MajorTCP/IP

TCP/IP Connectivity Software

for The MajorBBS and Worldgroup

by Vircom Inc.

Installation Guide

1997
v2.10-X

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Table of Contents

FOREWORD

The purpose of this guide is to get your BBS connected to your provider as swiftly as possible, this way, you can give your customers the ability to surf the net in record time. Included in this manual are the essential things you need to know to setup MajorTCP/IP properly in a step-by-step approach.

It is important to note that connecting to the internet is no small task. For all intent and purpose, you are trying to plug your computer bulletin board system into one of the most complex edifices that humankind has devised in the long history of our race. Unfortunately, the technology has yet to reach the simplicity say, of cable TV where all you need to do is plug a coaxial cable in your TV and voilà, instant access.

Because of the complexity involved here, it is important for us to break down the process of connecting your system into small bite-sized tasks. Each task is important as this will define the way your machine talks to every other machine that makes up this incredible assemblage of computing power and people that makes up the global internet.

All this being said, you should not let yourself be scared by what we just told you. Connecting to the internet is a fairly straight-forward process for those who have already done it. It may seem a little bit daunting at first for those whom this is the first time. The Internet uses its own terminology that stems from its roots in the Unix operating system which itself is pretty cryptic at times. Nonetheless, until the technology matures to the point where the Internet is plug-and-play, we are forced to deal with it as best we can. We sincerely hope that this manual will let you do just that.

One of the methods by which we will attempt to get you up and running is by the tried and true method of the checklist. Simply mark those sections you've finished and continue on to the next task. This systematic approach will make you feel more confident about what you are doing and will help us troubleshoot the problems when you find that you are unable to make any further headway.

So sit back, relax, take the time to read this manual a few times, grab a pen or one of those nifty fluorescent fuzzy highlighters and enjoy.

Limited Warranty

This documentation and any related software are sold "as-is", without any warranty either expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, and loss of profits or other economic damages. Vircom Inc. does not warrant that the operation of this software will be uninterrupted or error free. In no event and under no circumstances will Vircom Inc. be liable for any damages in excess of the sum paid by the customer for the product to which any claim for damages relates.

License

You may:

1. Install and operate this software on a single computer only.

2. Make one copy of this software into machine-readable or printed form, backup or archival purposes in support of your use of this software.

This software is licensed to a single corporation or person, for operation on a single machine only. Once licensed, the license to use this software is NOT TRANSFERABLE to any other person or corporation, without the express, written permission of an officer of Vircom Inc. Some geographical regions may require additional licensing in order to be valid. As a policy, we allow the transfer of license of MajorTCP/IP only when it is sold with the MajorBBS/Worldgroup system it was purchased for. We do not allow the transfer to another MajorBBS system.

YOU MAY NOT USE, COPY, MODIFY, MERGE, DISASSEMBLE OR TRANSFER THIS SOFTWARE, IN WHOLE OR IN PART, EXCEPT AS EXPRESSLY PROVIDED FOR IN THIS LICENSE.

Violation of any parameter of this license will result in the immediate forfeiture of said license.

Contacting us

If you need assistance or have suggestions concerning MajorTCP/IP, don't hesitate to call or write us. Our offices are open from 9AM to 5PM Eastern time, weekdays.

Majornet electronic mail	Support@GMS
Majornet support forum	MAJORBBS.DEV.TCP
E-mail: Technical support	support@vircom.com or majortcpip@vircom.com
E-mail: Suggestion box	suggest@vircom.com
You can also finger us	finger info@www.vircom.com
And surf the web to us	http://www.vircom.com
Our tech support line	(514) 990-2532, weekdays, 9AM to 5PM eastern.
Our support BBS	(514) 523-7979 **internet: bbs.vircom.com (port 23, Binary**) When you logon for the first time, one of the menu options you'll be offered is [M]ajorTCP/IP client registration. What we need from you is your MajorBBS/Worldgroup registration number and your incoming/outgoing activation codes for MajorTCP/IP. The registration module is automatic and will grant you full client access if the information given is valid.
Snail-Mail	Vircom Inc. 1205 Papineau Ave. Suite 352 Montreal, Quebec Canada H2K 4R2

What you can do with MajorTCP/IP in a nutshell

MajorTCP/IP gives you the connectivity tools you need to provide a wide range of internet services to your clients. Here is a summary list of each of these options. You can refer to their respective chapters (or setup steps) to get a better idea what each service is used for. Depending on which version of MajorTCP/IP you are using (Incoming, Outgoing or Combo), some of these options won't be available to you. Please refer to the chart at the end of this section.

Outgoing Telnets

Allows users who call your BBS to connect to remote systems using the target machine's internet address. Telnet is akin to a communications program: the target system needs to design a user interface to allow incoming Telnets. More precisely, systems you telnet into are listening to a port, and the communications go through that port. Rlogin on the other hand lets you login directly into the machine. Outgoing Telnets have the feature that they do not use up any of your precious licenses on a Galacticomm six-pack. One of the features provided by MajorTCP/IP is programmable Telnets. You can create menu pages with pre-defined services (like MUDs, MOO's or MUSHES ... basically text-based multi-user games) where people can access these by a simple menu selection or via a simple click of the mouse if you are using Worldgroup.

Outgoing RLogins

Allows user who call your BBS to connect to remote systems similarly to Telnet. RLogin is more akin to one of those programs that let you take control of your machine remotely at the DOS level enabling you to run any application this way. RLogin lets users login to "shell" accounts and run applications on remote Unix systems. Like outgoing Telnets, outgoing Rlogins do not use up any licenses from a six-pack. Also, Rlogin is programmable, letting you create pre-defined menu pages with Rlogin connections.

Incoming Telnets/RLogins

In the same fashion users on your system can connect to remote systems on the internet, people on the internet can connect to your BBS. This means that access to your BBS can become truly global because anybody with internet access can login to your system. These incoming calls, like normal modem calls, use up some of your licenses on a Galacticomm six-pack.

Multi-Homing support: MajorTCP/IP now supports multi-homing with incoming Telnets and Rlogins. What this means is that users who have their own domain name can have people from the internet Telnet to their domain name and wind up on the BBS proper. Furthermore, when people do so, they are assigned a special pseudo-key that allows you to setup alternate menu pages for these users. In essence, you can have a virtual BBS, where the BBS changes appearance depending on which address users are connecting to.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

FTP client module

FTP or File Transfer Protocol allows users to browse and download files from any FTP site on the internet. This means that your users will have access to the vast file libraries that exist out there. They can transfer the files to your system in a temporary cache area. Afterwards, they can either download it right away using the standard protocols available from your file Libraries or tag the file for later retrieval before logging off. Like Telnet and Rlogin, you can create menu pages with pre-defined FTP sites making your client's life easier.

Finger client module

Finger lets your users find out if someone is logged into or is a user of a remote system on the internet. This is akin to people using the /# command on your BBS. People can either finger a system to see all the users on-line at the moment, or the can finger a particular user to see if the person is currently on-line. If the person isn't on-line, your user can find out the last time the person logged-in and fetched his or her mail.

Finger now supports a /FINGER global command which lets users do a /finger without having to go to a special finger menu page.

Finger Information Server

This feature lets people on the internet find out who is on-line at the moment. Unlike the Unix finger however, the amount of information given out is the same as the /# command although you can change it by modifying the message files associated with these BBS functions. You can add various text variables to increase or decrease the amount of information available globally or specifically to a user.

