packet is discarded.

9 Inbound Mapping and Firewall Protection

The Gateway as a Firewall

A firewall is a router which blocks all or some IP traffic from reaching an IP network. This is particularly important when connecting to the Internet as without this security anybody on the Internet could make use of resources on the local network.

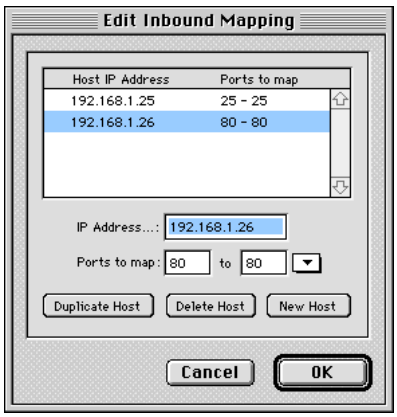
The VICOM Internet Gateway acts automatically as an Internet firewall. This means that computerson a network connected to the Gateway are able to access all other computers on networks attached to the Gateway and vice-versa. However, computers on the Internet cannot access hosts on your local network through an Internet Proxy Port unless the Gateway is configured specifically to permit it. The Inbound Mapping facilities described in this Chapter can be used to permit incoming access through the Firewall

Note that applications running on the Gateway machine itself are always accessible through a connected Internet Proxy Port. They do not have to be Inbound Mapped, and are not on the protected side of the Firewall.

Inbound Mapping

The Inbound Mapping facility is used to permit internal hosts to be accessed through the Firewall at specific TCP or UDP port numbers. Use this to make internal TCP/IP servers accessible to clients connected to the Internet, and to permit UDP-based applications to operate through the Firewall.

Inbound Mapping is set up using the "Inbound Mapping..." item in the Gateway pull-down menu, and is only available in Advanced User Mode.



To enable inbound traffic to reach a specific local host, create an entry by clicking "New Host", and enter the local IP address of the machine to be reached. Then enter the Port number range supported by this host. Typically this may be a Mail or FTP or Web server, and you will enter the well-known Port number for the service. The pop-up menu provides a convenient way to enter the common port numbers.

In the example shown, host IP address 192.168.1.25 has been assigned as an SMTP Mail Server, and 192.168.1.26 is a Web Server. These will now be accessible from the Internet, using the IP address of the Gateway's Internet Proxy Port.

NOTE: Each TCP or UDP port number can only be mapped to a single host address on your internal network. For this reason, where possible, choose the TCP option rather than UDP for client-side services.

Use the Duplicate Host button to add more services for an existing Host, and Delete Host to remove unwanted entries.

10 The Mirror Port

TCP/IP applications on the Gateway machine

It is possible to run a MacTCP or Open Transport applications, such as Netscape or a mail server, on the Gateway machine . However, since the Gateway is handling all IP packets, data sent or received by the application must pass through the Gateway. To do this, the Gateway creates a special port called a Mirror port. MacTCP or Open Transport communicates with the Gateway through this port.

During installation the Gateway places a MacTCP/Open Transport driver file called "-Gateway" in your Extensions folder. When set to use this driver, MacTCP or Open Transport will send and receive all data through the Gateway's Mirror port.

Because MacTCP/Open Transport must always have an IP address, the Gateway sets the port to "mirror" another Gateway port. The Gateway Macintosh then assumes the IP address of that port.

The Gateway will automatically pick the first suitable port to mirror, and marks it with a red dot in the Gateway Status window. However, you can choose an alternative port by highlighting it and choosing "Mirror This Port" from the Gateway menu. Note that you will have to quit and restart any currently running MacTCP/Open Transport applications after doing this.

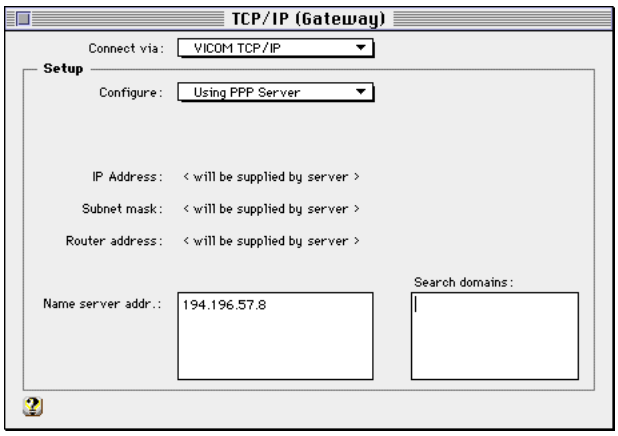
Setting up MacTCP to work with the Gateway

The Auto Setup process automatically sets MacTCP to use the Gateway. However, you can also do it manually as follows:

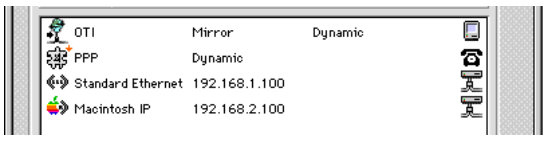
- Open MacTCP Control Panel
- Click on the “VICOM Gateway” icon. The icon will be highlighted.
- If the “VICOM Gateway” icon is not present, ensure that the "Gateway" extension is present in the Extensions Folder in your System Folder and restart the Macintosh.
- Click on “More…”. A new window will open.
- Select “Server” in the “Obtain Address” box.
- Leave the “Gateway Address” box empty.
- Enter the address of a DNS server (usually supplied by your provider) in the “Domain Name Server Information” box.
- Close the window by clicking on “OK”.
- Close the MacTCP Control Panel. Reboot the machine if MacTCP tells you to.

Setting up Open Transport to work with the Gateway

Create an Open Transport mirror port by selecting 'VICOM TCP/IP' in the 'Connect Via' pop-up menu in your TCP/IP control panel. You should also select "Configure: Using PPP Server", and enter a Domain Name Server address in the "Name server addr" box.



Restart your machine and launch the Gateway. An 'OTI Mirror' port should appear in the Gateway Status Window, as shown below.