WWW Server

The built-in web server lets you put up your own HTML pages (Hyper Text Markup Language), making it possible for you to create a plethora of services on the hottest feature on the net. One of the big attractions of the internet these days is the point and click ease of the World-Wide-Web. It's also very easy to provide all kinds of information to people because HTML offers a very simple method to create Hyper-Text documents, combing text, images and even sounds in one neat package.

One of the big features of our WWW server is the fact that incoming "web hits" (people who come to check out individual pages) do not use any Galacticomm Licenses out of your six-packs. To allow your own users to browse your web pages, you will need to use the SLIP/CSLIP/PPP server described in this section.

Our web server supports a plethora of new features including:

- HTTP 1.0 Compatibility
- Subdirectory Redirection
- Combined Log Format
- Clickable Image Maps
- Form to File Support
- Form to Email support
- WWW security
- User account information
- VRML, JAVA and Plug-In Compatibility

WWW Multi-Homing: Lets you run a "virtual web server" for clients who want to have their own domain name. What this means is that you can have a separate web server for each additional domain name assigned to the BBS. For instance, lets assume your BBS domain name is **yourbbs.com** with an alias of **www.yourbbs.com**. If at some point, you have a corporate client that wants to have his own domain name **hiscompany.com and www.hiscompany.com**, you can now operate a virtual web server that will allow people to do an **http://www.hiscompany.com/ directly**. This means that any client can have his or her own directory structure separate from your main BBS HTML directory hierarchy.

SMTP E-mail Server (For Real/Time Internet E-mail)

SMTP E-mail lets your users send and receive E-mail to/from anyone on the internet. E-mail is sent immediately after the person saves the message in the standard MajorBBS/Worldgroup facilities. SMTP E-mail is totally transparent. The only difference people will see between local mail and SMTP E-mail is the need to specify a valid internet E-mail address. Like the WWW server, SMTP E-mail traffic does not use up any of your Galacticomm licenses

SMTP Includes MIME support: MajorTCP/IP now supports MIME encoding and decoding as part of the basic SMTP package. That means that incoming MIME-encoded file attachments are converted into standard file attachments at the BBS level. Furthermore, the user who wants to send his file over the internet will see his files converted to the standard MIME format as well.

Multi-Homing support: SMTP can now handle multiple domain names for clients of your system that want to have their own domain name assigned to them. That means that, instead of sending mail from your principal domain name, you have the capability of having mail labaled as coming from the client's personnal domain name.

Telnet/RLogin Dial out Channels

These channels are a special feature of MajorTCP/IP that let you operate many of the third party add-on modules like Maillink or Chatlink over the internet. These modules were never designed to talk on the net, so we created an emulation protocol that lets us simulate a modem session with Telnet and Rlogin as the transport medium instead. This makes it incredibly valuable because of all the long-distance charges you save as opposed to calling these services via modem. Because we simulate a modem connection, Telnet/RLogin dial out channels do use up licenses from your user count.

SLIP/CSLIP/PPP Server

This more than any other service will be one of the major reasons people will want to become users of your system. The SLIP/CSLIP/PPP server lets you offer SLIP, CSLIP and PPP connectivity to your clients, enabling them to gain access to the World-Wide-Web. The only things your clients need is a TCP/IP stack (like Trumpet Winsock) and a graphical web browser (like Mosaic or Netscape). In fact, there are many client programs for Trumpet Winsock that can take advantage of your SLIP/CSLIP/PPP link, all of these being Windows-Based. People connected to your BBS via SLIP/CSLIP/PPP and going out over the internet do not consume any of your user six-packs, unless these use the Worldgroup Client or a Trumpet Winsock Telnet client to Telnet back into the system.

PPP server special features: From now on, chances are that you will abandon SLIP and CSLIP in favor of the more advanced PPP protocol now available with MajorTCP/IP's PPP Server. The new PPP server supports the following features:

- **Performance Optimization:** Support for Address Compression, Protocol Compression and Van Jacobson Header Compression, optimizing data throughput. In other words, **PPP is faster.**

- **PPP Smart-Sensing:** Our PPP server automatically recognizes that the caller is using a PPP stack. The Channel will switch to PPP mode, without any command prompt. This means that **you can throw complex custom scripts in the trash bin reducing your technical support load in the process**. PPP Smart-Sensing thus includes the following capabilities:

    - **PPP Authentication Protocol:** Most PPP stacks today support PAP. Used in conjunction with PPP Smart-Sensing, the PPP stack will feed your system a username and password automatically, without having to write that into some sort of script. PAP configuration on most platforms simply requires the user to enable it and input their username and password which is much easier than making them install a login script.

    - **IP Address Negotiation:** The automated negotiation capability makes entering the IP address in the stack obsolete. That means your users will no longer need to know, much less enter the IP address the server allocates. The server will automatically tell the PPP stack what address the user was assigned. The PPP stack will simply insert that IP address in it's configuration and work, without prompting the user. All of this is invisible as far as the user is concerned.

    - **Primary DNS Negotiation:** Microsoft published a new standard in December '95 to support automatic negotiation of the primary name server's IP address. Like the IP address in the last paragraph, this automatic negotiation takes the user one step farther from the technical aspect of connecting to the Internet. Since the standard is so recent, few stacks are supporting this feature. It has been tested with Windows 95's dialup networking, as well as Windows NT's.

BOTTOM LINE: The latest PPP standards supported in the new PPP module can contribute significantly toward decreasing your business' operating costs and give you more time to expand your market share. Vircom's no non-sense PPP implementation had one goal in mind: make Internet connectivity as simple as possible. How well have we done? A Windows `95 user has no login script to set up and only three information to enter to connect to your system: (1) BBS phone number (2) User ID (3) Password

We consider the above features essential to any sound PPP offering for the Worldgroup platform.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Improved User Ghosting: The feature that allows users connected in SLIP, CSLIP or PPP to telnet back into the system using Worldgroup Manager was improved security-wise. The Sysop can now control who can telnet back into the system and restrict such telnets to local users, preventing multiple people from using the same account concurrently. Credit consumption rates for the second telnet can be customized for your system's needs.

Internal SLIP/CSLIP/PPP dialer

Those of you who will connect to your provider via a SLIP/CSLIP/PPP dialup will be interested to know that we now have a built-in SLIP/CSLIP/PPP dialer. This means that you will not need to maintain the connection manually as it was the case with the old method that used to employ SLIPPER/CSLIPPER. If the connection to your provider is lost, the SLIP/CSLIP/PPP dialer will attempt to re-establish the connection totally automatically.

PPP Dialer features: Your system can take advantage of the new PPP features in the same fashion your users can. If you want to connect to your provider over a PPP Link, you can use the built in PPP dialer (part of the SLIP/CSLIP/PPP dialer) to accomplish this. Furthermore, all features that exist for SLIP and CSLIP connections to your provider are supported as well for PPP. This includes the ability to re-establish the connection to your provider if the connection is lost. You can still use the TCPDIAL.SCR script to do that although if you enable PAP, the script is no longer necessary. The PPP dialer supports the following features:

- **Authentication Protocol (PAP):** This feature is supported in the PPP dialer, removing the need for any script to connect to your Internet Service Provider (I.S.P.). UserID and Password information is entered in CNF fields. If the I.S.P. doesn't support this feature, the traditional login script can be used instead.

- **Addresses negotiation:** The IP and DNS addresses negotiation is also supported in the PPP dialer. This means that your BBS can now use a dynamic IP address, although this will essentially prevent anyone from reaching your BBS. (Imagine how easy it would be to reach someone randomly changing phone number.)

Keepalive feature: To avoid disconnections of the BBS' link to the Internet, due to the ISP's inactivity hang-up, a "keep alive" configuration option was added. It allows the system operator to configure a time interval, in seconds, to generate activity on the Internet link by pinging the BBS' primary DNS server.

NNTPD News Server

The NNTP or Network News Transfer Protocol is the means by which you will be able to send and receive Usenet News. You define those newsgroups you wish to carry by creating forums associated to the newsgroups you desire. Once the Newsgroup mapping is generated, you give to your provider the list of newsgroups you wish to carry. After configuring NNTP properly, your system will be able to pull in messages on a continuous basis. All messages are imported directly into the Forum system seamlessly. This means you won't need to teach your users how to use Usenet since it's fully integrated with the forum system, something they already know how to use already.

IRC Client

IRC or Internet Relay Chat is the Internet's equivalent to the MajorBBS/Worldgroup Teleconference system. The really impressive feature of IRC is the sheer size of it. At any one time, tens of thousands of users can be using the IRC system in thousands of different channels, with topics ranging from general chit-chat to discussions on the nature of the universe. IRC is to teleconferencing what Usenet is to the rather limited local forums of your system. It opens up an incredible world where people can meet in real-time. MajorTCP/IP's IRC client provides your users with the basic functions required to talk over the IRC system. It includes all of the channel operator functions, and incoming DCC (Direct Client-to-Client) reception of chats and file transfers.

The IRC Client now supports multiple default IRC servers and personalized IRC settings for each user (default Nickname, IRC channel and server or server group).

FTP Server

MajorTCP/IP now comes with a built-in FTP Server, allowing your users to access files in your file library directories via the standard FTP protocol. Furthermore, the FTP server will also have some support for **Multi-Homing and Home-Page** maintenance for people who want to be able to access a private area where their web pages are stored (requires a home-page maintenance module like Web-Master (High-velocity software) or Web-Blaster (DialSoft)).

DMA 2.1 (Distributed MajorBBS Architecture)

DMA opens up whole new possibilities for your MajorBBS/Worldgroup system. In a nutshell, DMA lets you create a "network" of sub-BBSes. This network can be located insitu or you can connect to a remote sub-BBS, all of this transparently. What this means for you is that you can:

- Go beyond the 16 megabyte barrier by offloading modules to the sub-BBS.
- Create a separate game machine. If it crashes, the rest of the BBS remains.
- Create a common service machine that can be shared by many BBSes.
- Offload resource-hungry applications, increasing system-wide performance.

And many many more. DMA is one of those exciting new features that can increase the flexibility of your system by leaps and bounds. Issues specific to DMA can be found in the separate DMA manual that came with this document.

OTHER STUFF

One of the nice features of MajorTCP/IP's Rlogin protocol is the ability to pass information from the BBS to a system you are connecting to. One of the common things people do to increase the number of services available is to setup a Unix box networked to the BBS machine. Using an a pre-programmed Rlogin connection, people can offer Unix services that aren't yet available directly through MajorTCP/IP. Services like: IRC, MUDs (Multi-User Dungeons), Archie, Gopher, Shell accounts ... the list is endless.

LOW SIX PACK USAGE

Contrary to our competition, MajorTCP/IP uses far fewer of the familiar six-packs. In fact, 6-packs are used only for the following features:

- **Incoming Telnets and Rlogins:** Each incoming telnet channel needs to be defined in the Channel group configuration. This means that they will consume licenses off of your six-packs.

- **Dialout Channels:** Dialout channels use a modem channel to simulate a modem, so as to carry traffic over the internet instead for modules that have never been designed to operate over the net. Each Dialout or TELOUT channel you define uses up a license from a six-pack.

- **The SLIP dialer:** If you use the built-in SLIP/CSLIP/PPP dialer to establish the connection to your provider, the connection will use one of the modems from your modem pool which uses up one license from a six-pack.

- **The FTP server:** Incoming FTP sessions use up one license from a six-pack.

Chart of MajorTCP/IP features

Features in MajorTCP/IP	"Combo"	Incoming*	Outgoing*	DMA Server
Outgoing Telnets	Yes	No	Yes	No
Outgoing Rlogins	Yes	No	Yes	No
Incoming Telnets/RLogins	Yes	Yes	No	Yes**
FTP client module	Yes	No	Yes	No
Finger client module	Yes	No	No	No
Finger Information Server	Yes	No	No	Yes
WWW Server	Yes	No	No	Yes
SMTP E-mail Server w/MIME	Yes	No	No	Yes
Telnet/RLogin Dialout Channels	Yes	No	No	No
SLIP/CSLIP/PPP Server	Yes	No	No	No
Internal SLIP/CSLIP/PPP dialer	Yes	No	No	No
NNTPD Usenet news server	Yes	No	No	Yes
IRC Client	Yes	No	No	No
POP3 Server	Yes	No	No	No
FTP Server	Yes	No	No	Yes
DMA 2.1 Client	Yes	No	Yes	No

* As of November 1995, the incoming-only version of MajorTCP/IP is no longer available.
** As of May 1996, the outgoing-only version of MajorTCP/IP is no longer available
*** Restricted to incoming traffic from a Master BBS only.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Installation Summary

You've read the foreword, you've seen where you can get help. Now what? It's time to get to work. This is the summary of the steps involved in setting up your computer system to talk to the Internet. You can use it as a global checklist if you wish (in fact, we recommend it). You can skip those steps that do not interest you. (if you're not interested in running a web server on your system, simply skip that section). We assume you already have a basic knowledge of MS-DOS and the proper care and feeding of a MajorBBS or Worldgroup BBS System. Keep your MS-DOS and BBS manuals handy.

STEP	Description	Done
#1	Get the information you need before installing the product	
#2	Get MajorTCP/IP off of your diskette and on your computer system	
#3	Configure the MajorTCP/IP core modules	
#4	Configure MajorTCP/IP to talk to the net	
#5	Configure the Rlogin module	
#6	Configure the Telnet module	
#7	Configure the FTP client module	
#8	Configure the Domain Name and Finger Server	
#9	Configure the World-Wide-Web Server	
#10	Configure the SMTP module	
#11	Configure the SLIP/CSLIP/PPP server	
#12	Configure the NNTPD News Server module	
#13	Configure the IRC Client module	
#14	Configure the POP3 server module	
#15	Configure the FTP server module	
(a)	Advanced Features: Multi-Homing capability.	
(b)	Advanced Features: Banning outside systems.	
(c)	Advanced Features: DMA Server configuration.	

A note about the manual format

ITEM
Default-Value

When the discussion talks about a parameter that has to be configured in a message file in the various configuration options, these will take the following format. The name of the item is on the first line to the left in **BOLD.** The default value is right under the name of the item in normal characters. The description of the item is written as this example here.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

STEP #1:

Information you need before installing the product

Before even putting the distribution disk in the machine, you need to find out a few things so that the following steps go smoothly. This portion of the installation guide also defines some of the terminology used by folks on the internet.

Hardware Requirements

Computer Hardware

MajorTCP/IP will run comfortably on the same hardware your MajorBBS or Worldgroup is currently running on right now. Memory-wise, MajorTCP/IP requires only 4 kilobytes of main memory. The brunt of MajorTCP/IP resides in the upper memory area, where it will consume half a megabyte of ram (500k).

The software was designed specifically to be extremely efficient by using up as little space and CPU time as possible within the constraints imposed by the MajorBBS and Worldgroup software. MajorTCP/IP has been clocked at being able to handle upwards of 600 packets per second in peek loading periods.