Using TCP/IP client applications on the Gateway machine

A *client* MacTCP or Open Transport application is any application that uses MacTCP or Open Transport to connect to a server on your local network or across the Internet. For example, a Web browser is a client application that connects to a Web server on a TCP/IP network. Client applications *initiate* connections to *listening* Server applications.

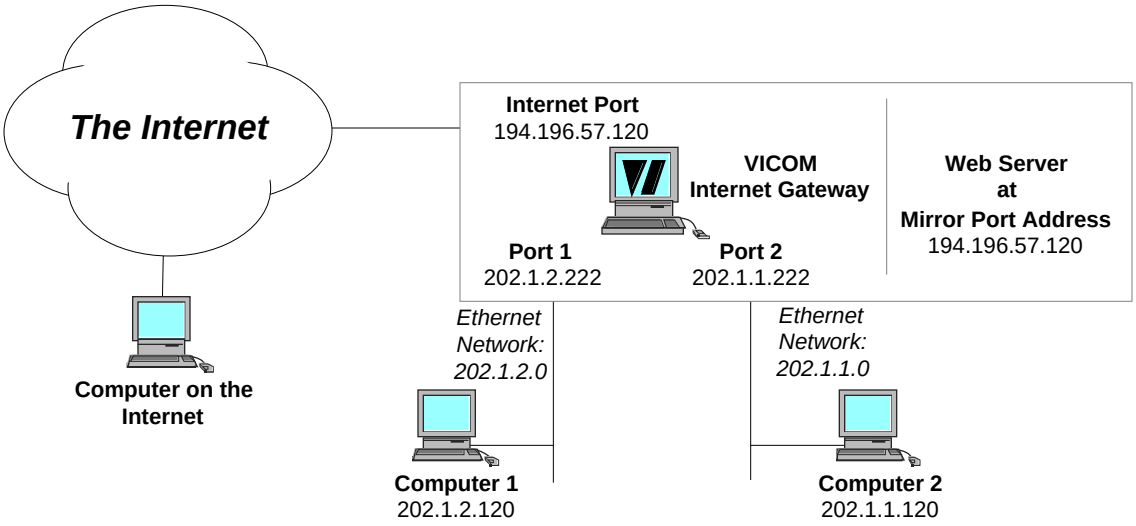
Client applications are used in exactly the same way as on any other client machine. The application will be able to access any TCP/IP network connected to the Gateway.

Since the Gateway has to handle traffic for all machines on the network, the client application may work slower that it would on a stand-alone machine. However, in most cases the slowdown will not be noticeable. A useful guide to see if the machine is overloaded is the "CPU Load" indicator in the "Gateway Status" window. If that indicator is consistently over 20% of CPU load, the machine is probably overloaded.

Using TCP/IP server applications on the Gateway machine

A *server* MacTCP or Open Transport application is any application that makes its services available to other computers connected to the IP network. A prime example is a Web or Mail server. Server applications *listen* for connections, *initiated* by Client applications

Server applications running on the Gateway machine are reachable on the network at the IP address of the Mirror port. Here is an example:



The Gateway machine is running a Web server. The Gateway's Internet port at 194.196.57.120 is set as a Mirror port, so the Web server is accessible from all the computers on all the networks (including the Internet) at address 194.196.57.120.

Please note that this setup poses a potential security risk, as any computer on the Internet will be able to access the Web server running on the Gateway machine. However, server applications running on other Gateway client machines will *not* be accessible.

Multihoming

MacTCP or Open Transport uses the address of the port it is mirroring. TCP/IP applications on the Gateway machine are always accessible at the IP address of the mirrored port.

For some intranets it may be a requirement that server applications on the Gateway machine should be accessible at all the IP addresses of the Gateway's Ports. The Multihoming option provides this facility.

To enable Multihoming, open the Preferences window by selecting "Preferences" in the Edit pull-down menu. Select "MacTCP Port" in the pop-up menu, and check "Enable Multihoming". Close the Preferences window.

11 The DHCP Server

About this Chapter

The VICOM Internet Gateway incorporates a DHCP server to simplify the setup and maintenance of its attached TCP/IP networks.

This Chapter covers the benefits of DHCP, and explains how to set your network up to use it. For users needing more detail, it also explains how the DHCP server operates.

What is a DHCP Server?

DHCP stands for Dynamic Host Configuration Protocol. Using DHCP, client computers do not require individual, manual configuration. Instead, they obtain their IP addresses from the Gateway each time they start up. This reduces the work required to set client machines up, and reduces the likelihood of user errors.

The Gateway's built-in DHCP server provides this configuration service for Open Transport, Windows and Unix clients. It also allows the older BOOTP protocol to be used by, for example, MacTCP clients.

Configuring DHCP

The DHCP server is installed as part of the Gateway software. To activate it you need to set up the DHCP server itself, and set the client machines to use it. These steps were covered in the first part of this user guide as part of the Auto-Setup sequence. Manual DHCP configuration is covered below.

Setting up the DHCP server

1. Select the Edit / Preferences... menu item in the Gateway application.

2. Select Routing in the pop-up menu, and check the "Enable DHCP" box.

3. Select Name Servers in the pop-up menu, and enter the Domain Name Server name and address you wish to be sent to the Clients. This should normally be the Domain Name Server name and address of your Internet Service Provider.

4. The DHCP server is now ready to accept requests from Client machines for IP addresses.

Setting up the DHCP clients

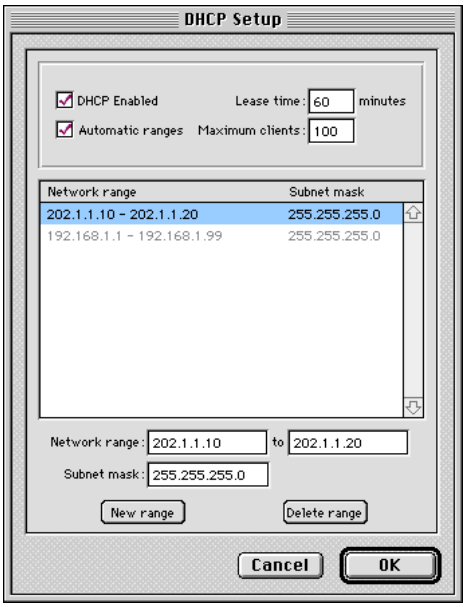
Chapter 3 provides full details on setting up the clients to use the DHCP server.