Connection Hardware

MajorTCP/IP will talk to the internet using two different methods, either via an asynchronous SLIP, CSLIP or PPP connection using a high-speed modem, or via an Ethernet connection.

Asynchronous SLIP/CSLIP/PPP modem Connection

Most sysops start with a modem connection for several reasons. SLIP/CSLIP/PPP dialup connections are usually the least expensive means to get on the information superhighway. Also, the relative simplicity of this type of connection gives the sysop the opportunity to get used to the internet on a gentler learning curve, and gives him a taste of what the internet can be at higher speeds. Finally, most people start with a dialup connection to build-up the clientele necessary to afford a faster link later on.

For a modem connection, you basically need an available COM port or a serial port on a multi-port unit. The port must use a 16550 UART chip to be able to handle the high speed data transfers the modem will be dealing with. You must also have a modem cable that will support hardware flow control (with the CTS/RTS pins). The modem you use should be Hayes-Compatible in terms of the command set used. Our software will work fine with baud rates ranging from 9600 baud to 38400 baud inclusively.

Ethernet Connection

MajorTCP/IP will work over most types of Ethernet connection and will operate fine over a straight TCP/IP network or a Novell Network. MajorTCP/IP will not work over Lantastic or NT networks unless these are configured to emulate Novell-style connections on the station that will act as the BBS server. Sometimes, it's simply easier to put a second network card in your computer, using one card to handle the connection of your machine to your local Lan, and the other card handling the internet connection. This helps us avoid many headaches with some of the more

unconventional Lan networks. The Ethernet cards we suggest people use are the SMC Elite Ultra or the 3COM Etherlink III. We've had very good results with these cards and are very easy to setup and configure.

For an ethernet type of connection, you NEED some sort of routing mechanism. Usually, this involves esoteric pieces of hardware called CSU/DSUs, Frads and routers. Some people use a PC running unix as a router. What all of these devices do is serve as an interface between your computer system or local area network and the internet. They basically act as a "relay station" that take packets from the internet and puts them on your local LAN and vice versa. Routers can differentiate between information which is only local in scope (traffic between two local machines) and global in scope (traffic destined to the internet). The best people to talk to concerning routers is your Internet Service Provider. Usually, it's best to use the equipment they suggest to get optimal technical support from them.

The benefits of ethernet connections is SPEED SPEED and more SPEED. Not only can an ethernet connection handle multi-megabit per second transfer rates, it has the added benefit of giving you the ability of using multiple computers to share the burden of running the BBS. You can use a file server to handle most disk I/O for instance. You can setup a unix machine or a windows-based machine to run a separate Web/FTP server to alleviate some of the burden that was handled mostly by the BBS before. You can even setup some machines running MajorTCP/IP's DMA Server which lets you offload modules from your MajorBBS/Worldgroup system to these secondary computers increasing the overall performance of your BBS. The possibilities are endless.

Finding an internet provider

What is an internet provider? An internet provider is an organization that provides , for a fee a connection from your system to the internet. The fees vary wildly from region to region and we would be hard-pressed to maintain a list of providers as these flicker in and out of existence constantly. Even in Montreal, our home town, several providers have closed down due to the cut-throat competition that exists in this market.

Generally, what you want from an internet provider is some form of dedicated connection to the internet. These can take the form of a simple 28.8k Modem dialup connection using SLIP, CSLIP or PPP, up to a full T1 connection which transfers data at a whopping 1.2 megabits per second. Obviously, the difference in price between the former and the latter can be equally staggering. As far as MajorTCP/IP is concerned, the only thing we require is that the connection to the BBS computer be done either through an **asynchronous serial port OR an ethernet card using the appropriate packet drivers**. The rest is up to you and your provider.

The single most important piece of advice you'll ever need for the selection of a provider is this: **Take the time to shop around.** Most major cities have more than one provider and it is in your best interest to get the best price you can if you want to make the BBS as cost-effective as possible. It is important that you be very careful and research the various providers thoroughly. Sometimes, it may be worth it to pay a little bit more money if it means you're going to deal with a top-notch provider.

It is an unfortunate side effect of market-driven economics, but the fact is, if you live in a remote area, the price charged by most providers will usually be much higher than what you would pay if you lived in a large urban area.

Because MajorTCP/IP gives you the capability of becoming for all intent and purpose a bonafide internet provider, you may also run into providers that will artificially inflate their prices because they know you will cut into their market. Some may even refuse to provide you with services if you offer to your clients certain services (example: SLIP, CSLIP and PPP).

Does the provider offer Primary Domain Name services?

The primary domain name services are one of the fundamental parts required for MajorTCP/IP. The DNS is what serves as the "internet" white pages. Usually, when user wants to connect to another computer, the user asks for a text internet address like gm.gamemaster.qc.ca. The DNS resolver that comes with MajorTCP/IP queries your provider's DNS database to find out the numeric internet address (called the IP address) required before establishing any form of connection with the outside world. If your provider doesn't give you basic DNS services (MCI is one of those companies that don't), this may force you to get a machine on your network running Unix or Linux to serve as your DNS server.

Does the provider offer Sendmail Smarthost services?

A Sendmail Smarthost acts as an E-mail switchboard where incoming mail is sent directly to your BBS while outgoing mail is sent directly to the target sites the e-mail is destined for. MajorTCP/IP comes with it's own built-in Smarthost as of version 1.77 and above. Despite this, having an outside smarthost has one big advantage: Should your system go down temporarily, your provider's Smarthost will keep in storage the mail that is addressed to your system. An added advantage is that having your provider act as the Smarthost reduces some of the load on your system hence, increasing your own system performance.

Does the provider offer News Server services?

Should you provide SLIP, CSLIP or PPP access to your users, these will be able to utilize client programs that run over a TCP/IP stack (such as Trumpet Winsock for windows). Some of these programs act as graphical newsreaders. This means that your users can get their newsfeed off of your provider. Even with the built-in NNTP server, it's doubtful that you will want to carry a full newsfeed. (A full newsfeed means carrying up to 12000 newsgroups, which implies several hundred megabytes worth of messages a day!). Hence, if your clients want to have access to newsgroups that you don't carry, you will need access to an external NNTP server. Usually, most large internet providers carry full feeds.

As of version 1.78-7, MajorTCP/IP comes with a built-in NNTP server. This means that MajorTCP/IP can import Usenet messages directly into your forums. People can reply to messages by E-mail or publicly, they can even include file attachments in some cases which will be UUENCODED or on the Usenet side. You need an NNTP feed from a provider if you want to offer your own Newsfeed. Since the current incarnation of NNTP doesn't support NNRP yet, your clients that are using SLIP/CSLIP/PPP Newsreaders will still need to get their feeds off of your provider's NNTP site.

Can the provider give you a full class C address?

If you are going to provide SLIP or CSLIP access to your clients, you will need a range of IP addresses (apart from the IP address you will get for your own BBS) that will be allocated to your clients when they establish a connection to you via the SLIP/CSLIP/PPP server. In essence, getting a class C address means that you will have access to 254 IP addresses for your own personal use. These addresses will then be "lent" to people through dynamic allocation when they connect to you using Trumpet Winsock or any other TCP/IP stack. A full class C is not essential to provide SLIP/CSLIP/PPP access. Some providers can give you a restricted range of IP addresses for your SLIP/CSLIP/PPP server. You simply won't have the same flexibility in the latter case.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Information you need for MajorTCP/IP

Before setting up MajorTCP/IP, you need to find out a few things from the distributor you purchased the product from and your internet service provider (ISP):

- The MajorTCP/IP activation codes
- The BBS system's IP address
- The Netmask required for your system
- The gateway IP address
- The IP addresses for your primary and secondary domain name servers
- The internet name of your BBS
- The IP address of your Sendmail Smarthost (Required for SMTP)
- The range of IP addresses required for the SLIP/CSLIP/PPP server
- The IP address of your provider's NNTP Server
- Connection information if using a dialup SLIP/CSLIP/PPP connection

The MajorTCP/IP activation codes

Every version of MajorTCP/IP requires a set of activation codes. These can be found either on the diskettes you obtained from your distributor, or on the invoice that came with your purchase. The codes usually go by the name of incoming and outgoing codes. If you purchased a limited version of MajorTCP/IP (restricted to either incoming traffic or outgoing traffic, you will only get one activation code of the appropriate type).

Use this space to write your activation code(s):

Incoming activation code	
Outgoing activation code	

The BBS system's IP address

Each computing piece of equipment that gets connected to the internet requires what's called an IP address (Internet Protocol address) which is a unique identifier for your system. This address is essential because without it, someone on the internet has no way to know where to send any information to you. Your provider is the one that will give you your IP address. The address takes the form of a number delimited by periods.

Example: 199.84.216.2 is the IP address of our support system running on the MajorBBS.

If you are going to provide SLIP/CSLIP/PPP access to your users, it's here that you have to ask your provider to give you a class C address. A class C address means that you'll have access to a range of 254 addresses. For MajorTCP/IP, **the BBS IP address must be a member** of this Class C range. If you cannot obtain a Class C license, your provider may still offer you a range of IP addresses to use with your SLIP/CSLIP/PPP server. This range of addresses must share the same three first numbers as your BBS IP address.

Example: In our case, our provider gave us the whole range between 199.84.216.0 to 199.84.216.254. The BBS IP address must be within that range of IP addresses (as it is in our case for 199.84.216.2).

Your system's IP address	

The Netmask required for your system

The netmask is used as a filtering mechanism between your local network and the global internet. By default, a netmask of 255.255.255.0 is usually what your provider will tell you to use. It's important for you to get the appropriate Netmask from your provider. If you are using a 28.8k dialup type of connection to your provider, a netmask of 255.255.255.0 will be just fine.

Your system's Netmask	

The gateway IP address

The gateway IP address tells MajorTCP/IP which system or router that acts as the connection between your local network and the internet. If you are using a 28.8k SLIP/CSLIP/PPP dialup connection, this information is not required. In most cases, this is an IP address assigned by your provider to your Router, FRAD, or any other piece of equipment that acts as your bridge to the internet.

Your gateway IP address	

The IP addresses for your primary and secondary domain name servers

MajorTCP/IP requires an IP address pointing at your provider's domain name server. A domain name server acts as the local "internet white pages" that converts a textual internet address (like gm.gamemaster.qc.ca for instance) into its numerical equivalent (199.84.216.2). Occasionally, some providers do not offer DNS services, which means you must find other means to make these translations. Usually, this implies setting up a unix machine running the appropriate DNS applications, or a windows-based machine running Name Server software.

The secondary domain name server is an optional item. Should one server fail to translate a textual address into an IP address, the other server acts as a backup. Sometimes, because of the distributed nature of the internet, some servers may have an "incomplete" directory. Having a secondary DNS reduces the chances that such a problem may occur with your system.

Primary DNS address	
Secondary DNS address	Optional

The internet name of your BBS

Every system on the internet has a name associated to it, also known as the "Host's domain name". A typical name is composed of a machine name and an extension (called the top-level domain) which is associated with the type of organization your system operates from or the nationality of the system.

Say you'd like to have a BBS with the name "widgets" as part of the whole domain name. You're running a local LAN and you have other machines that will also require domain names. The top-level domain name you could call anything on your network could be something like "widgets.com". Your BBS on the LAN could then be called "bbs.widgets.com". The machine acting as a separate world-wide-web server could be called "www.widgets.com", and so on and so forth. For a single machine, a two part name is usually best. In fact, if you use the World-Wide-Web server on the BBS, you could even have an ALIAS of a primary name. "bbs.widgets.com" and "www.widgets.com" could both be associated to the same IP address, but this requires you to ask your provider to set it up like that on his side.

In any case, whatever name you chose for your system, this name will eventually need to be registered at the Internic, which takes care of synchronizing the name servers on the internet (ie: keeping the internet white pages up-to-date), which requires you to fill out a form that your provider will give you.

There are generic domains that people use as part of their whole host domain name.

COM	Commercial	MIL	US Military
EDU	Educational	GOV	US government
NET	Internet	ORG	Other organizations

Your BBS (host's) domain name	

The IP address of your Sendmail Smarthost (Required for SMTP)

The IP address of your sendmail Smarthost is only required if you're going to send and receive internet E-mail. As of version 1.77 of MajorTCP/IP and above, the software comes with a built-in sendmail smarthost meaning that this IP address is no longer mandatory for proper electronic mail delivery. In some circumstances however, the use of an external smarthost can be beneficial and the big majority of ISPs provide smarthost facilities.

There are many advantages of having an external sendmail smarthost: Should your system go down temporarily, your provider's Smarthost will keep in storage the mail that is addressed to your system. An added advantage is that having your provider act as the Smarthost reduces some of the load on your system hence, increasing your own system performance.

IP address of your Sendmail Smarthost	Optional

The range of IP addresses required for the SLIP/CSLIP/PPP server

To provide your clients with SLIP/CSLIP/PPP connectivity requires a range of IP addresses that can be allocated either dynamically or staticly to your clients. These IP addresses have to be in the same Class C as your BBS IP address (translation, the first three numbers have to be the same).
If you have a whole class C to yourself, you'll have the addresses from 0 to 254 available. On the other hand, if you don't have a Class C address, it's your provider who will give you a restricted range of addresses. These are only required if you intend on providing SLIP, CSLIP or PPP connectivity.

IP address for SLIP/CSLIP (low end)	Optional
IP address for SLIP/CSLIP (high end)	Optional

The IP address of your provider's NNTP Server

To use the built-in NNTP server, you will need to ask your provider if they can provide you with a Newsfeed using the IHAVE (Aye-Have) protocol. Aside from the newsfeed itself, you'll need to ask your provider to give you the IP address of the NNTP that will feed your system with news. You will also need an IP address where user postings will be forwarded to when these write messages in the Usenet newsgroups. **Another good thing to ask your provider for is the list of all the newsgroups he carries. That way, you'll be able to pick and choose the ones you will want to carry**. Once everything is setup as per the NNTP installation section, you'll hand over to your provider the list of newsgroups you've selected.

IP address for the system that will feed you news	
IP address for the outgoing responses and posts	

Other Information

If you're going to use a SLIP/CSLIP/PPP dialup type of connection via Modem, you will need some additionnal information from your provider:

Basic SLIP/CSLIP/PPP dialup connection

Usually, ISPs will let you have three different types of connections: SLIP, CSLIP or PPP.
You need to know which one you will use, although chances are **that the prefered form of connection will be thru PPP.** Both CSLIP and PPP support Van Jacobson header compression.

Normal packets being sent via a serial connection have a 40 byte header. If somebody uses say, an interactive application where each individual keystroke is sent one packet at a time, that means that for each keystroke typed, 41 bytes are sent. What Van Jacobson header compression does is chop down the headers from 40 bytes to 7 bytes. Reducing the amount of overhead. CSLIP and PPP are always preferable over SLIP.