A note about MacIP clients

Clients connected to a MacIP port can also obtain their IP addresses from the Gateway acting as an address server. However, this is done within the MacIP protocol (also known as "KIP"), and so these MacIP address assignments are not governed by the DHCP methods and settings.

Customizing the DHCP Server

When it starts, the DHCP server operates in its default mode. You can change its settings using the "DHCP Settings" item in the "Gateway" menu to adjust the maximum number of addresses the Server will assign, the ranges of addresses it can distribute, and the lease time for DHCP assignments.



The server can assign up to 100 simultaneous client addresses in its default configuration. This limit can be adjusted up to a maximum of 1024 in the DHCP Settings dialog.

If you increase the number of DHCP addresses to be supported, we recommend that you increase the memory allocation for the Gateway application by 100K Bytes. To do this, quit the Gateway and highlight its icon in the VICOM Internet Gateway folder. Select "Get Info" in the Finder's File menu. Edit the "Preferred size" to increase it by 100.

DHCP clients are issued with addresses on a limited lease, and they can renew at any time during this period. BOOTP clients are assigned addresses indefinitely. The default DHCP lease time of 60 minutes can be modified in the DHCP Settings dialog

When a client needs to start up TCP/IP operations, it broadcasts a request for address information. The DHCP Server assigns a new address and sends it to the client together with the address of its gateway port, the subnet mask for the gateway port, and the domain name server address configured in the Server. This information is acknowledged by the client, and used to set up its configuration.

The DHCP server calculates a default dynamic address range for each configured Gateway port. The default behavior is as follows:

The server assigns addresses in each Port's subnet range starting at host address 1. It assigns increasing host numbers up to a maximum of one less than its own port address. So, by selecting a suitable port address, the subnet address range can be split into static and dynamic ranges automatically.

For most network systems it will be unnecessary to modify the defaults. However, the dynamic address ranges can also be edited and augmented by the user. In Advanced user mode, the Gateway menu item "DHCP Setup…" opens a list of the current address ranges.

The "New Range" and "Delete Range" buttons can be used to change them. Served address ranges need not be constrained to the directly connected networks if suitable BOOTP relay agents exist in the routing system

DHCP Clients File

An empty text file called "DHCP Clients" is put in the Gateway's home folder by the Installer. You can use TeachText or other text editors to edit this file to define fixed address assignments for specific machines. This is useful in the case of Servers which must have the same address at all times. You can also use it to assign a user or machine name to each client, making it easier to monitor which clients are active, and to trouble-shoot client problems.

The file format is:

<Media Access Control ("MAC") Address> <TAB> <IP Address> <TAB> <Name>

For example:

08:00:54:b0:fd:36	0.0.0.0	My_dynamic_Mac
08:12:07:be:5f:72	192.168.1.120	Web_Server_fixed
03:11:0c:3e:ea:9c	192.168.1.121	Fixed_admin_PC

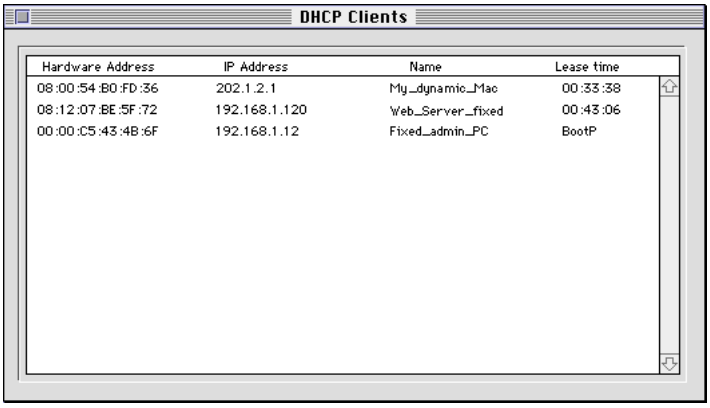
The MAC Address is the physical address of the Ethernet or Token Ring adapter in the client machine. (It has no direct relationship to "Macintosh"). An Ethernet address is represented as xx:xx:xx:xx:xx:xx, where each "x" is a hexadecimal character. For example you can find the MAC address of a Macintosh computer running Open Transport on Ethernet by opening the AppleTalk or TCP/IP Control Panel and selecting "Get Info" in the File menu. In MacTCP, hold down the Option Key while clicking the Ethernet icon to display the MAC address.

If the IP address is entered as "0.0.0.0" then the DHCP Server will assign an address automatically. If any other valid address is entered then this will be reserved for that client, and always assigned to it on demand.

The Name field can be up to 16 characters, with no spaces or tabs.

View DHCP Clients

During Gateway operation, the DHCP Server's current list of assigned addresses and active clients can be displayed by selecting "View DHCP Clients" in the File menu.



12 Host Access Rights

About this Chapter

Host Access Rights determine which local hosts (computers) can use individual Ports, and which remote hosts can be accessed through specific Ports or via the Gateway.

Two sets of Host Access Rights are provided.