So here's a list of things you need to know from your provider to establish your connection. You should write the answers down here as this information will be usefull further down in the manual.
If your provider supports PPP, you should find out if he also supports PAP (PPP authentication protocol). This would abolish the necessity of a login script.

1	Type of connection: SLIP, CSLIP or PPP?	
a	If has PPP, does he support PAP?	
2	Phone number of the dialup line	
3	User name that will be used at login	
4	Password used at login	
5	Is it set to disconnect because of inactity?	

Please note that most systems have case sensitive user names and passwords, make sure that you note these down correctly. Furthermore, if you want to avoid constant disconnections due to inactivity, you should ask your provider to disable the feature noted at option 5.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

STEP 2:

Get MajorTCP/IP off of your diskette and on your computer system

This is thankfully the easiest part of the process. The installation program that comes with the module is the standard Galacticomm install program, so you should already be familiar with it's basic layout.

STEP	Description	Done
#1	Place the distribution disk in the floppy drive (drive a: is assumed)	
#2	Type in the following at the DOS prompt: **A:INSTALL**	
#3	When asked for a directory to install the software in, the program defaults to C:\WGSERV which is the Worldgroup default directory. If you are running MajorBBS and are using the C:\BBSV6, you should change the entry accordingly. This also applies if you installed the software in a directory that you named yourself.	

If you downloaded MajorTCP/IP from our support BBS, follow this procedure instead:

STEP	Description	Done
#1	Copy the TCPxxxx.ZIP file to a temporary directory on the same drive as MajorBBS or Worldgroup. (xxxx is usually the version number, ex: TCP185.ZIP)	
#2	Unzip TCPxxxx.ZIP in the directory you created using PKUNZIP or UNZIP.	
#3	Go into that directory and type in the following at the DOS prompt: **INSTALL**	
#4	When asked for a directory to install the software in, the program defaults to C:\WGSERV which is the Worldgroup default directory. If you are running MajorBBS and are using the C:\BBSV6, you should change the entry accordingly. This also applies if you installed the software in a directory that you named yourself.	

Should the installation process fail and MajorTCP/IP interferes with the proper functioning of the BBS, you can deactivate MajorTCP/IP temporarily by deactivating the TCP/IP modules using option **#7: Basic Utilities** in the main configuration menu. You need to use the **BBSDMOD** program if you are running MajorBBS. The equivalent under worldgroup is called **WGSMOD**.

The modules to deactivate temporarily are:

Module name	Filename	Description
TCPLIB	TCPLIB	The protected mode TCP/IP Stack
Rlogin*	TCPRLGN*	Rlogin/Rshell Client module*
Telnet	TCPTELNT	The basic Telnet Client module
FTP	TCPFTP	The FTP Client module
TCP/IP Misc. Functions	TCPMISC	The DNS and Finger server module
TCP/IP SMTP Server	TCPSMTP	The SMTP server module
TCP/IP WWW Server	TCPWWW	The WWW server module
TCP/IP Slip Server	TCPSLIP	The SLIP/CSLIP/PPP server/dialer module
TPC/IP IRC client	TCPIRC	The IRC client for MajorTCP/IP
TCP/IP IdentD Server**	TCPID**	The User Identifier Daemon. Used with IRC.**
TCP/IP NNTPD Deamon	TCPNNTPD	The NNTP Daemon for newsgroups
TCP/IP POP3 Server	TCPPOP3	The POP3 server module
TCP/IP WEB2 Server	TCPWEB2	The new WWW server module (replace TCPWWW)

* There is one module, TCPLIBR that is called by TCPLIB. This module is not selectable from the module activation/deactivation utilities. But it is needed in case you do the procedure manually. TCPLIBR contains the Real mode buffer copy functions (around 1.5k).

** The TCPID module is used in conjunction with TCPIRC. If you activate the IRC module, you should always activate the TCPID module as well.

Notes: upgrading from WG 1.X to WG 2.X or moving away from ICO/AIO

If you're **going from WG 1.00 or WG1.01 to WG2.00**, you need to know that WG2.00 comes with it's own TCP/IP stack dubbed **"ICO-Lite",** which is a no-frills group of TCP/IP connectivity modules that are a small part of the complete **ICO/AIO package** (MajorTCP/IP's main competition). MajorTCP/IP will not co-exist with these "ICO-Lite" features, so it's important that when you do the upgrade, you disable the built-in internet connectivity features of WG2.0. To do this, all you need to do is answer **"NONE"** when queried for the connection type (dialup, TCP/IP or none). This will disable all the modules that are part of the base WG2.00 internet connectivity features.

On the other hand, **if you're already running WG2.00 and are abandoning the full ICO/AIO** connectivity packages, you need to manually run the **GALICOIN** program from the WGSERV directory and answer **"NONE"** when queried for the connection type (dialup, TCP/IP or none). **This will fully disable ICO/AIO**.

If you are running other internet connectivity add-ons with your ICO/AIO or WG2 like Murkwork's Worldsock, Web-Master, Web-Blaster, CGI-Magic, so on and so forth ... you must reinstall them after disabling ICO/AIO/WG2 and installing MajorTCP/IP.

STEP 3:

Configure the MajorTCP/IP core modules

Last Revised September 16th, 1996

- Added Option **TCPMODDF** in TCPLIBM.MSG, level 4 configuration. This option is used to display the location of the user when he is **not** in a MajorTCP/IP module. This is related to the **TCP_RL_MOD text variable** documented in *the **"Text Variables: Changing the /# command to display the Rlogin destination"*** section of the **chapter on Rlogin** (see Table of contents).
- Added Option **TCPGLALS** in TCPLIBM.MSG, level 4 configuration. This option is used to allow use of the GALALIAS alias management that comes with WG2.0 or better, instead of MajorTCP/IPs own alias system. See the **SMTP chapter** of this manual, in the section called ***"Determine which Aliasing scheme you will be using".*** (see Table of contents)

Before establishing the physical connection to your provider, you need to prepare MajorTCP/IP by configuring the BBSMAJOR.MSG and the TCPLIBM.MSG message files that contain the system's startup parameters. These tell the MajorTCP/IP and MajorBBS/Worldgroup the hardware you have on your machine and the various IP addresses the BBS is going to use to know in what fashion it will communicate with the internet.

STEP	Description	Done
#1	Increase the FILES statement in CONFIG.SYS	
#2	Place the TCPLIB, Telnet and Rlogin modules in the menu tree	
#3	Set your Incoming Telnet channels	
#4	Set your Telnet/Rlogin dial-out channels	
#5	Configure the TCPLIBM.MSG parameters	

Increase the FILES statement in CONFIG.SYS

MajorTCP/IP's various modules will need file handles to function properly. These file handles are required to open the various system files internally, and to allow people to access web pages and other services where files are opened to access them. Using a text editor, edit your CONFIG.SYS file and increase the FILES statement by at least 40, If you already have the maximum of handles allocated (254), there shouldn't be any problems.

Place the TCPLIB, TELNET and RLOGIN modules in the menu tree.

For proper MajorTCP/IP operations, you need to add these three modules to your menu tree.

TCPLIB (TCPLIB.DLL) is the module that acts as the protected mode TCP/IP stack, it's the API (application interface) between MajorBBS/Worldgroup and other MajorTCP/IP modules. It makes use of the Telnet, RLogin and TCPLIBR modules. (Note: TCPLIBR shouldn't be put in the menu tree).

Telnet (TCPTELNT.DLL) is the module that acts as MajorTCP/IP's telnet client.

Rlogin (TCPRLGN.DLL) is the module that acts as MajorTCP/IP's RLogin/RShell client

Use the following procedure to add the modules to the menu tree:

- From the main configuration menu (CNF), **select F2 - Design Menu Tree**
- Make sure that the menu item cursor is located on the **TOP page**
- Select **F5 ADD**, when queried for the name, **enter TCPLIB**
- Select **F5 ADD**, when queried for the name, **enter Telnet**

- Select **F5 ADD**, when queried for the name, **enter Rlogin**
- Move the cursor to the **floating TCPLIB page**
    - Press **F2 Edit**
    - Allow go to this page ..... should be set to **YES**
    - Key required ..... should be the **MASTER key**
    - Select module window, you should chose the **TCPLIB module**
    - Display header ..... should be set to **YES**
    - The command string should be left **empty**
- **Repeat the same procedure for the Telnet and Rlogin modules**

Set your Incoming Telnet channels

Incoming Telnet channels are the means by which people on the internet will be able to login to your BBS remotely. Each incoming telnet channel uses up one license off of your galacticomm six-packs. You may need to purchase sufficient numbers of six-packs depending on the maximum number of concurrent incoming telnet users you would prefer. If you do not wish to setup an incoming Telnet channel, you should at least put up one channel for testing purposes while your system is in the configuration phase by using the license of one of your modems.

Use the following procedure to add a Telnet channel group:

- From the main configuration menu (CNF), select **F1 - Hardware configuration**
- At this point, you should be editing the **BBSMAJOR.MSG** parameters.
- Use the **down arrow** key to get to next available channel group.
- Press **F2 - Pick one**
- From the **Channel Group Type window**, select **TELNET**
- Starting channel number should be the **next one available** (per the last channel group)
- Number of channels as desired, as long as you don't run out of six-pack licenses.
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu.

Set your Telnet/Rlogin dial-out channels

Telnet/RLogin dial-out channels are used to disguise Telnet/RLogin sessions to look like a normal Modem connection, allowing your BBS to connect to other services via the internet, saving you hundreds of dollars in long-distance or X.25 costs. Specifically, you can use them to run various connectivity add-ons that weren't designed to work with MajorTCP/IP. (Worldlink, Chatlink, Interlink, Maillink, Entertainment Teleconference Link-up, Galacticomm's Dial-out module). Each dial-out channel uses up a license out of your Galacticomm six-packs.

Use the following procedure to add a Telnet/RLogin Dial-Out channel group:

- From the main configuration menu (CNF), select **F1 - Hardware configuration**
- At this point, you should be editing the **BBSMAJOR.MSG** parameters.
- Use the **down arrow** key to get to next available channel group.
- Press **F2 - Pick one**
- From the Channel group type window, select **MODEM**
- Starting channel number should be the **next one available** (per the last channel group)
- Number of channels as desired, as long as you don't run out of six-pack licenses.
- I/O base adress .....should be skipped (down arrow)
- Maximum baud rate ..... skip
- Lock port at this baud rate ..... skip
- Echo keystrokes to this channel ..... skip
- Hardware type, you should **press F5** for **TELOUT**
- Offset between channels ..... skip
- Init String should be left as is or you could replace it with ATZ
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu

When a third party module requires you to enter a channel and dialing string to use, you can tell it to use one of the dialout channels and this dialing string: **ATDT<numeric IP adress>[:port][R]**

Example:	**ATDT199.84.216.1**	**(Connect to default port 23 in telnet mode)**
	ATDT199.84.216.1:2500	**(Connect to port 2500 in telnet mode)**
	ATDT199.84.216.1R	**(Connect to default port 23 in RLogin mode)**
	ATDT199.84.216.1:2500R	**(Connect to port 2500 in Rlogin mode)**

Configure the TCPLIBM.MSG parameters

The TCPLIBM.MSG parameters describe the low-level behavior of the MajorTCP/IP interface. We will only deal here with the parameters that are essential prior to establishing your connection to your provider. We assume that you correctly filled out the "**Information you need for MajorTCP/IP**" section from pages 23 to 26. You will sometimes see parameters that aren't mentionned in this part of the manual. Simply skip over them and alter only those that are mentionned in the following list.

Level 1 - Hardware Configuration

- From the main configuration menu (CNF), select **F1 - Hardware configuration**
- Press on **F8 - Search**, type **MYIPADDR.**
- You should find yourself at the **MYIPADDR** Item in the **TCPLIBM.MSG** file.
- Edit each item as described below, moving from item to item using the arrow keys
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu

MYIPADDR
0.0.0.0
This is **your system's IP address**, noted down on **page 23 of this manual**. Simply type it in using the dotted format seen in all the examples so far in this manual.

NETMASK
255.255.255.0
This is **your system's Netmask**, noted down on **page 24 of this manual**. Enter it in dotted format, or use the default 255.255.255.0 if you are connected to your provider via a SLIP or CSLIP dialup connection. **This option will not be visible if you are using the SLIP/CSLIP/PPP dialer (SLIPINT set to YES)**.

GATEWAY1
0.0.0.0
This is **your system's Gateway address**, noted down on **page 24 of this** manual. Enter it in dotted format. If you are connected to your provider via a SLIP or CSLIP dialup connection, you should put an IP address of 0.0.0.0 instead. **This option will not be visible if you are using the SLIP/CSLIP/PPP dialer (SLIPINT set to YES)**

MSS
1400
Maximum Segment Size. This parameter tells MajorTCP/IP the size of the packets the software will use to transmit data to and from the provider. By default, the MSS is set to 1400. That means that any packet transmitted will be of that size (or less), regardless of the size of the item being transmitted. For instance. A file being download via FTP of 512 kilobytes will be received in 1400 bytes chunks. In general, you should not change this value unless we've told you via Tech Support.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Sometimes, it may be desirable to reduce the MSS. One of the basic premises of TCP/IP packets is the ability to handle multiple users sharing the same line. The way the TCP/IP protocol does this is by bundling the information into discrete chunks called packets. Each packet carries information about who generated the packet and who this packet is destined to. One of the limiting factors on the internet is inter-packet delay. If you have large packets, say, 1400 bytes long and your connection is a 28.8k SLIP dialup for instance, that means that a user telnetting to a remote site say, like a MUD (Multi-User Dungeon), sharing the line with another user getting a file via FTP will probably see his keystrokes slow down, as each keystroke must wait for the FTP user's next packet to pass by. Even at 28.8k, waiting for 1400 bytes to get through can take a good fraction of a second. Although in this example, the problem would be hardly noticeable, if you add even a few more Telnet users and one or two FTP users, the lag between keystrokes will become pronounced.

The solution to this problem is to a) increase the bandwidth (ie: drop the 28.8k modem connection to the provider and go for a faster link) or b) reduce the MSS. Smaller packets means less inter-packet delay. This benefits interactive sessions like Telnet and Rlogin which are keystroke by keystroke clients, while penalizing the high speed data transmission clients like FTP. Usually, this means that the sysop should experiment with different values of the MSS ranging from 256 to 1400 to find a happy medium.

PRIDNS 0.0.0.0

This is **your system's Primary Domain Name server address**, noted down on **page 24 of this manual**. Enter it in dotted format. You need a Primary DNS server address if you want your users to be able to telnet out using the target systems host name instead of a numeric IP adress. If the DNS fails in this case, MajorTCP/IP will automatically attempt to resolve the adress using the Secondary Domain Name Server. Enter 0.0.0.0 if you do not wish to define a primary Domain Name Server.