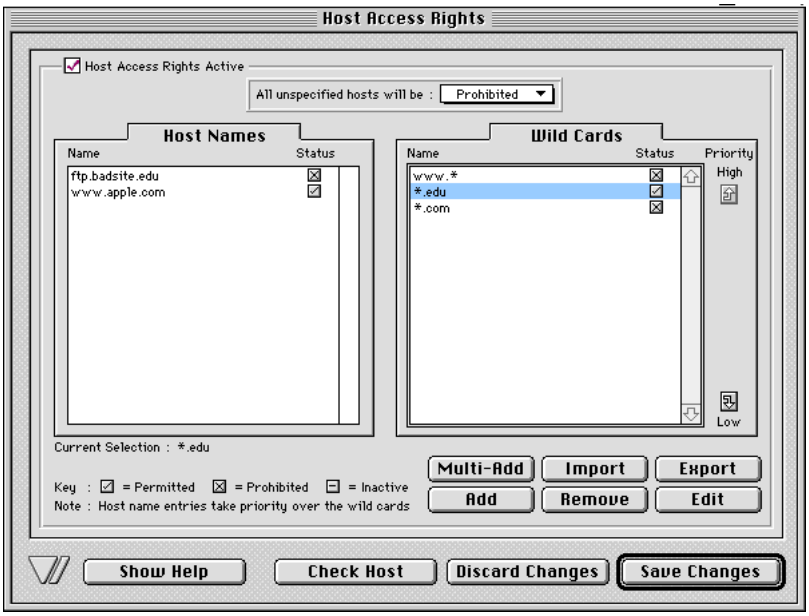
- Global Host Access Rights control access to named hosts and domains. They apply to all traffic passing through the Gateway, and provide a powerful and flexible way to limit the Internet sites which are reachable through the Gateway.

- Local Host Access Rights can be specified for each Port.
  They define which Clients can use the Port, which Clients can instigate an Internet connection, and which host IP addresses can be reached through the port. The latter function can be used for limiting access from certain subnets to specific local Servers.

These facilities are only available in Advanced and Administration User Modes.

Global Host Access Rights

Global Host Access Rights are set using the "Host Access Rights" item in the "Gateway" pull-down menu. A window appears:



The Global Host Access Rights can be enabled and disabled by clicking the "Host Access Rights Active" checkbox. When they are disabled the Gateway permits all access attempts.

Two lists of host and domain name rules can be edited. On the left is a list for specific Host Names to be Permitted or Prohibited. On the right you can enter host or domain names containing one or more asterisk (*) characters to denote "Wild Cards". A Wind Card entry allows you to specify a range of host names that have any sequence of characters in place of the asterisk.

A default rule is defined using the pop-up menu above the lists, to be applied to all unspecified addresses.

Each entry can be set to "Permitted", "Prohibited" or "Inactive" by clicking its check box control. This combination of facilities can be used to build powerful and complex filters.

In normal operation, the Gateway tests all new host name access attempts against the defined rules in sequence, and obeys the first one it finds that applies. The specific Host Name list is scanned first. If there is no match in this list, the Wild Card entries are checked in sequence from the top of the list. If no rule is found that explicitly Permits or Prohibits an access attempt then the default rule applies.

In the example screen shown, Gateway users are only permitted to reach the following hosts:

- no "www" server except www.apple.com
- any host in a .edu domain except ftp.badsite.edu
- any host in a .com domain

Single new entries are made by clicking the "Add" button. This opens a new entry, where you can type a string. The "Enter" button changes to "Enter Text", click it or press the Enter or Return key to put your new entry into the list. If you try to enter a wild card character in the specific names list, or a specific name in the Wild Card list, you will be asked if the entry should be added to the appropriate list instead.

If you have a large number of rules to enter, click the "Multi-Add" button. After you complete each entry a new one is opened for your next string. The "Enter" button changes to "Finish Entering". Click it to end the Multi-Add sequence.

The "Remove" button allows you to delete entries, and the Edit button will allow you to modify a selected entry.

As soon as you have modified the Global Host Access Rights the OK button changes to "Save Changes" and the Cancel button changes to "Discard Changes"

The Wild Card list entries are scanned in sequence, so you must get them in the right order to achieve the constraints you need. They can be selected and dragged individually or in groups to change their order. Discontinuous selections will group together when dragged to a new location in the list.

Use the mouse with the Shift key for continuous selections, and with the Command key to toggle separate entries into or out of the selection. Any change you make to one check box in a multiple selection will be applied to all entries in the selection.

To assist you in developing and testing filters, the Window has a "Check Host" button which opens an edit box. Enter a host name and click "Check", and the system will test it against the filters and tell you whether access to it would be permitted or prohibited by your current set of filters.

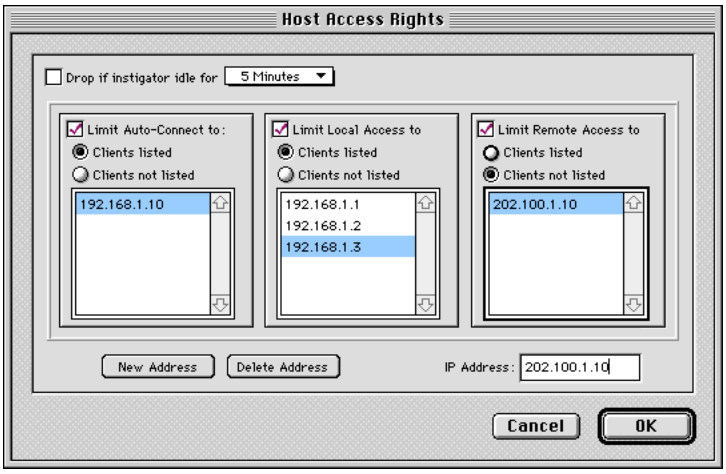
Help screens with brief explanations of filter rules can be displayed at any time by clicking the "Show Help" button.

Once you have a set of rules that achieves the restrictions you require, click the "Save Changes" button to save them into the Preferences file. You can export your filters to a file using the "Export" button, and import them using the "Import" button. In this way you can maintain several alternative sets of filters, or exchange sets with other Gateway users.

Local Host Access Rights

Local Host Access Rights are set using the "Host Access Rights" button in the "Edit Port Settings" window for an individual Port. They determine which local hosts (computers) can use this port, and which remote hosts can be accessed through this port. The Gateway imposes no restrictions by default.

To set up host access rights, click on the “Host Access Rights” button. The following window will be displayed:



Each of the list boxes is activated by setting the checkbox above it. The lists contain IP addresses of corresponding computers. It is not possible to enter computer names instead of addresses. By selecting one of the two radio buttons above the list, you can choose whether the restriction applies to listed computers or computers not listed.

The “Limit Auto Connect” list contains the computers on local networks that can cause this port to automatically connect. This is only valid for ports that need to establish a connection, such as PPP or SLIP, and then only if the “Allow auto connection” option is set (in “Connect Info”).

The “Limit Local Access” list contains computers on local networks that can use this port. Computers not listed here are not allowed to use this port. Alternatively, if you select the “Clients not listed” radio buttons, only computers that are *not* in the list will be able to use the port (and access the Internet through it).

The “Limit Remote Access” list contains *remote* computers that can be accessed through this port. No other computers can be accessed through this port. This list can also be used to specify hosts that *cannot* be accessed, by selecting the “Hosts not listed” radio button. This can be used to augment the Global Host Access Rights detailed above, by providing control over access to known absolute numeric addresses.

When an automatic connect is triggered the Gateway retains the IP addresses of the computer which started the connection. This computer is know as the *instigator*. If the “Drop if instigator idle” checkbox is enabled, the menu setting specifies the time after which the Gateway will disconnect the port after it has been automatically connected. This will happen once the instigator has been idle for the specified period, even if other computers are still using the port.

13 Troubleshooting

About this Chapter

TCP/IP networks are notoriously difficult to set up and operate. VICOM Technology seeks to reduce the complexity of the process wherever possible. When the Gateway does not work as you think it should, ask some basic questions:

- If it never worked, are you sure you followed the installation steps in this Guide?
- Was it working before? Check what you did that stopped it.
- Is your Internet Service operating?
- If these steps do not solve the problem, read this Chapter.

Help is also provided in the Support Area on our Web Site at **www.vicomtech.com,** where we maintain tutorials, technical notes, answers to Frequently Asked Questions, and a Support Request form.

If these resources do not resolve your problem, send us email at **support.vicomtech.com**, or call one of our Support centers.

Modem Problems

For speeds of 9,600 bps and above it is essential to have a hardware flow control cable and for "DTR & CTS" flow control to be enabled.

When using the Apple Modem tool, it is important to choose the right modem type. If your modem does not appear in the list select "Hayes Compatible" instead. Specific initialization strings may also be required for certain combinations of modems and Service Provider equipment.

If a modem appears to be "hung" try resetting the port. If problems still occur, refer to the manual that came with the modem, or contact VICOM Technical Support for assistance.

AppleTalk(MacIP) Problems

LocalTalk interferes with high-speed serial connections. It may be necessary to get a separate serial card to drive a modem; see "Performance Considerations" below for more details.

Login Problems

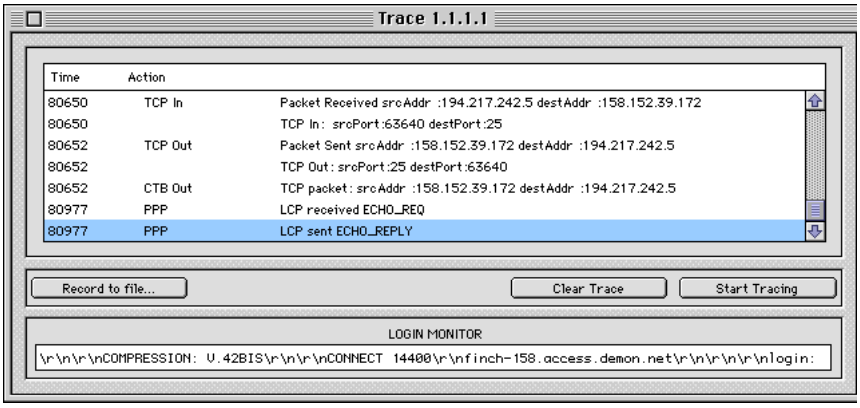
If the modem connects but the Gateway cannot log in, check that the login sequence is correct. Tracing a port can be very helpful.

Tracing Ports

The Trace window is used to monitor the traffic through a port. This is particularly useful when trying to solve login problems, as you can see the login sequence. If a login fails, the Trace window will indicate the reason such as time-out, or waiting for prompt, etc.

Only use the Trace window for diagnostic purposes as it will slow the Gateway down substantially during normal operation.

To open a trace window for a port, select the port and choose "Start Tracing Port" from the "Gateway" menu. The Trace window can be set to open automatically during login if the "Auto Trace" preference is set. The window will then automatically close if the connection is successfully established. The Trace window looks like this:



The title of the window shows the IP address of the port. The list displays packets going through the port and any messages generated by the Gateway. The Login Monitor is shown for the dial up port, and displays the data exchanged during the connection phase.

Problems with Internet or Local Hosts

If you can connect to the Internet Service but are not able to reach Internet servers, check that you are using the correct Domain Name Server address in the DNS Address field in Preferences, AND in the MacTCP or TCP/IP Control Panel for your Gateway Macintosh.

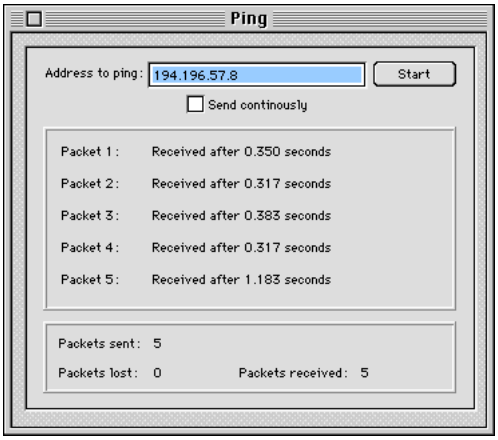
If your Client computers cannot communicate through the Gateway, check the Client setup.

You can use "Ping Host…" in the File menu to investigate these problems further.

Pinging Hosts

The Gateway includes a useful diagnostic tool called “PING”. This allows you to send an echo request (ping) packet to an IP address and check to see if it responds.

With the Gateway running and connected to the Internet, use “Ping Host…” in the File menu to open the Ping window.



To Ping a computer you need to know its IP address. The Gateway defaults to the address of a VICOM Server you can use to verify that you can access Internet services. Click “Start”. As each ping is sent, the Gateway will display “Sent, waiting for reply”. If the Gateway can reach VICOM the message will change to “Received after x.xxx seconds”. If not, the message will change to “Timed Out” after about 15 seconds.

If this works, use Ping to check that the Gateway can reach a Domain Name Server. Enter the IP address of the Domain Name Server for your Service Provider in the “Address to ping” field and click “Start”. You can also use Ping to check that Client computers can be reached. Note that a Macintosh Client will usually only echo a Ping if a TCP/IP application such as a Web Browser has been launched on it.

Open Link Ports

Certain Open Link port drivers need their own configuration and setup. If an Open Link port fails to connect for no apparent reason, try initializing the driver with the application supplied with the driver.

Performance Considerations

Serial ports on some earlier Macintosh models do not work well with speeds above 9,600 bps. The processor on these models is not fast enough to handle the amount of incoming traffic, so some data is lost.

An additional problem arises when LocalTalk is used. Since LocalTalk is driven by the same chip as the serial port, it interferes with reception of incoming data. This is caused by any LocalTalk activity, such as File Sharing, Printing or using E-mail. Serial speeds above 9,600 bps cannot be used on low performance systems if the Gateway is configured for LocalTalk. Please note that more recent Macintosh models do not usually suffer from these limitations.

Serial port speed limitations can be solved by using a separate serial card such as a “Hurdler” from Creative Solutions Inc. or “Smart Serial”, for PCI machines, from Keyspan Inc.

Any other processor-intensive or network-intensive task, such as file sharing or a mail server, will slow down the Gateway. In extreme cases this may cause the client machines to time out and lose connections. The Gateway displays a “CPU Load Indicator” in its status window, which shows how much load the Gateway is putting on the CPU.

Please note: System software 7.5.3 improves serial port performance on all PowerPC and Quadra AV machines. If you are experiencing problems of this nature please upgrade your System software to this version .

A Manual Client Configuration

About this Appendix

Client computers must be set up so that they can use the Gateway when they need to connect to the Internet.

All client machines need to have three items of information to be able to use the Internet. These are:

1. A unique IP address for the client machine.
2. An IP address of a Domain Name Server (usually your Internet Provider's DNS).
3. The IP address of a default router or gateway.

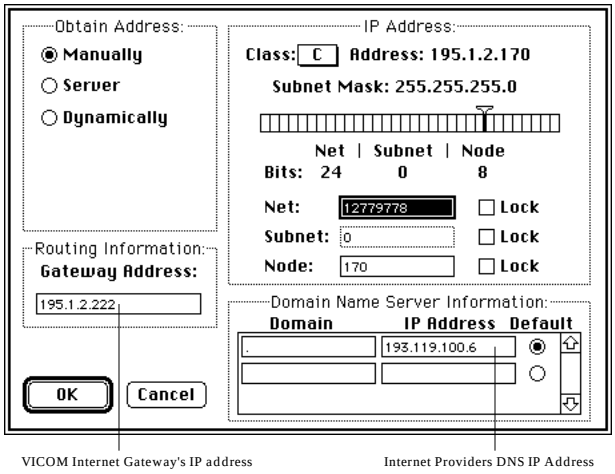
The above information can either be set up automatically, using the DHCP Server, or manually for each Client.

Chapter 3 described how to do this assuming you are using the DHCP Server function. This is the recommended method wherever possible, as it removes the need to set each machine up manually with all the correct host and router address information, it ensures that Client addresses are unique, and it recovers them automatically when machines are removed from the network.

However, for various reasons you may prefer to configure your network manually. If so, this Appendix provides guidelines for Macintosh, Windows and Unix system configuration. Please use this information in conjunction with the documentation provided with your client equiment and its TCP/IP software.

Setting up Macintosh MacTCP Clients

1. Open the MacTCP control panel.
2. Configure the network connection for Ethernet, LocalTalk or Token Ring according to your cabling.
3. Click on the "More" button to display additional options:



4 Select “Manually” in “Obtain Address”.

5 Select the Address Class in the pop-up menu, and adjust the subnet mask using the slider if necessary.

6 Enter the IP address of the Gateway’s Ethernet, MacIP or Token Ring Port in “Gateway Address” field.

7 Enter “.” in “Domain” and the IP address of the domain name server in “IP address” field in the “Domain Name Server Information”. This address may be supplied by your Internet Service Provider, or you may have a local DNS.

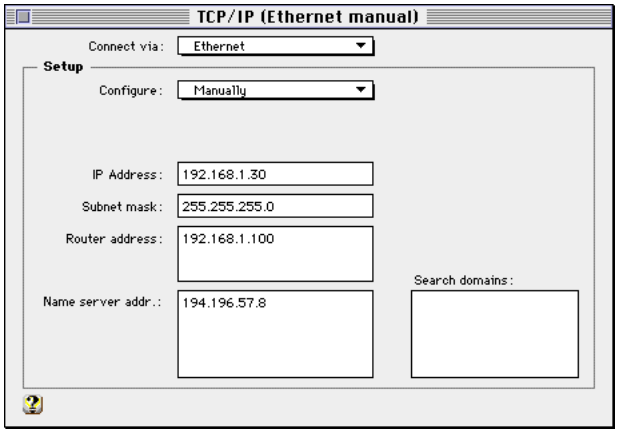
8 Click OK to return to the first MacTCP screen.

9 Enter the IP address selected for this Mac. The network number of the address must be the same as the network number of the Gateway’s Ethernet or Token Ring port. In the above example, both network numbers are 195.1.2.

10 Close the MacTCP control panel and restart the Macintosh.

Setting up Macintosh Open Transport Clients

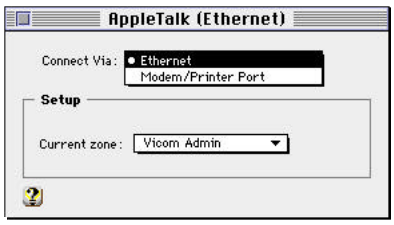
1. Open the "TCP/IP" Control Panel. Set "Connect via:" to Ethernet or TokenRing as appropriate.



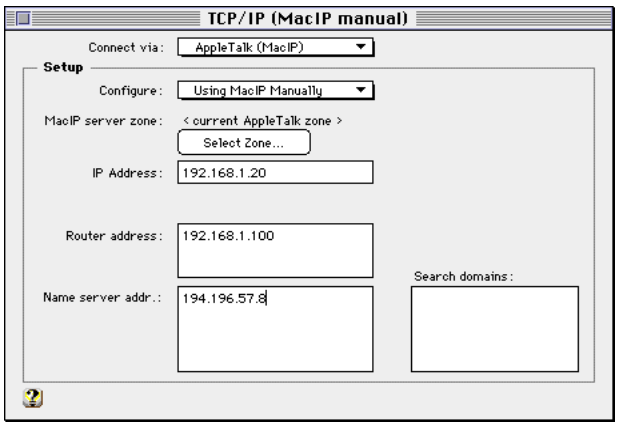
2. Select "Manually" from the "Configure" menu.
3. Enter your IP address. The address should be provided by your network administrator. The network number of the address must be the same as the network number of the Gateway's Ethernet or Token Ring port.
3. The "Subnet mask:" field should be set to "255.0.0.0" for class A networks, "255.255.0.0" for class B networks and to "255.255.255.0" for class C networks. Please see Chapter 8, Routing, for further explanation of network classes.
4. Enter the IP address of the Gateway in the "Router address:" field.
5. Enter the IP address of your Domain Name Server in the "Name server addr." field. This address should be supplied by your Internet Service Provider.

Setting up Macintosh MacIP Open Transport Clients

1 Open the “AppleTalk” Control Panel and select the appropriate AppleTalk connection and zone .



2 Open the “TCP/IP” Control Panel:



3 Set “Connect via” to “AppleTalk (MacIP)”. Select “Using MacIP Manually” from “Configure”. Select the Gateway’s zone in “Select Zone...”.

4 Enter your IP address. The address should be provided by your network administrator. The network number of the address must be same as the network number of the Gateway’s MacIP port, i.e. 202.1.1.180 being the address of the Gateway's AppleTalk port, to work with the above.

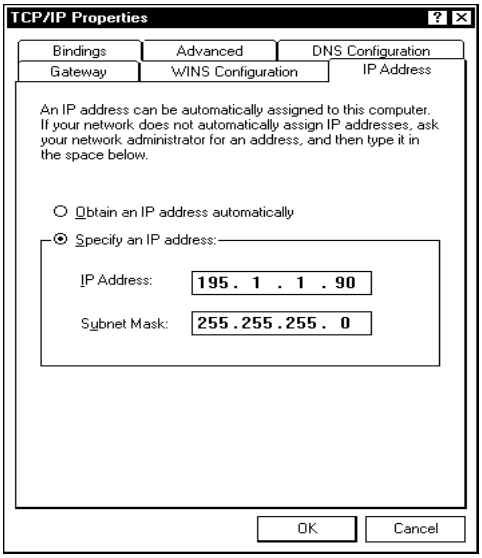
5 The “Subnet mask:” field should be set to “255.0.0.0” for class A networks, “255.255.0.0” for class B networks and to “255.255.255.0” for class C networks. Please see Chapter 8, Routing, for more details of network classes.

6 Enter the IP address of the Gateway in the “Router address:” field.

7 Enter the IP address of your Domain Name Server in the “Name server addr.” field. This address should be supplied by your Internet Service Provider.

Setting up Windows 95 Clients

1 Open the “Network” Control Panel. Double-click on “TCP/IP” in the network component list. Click on “IP Address” tab:

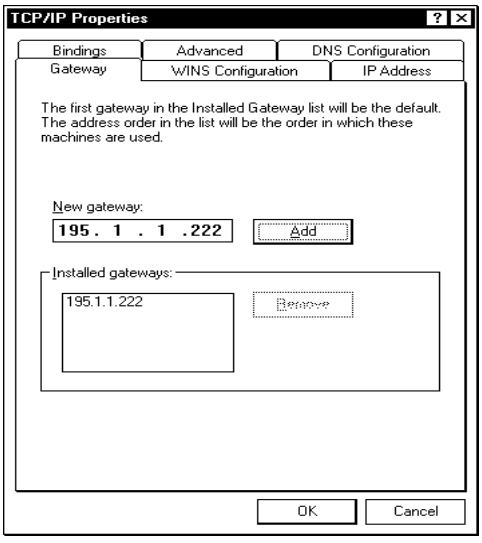


2 Select “Specify an IP address:”.

3 Enter your IP address. The address should be provided by your network administrator. The network number of the address must be same as the network number of the Gateway’s Ethernet or Token Ring port.

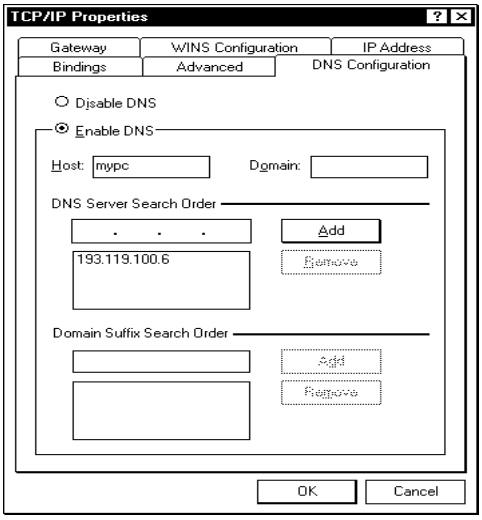
4 The “Subnet mask:” field should be set to “255.0.0.0” for class A networks, “255.255.0.0” for class B networks and to “255.255.255.0” for class C networks. Please see Chapter 8 on Routing for further explanation of network classes.

5 Click on the “Gateway” tab:



6 Enter the Gateway's IP address. Click "Add" to insert the entry as the **first item** in the "Installed Gateways" list.

7 Click on the “DNS” tab:



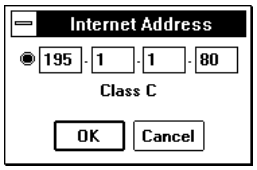
8 Select “Enable DNS”. Add the Domain Name Server IP address to “DNS Server Search Order” list. This address should be supplied by your Internet Service Provider.

9 Restart the computer. The Gateway should now be accessible.

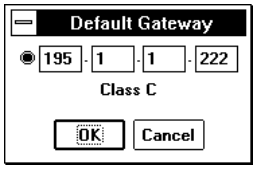
Setting up other Windows Clients

TCP/IP setup procedures vary according to the software installed. The following is a typical example, based on Netmanage NEWT:

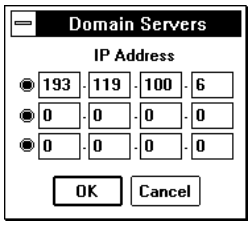
1 On a client NEWT machine select the “IP Address” item from the “Hardware...” window in the “Custom” application. Enter your assigned IP address and click “OK”.



2 Select the “Default Gateway” item from the “Services” menu of the “Custom” application. Enter the Gateway's IP address.



3 Select the “Domain Servers...” item from the “Services” menu of the “Custom” application. Enter the domain name server address as provided by your Internet Service Provider.



4 Restart the computer. The Gateway should now be accessible.

Setting up Unix Clients

Because of the wide range of Unix versions and Command Line and Graphical user interface shells in use, it is beyond the scope of this Guide to provide detailed information on configuration of these systems. If you are installing a new Unix system, then refer to its installation instructions to set the addresses up. Some general guidance is provided below for adapting existing installations to use the Gateway.

Typically, an existing Unix machine will already have an IP address. The most likely change you will have to make when you install the Gateway is to add a routing table entry to define the Gateway as its default router.

The following command (or an equivalent) will show the existing routing table:

```
netstat -nr
```

The first two columns in the routing table (Destination and Gateway) are the items that are the most important. There should be an entry such as "0.0.0.0" in the Destination column, and it is necessary to edit this entry to set the Internet Gateway's address in the Gateway field.

To add an item manually to the routing tables, your system will provide a command such as "route". The format of this command will be something like this:

```
route add 0.0.0.0 [Gateway Address] [hop count]
```

Enter the appropriate command, using the Vicom Internet Gateway's internal IP Address and setting the hop count to 1.

Once you have tested it successfully you should add this command to the system's start-up file. This file will probably be found in the "/etc" directory and the file name will start with "rc". Insert the tested route command to the start-up file to execute it every time the UNIX machine is started.

B Legal and Commercial Matters

Legal Matters

License

The purchase price of the software includes a personal non-exclusive license for the person/company purchasing the license to use or install the program and associated files for their own purposes, on *ONE* Macintosh computer at one time.

The license does *NOT* include the right to make any copies of the program and files for any purpose other than backup or to have the program installed on more than one Macintosh at one time. No copies of all or portions of manuals are to be made. Any copies of software or installation on more than one hard disk or copies of manuals (or portions thereof) shall constitute a breach of copyright and shall be dealt with to the fullest extent of the applicable law.

The word "backup" means a copy for the licensee's own personal security in the event of failure of the disks provided by VICOM Technology Limited. The licensee undertakes not to transmit any copy of his backup to any third party, whether for sale or otherwise. Any such unauthorized transfer shall constitute a breach of license and copyright.

Should the licensee desire to transfer his license to use the software to a third party, he shall firstly obtain the consent in writing of Vicom Technology Limited which consent shall not be unreasonably withheld. Licensees requiring copies of VICOM software to run on multiple CPUs should contact Vicom Technology to obtain details of quantity discounts and site licenses.

Warranty

Should the supplied disks fail, for reasons of defect in material within 12 months of purchase and registration, Vicom Technology will replace such failed disk for the Registered Owner free of charge.

Notwithstanding the above, Vicom Technology shall not replace, or be obliged to replace any disk if it has failed as a result of misuse.

Disclaimer Fitness For Particular Purpose

Vicom Technology makes no representations or warranties of any kind whatsoever with respect to the software, or the contents thereof, other than that herein set out, and specifically disclaims warranty for fitness for any particular purpose. Vicom Technology shall not be liable for errors contained in the software or herein or for incidental or consequential damages in connection with the furnishing, performance or use of the software or the manuals.

Changes to Software or Documentation

Vicom Technology reserves the right to revise the software and / or the User Guide and to make changes in the content thereof, without the obligation to notify any person of such changes.

Trademarks Acknowledged

All trademarks, Service Marks and the like owned or used by third parties and mentioned in this guide are hereby acknowledged.

Commercial Matters

Technical Support

Vicom Technology shall provide technical support via Email or by telephone, only to bona fide licensees of VICOM software who have completed, signed and returned their Warranty Registration forms.

Upgrades

From time to time Vicom Technology issues upgrades to the VICOM software. These upgrades shall only be available at special discount prices to bona fide licensees of VICOM who have completed, signed and returned their Warranty Registration forms.

Feedback

Vicom Technology have been creating communications products since 1985. Many people have provided input which has contributed to the many improvements and enhancements.

Input from users, corporate support departments, VARs and dealers regarding future improvements and enhancements, is actively encouraged and gratefully accepted.

A

B

C

D

E

F

G

H

I

J

K

L

M

T

U

V

W

X

Y

Z