SECDNS 0.0.0.0

This is **your system's Secondary Domain Name server address**, noted down on **page 24 of this manual**. Enter it in dotted format. It serves the same function as the Primary DNS server, but can be left to 0.0.0.0 if none were provided to you. If MajorTCP/IP fails to resolve an adress via the Secondary Domain Name Server, it will automatically switch back to the Primary DNS.

NBTCP

Maximum number of concurrent TCP sessions supported.

The NBTCP OPTION was removed. We leave the description of NBTCP simply as an educational tool. NBTCP is now computed automatically by the application so it no longer requires that you set it by hand. Should you exceed your user count in terms of TCP Handles, or run out of memory, you will be warned of this fact.

Depending on which version of MajorTCP/IP you purchased, the maximum number of TCP sessions will vary from 64 to 1024 in the "unlimited" version. Each session allocate what's called a **TCP Handle**. In Unix, people call these "*Sockets*". Each of these sessions require 5K of extended memory. You are therefore limited by the amount of memory you have and the type of MajorTCP/IP license you have. The MajorTCP/IP combo version gives you up to 256 TCP Handles. The "Unlimited" version provides you with 1024. The Outgoing-Only version of MajorTCP/IP and the DMA Server provide you with 64 TCP Handles.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Here is the list of MajorTCP/IP services and the number of TCP Handles they consume:

Item	TCP Handles consumed
Incoming Telnets	1 per Telnet channel (BBSMAJOR.MSG)
Outgoing Telnets	1 per session (non-hardware)
Incoming Rlogins	1 per Telnet channel (BBSMAJOR.MSG)
Outgoing Rlogin	1 per session (non-hardware)
Telnet/RLogin Dialouts	1 per TELOUT channel (BBSMAJOR.MSG)
FTP sessions	2 per FTP Session (non-hardware)
Finger Connections	1 per session (Max=FINMAX, TCPMISC.MSG)
DNS Resolution	1 per resolution (used till resolution ends)
WWW page hits	1 per hit (Max=WWWMAX, TCPWWW.MSG)
Incoming SMTP Mail	1 per session (Max=SMTPMAX, TCPSMTP.MSG)
Outgoing SMTP Mail	1 per session (Max=SMTPMAXO, TCPSMTP.MSG)
Incoming NNTP feed	1 per feed. (Max=NNTPMAX, TCPNNTDP.MSG)
Outgoing NNTP feed	1 per feed. Always one export session at a time.
IRC usage	1 per session, 2 if user is doing a DCC connection
POP3 usage	1 per sexxion (Max=POP3MAX, TCPPOP3.MSG)
SLIP/CSLIP/PPP session	None

Non-hardware channels are channels that don't use up licenses from your Galacticomm six-packs. Note that FTP, Finger, DNS, WWW, SMTP and SLIP/CSLIP/PPP type of connections are non-hardware.

TCPIRLG
YES

Should MajorTCP/IP accept incoming Rlogin connections.
MajorTCP/IP can be set to automatically accept rlogin calls as well as telnet calls. If you set this option to yes, the incoming telnet channels will accept telnet and rlogin calls. If you set to no, only telnet calls will be accepted.

TCPNEBUF
50

Number of Packet Buffers. You can specify here how many buffers you wish to alloacte for packet processing. The more buffers you allocate, the higher the performance of the software. Each buffer requires 2100 bytes of extended memory, and defaults at 50. If your system experiences performance problems, you can increase this value up to 1024.

HOSTNAME and DOMNAME

This is where you specify the Internet name of your system (host's domain name). Refer to **page 24 of this manual**. The name of the parameters are somewhat of a misnomer in this case. The **HOSTNAME** field refers to your system's unique identifier while the **DOMNAME** field refers to the high level domain name used on your system. Say your BBS is called **widgets.com**. Your **HOSTNAME** would be **widgets**, while **DOMNAME** would be **com.**

On the other hand, if your BBS is part of a local LAN that has as a **high-level domain name widgets.com**, and you'd like to call your BBS **bbs.widgets.com**, you could then put in the **HOSTNAME** field the word **bbs**, and the words **widgets.com** in the **DOMNAME** field.

The combination of HOSTNAME and DOMNAME is used by the SMTP E-mail system. A user on your system called john would thus have an E-mail address of **john@bbs.widgets.com** as per the second example.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Level 3 - Accounting and Security configuration

- From the main configuration menu (CNF), select **F3 - Accounting and Security**
- Press on **F8 - Search**, type **ACTCODE**.
- You should find yourself at the **ACTCODE** item in the **TCPLIBM.MSG** file.
- Edit each item as described below, moving from item to item using the arrow keys
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu

ACTCODE This is **MajorTCP/IPs outgoing activation code**. When you purchased the <empty> product, you should've received activation codes written on your diskette's label or on your invoice. If you didn't receive these, you should call your distributor. MajorTCP/IP will not function without these codes. The outgoing activation code is **required for the Outgoing-Only and Combo versions**. Leave empty if you have the DMA server or you are running the Incoming-Only version of MajorTCP/IP. **You should find the activation code on page 24 of this manual.**

ACTICODE This is **MajorTCP/IPs incoming activation code**. When you purchased the <empty> product. MajorTCP/IP will not function without the proper codes. The incoming activation code is **required for the Incoming-Only and Combo versions**. Leave empty if you have the DMA server or you are running the Outgoing-Only version of MajorTCP/IP. **You should find this activation code on page 24 of this manual.**

KEYOLOC This is a mandatory key that must be set to give users access to MajorTCP/IP
NORMAL services on the local network. (ie: this key will let people Rlogin or telnet to machines that are on your Local area network). By default, this key is set to **NORMAL** (every valid user can use these services). Note: applies only to outgoing Telnet, Rlogin and FTP.

KEYOREM This key is also mandatory. This one tells us if the user has access to outside
NORMAL connections, ie: it determines if the user can Telnet or Rlogin to the outside world. This is dependant on the NETMASK specified earlier. By default, this key is set to **NORMAL** (every valid user can use these services). Note: applies only to outgoing Telnet, Rlogin and FTP.

NOTE about KEYOLOC and KEYOREM

If you plan to give the KEYOREM key to paying users while normal users get the KEYOLOC key (so they can use local resources like a local Unix box for instance). Make sure that the users who own the KEYOREM key also own the KEYOLOC key. This is important because if say, a paying user with the KEYOREM key tries to use a resource on your local network, he will not be able to unless he owns the KEYOLOC key as well.

SUROLOC **Surcharge in credits/minute for a local connection**.
0 If a user tries to use a MajorTCP/IP connection to systems on the local area network, you can specify how much you wish to charge him OVER the basic system charges (hence, a surcharge). By default, we don't charge anything extra for local connections. Note, this amount will be added to the basic charges, but it's quite possible that certain particular services can be set to surcharge over this primary surcharge.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Example: say you charge 60 credits per minute for basic usage. Any usage of MajorTCP/IP services can have a base surcharge of say 10 credits (You set SUROLOC to 10). If the person then decides to use FTP, you could add another 10 credit surcharge defined in the FTP module (set FTPRAT to 10, later in this manual). The bottom line, the person would then be charged 80 credits per minute for FTP.

SUROREM **Surcharge in credits/minute for a remote connection.**
0 This is the same as the SUROLOC parameter but involves people going onto the global internet. Chances are, you will not apply a surcharge at all for using MajorTCP/IP services on the local Lan, but will charge for connections beyond the Lan.

MajorTCP/IP is now ready to be configured for connection and testing.

Level 4 - Configuration Options

- From the main configuration menu (CNF), select **F4 - Configuration Options**
- Press on **F8 - Search**, type **DNSTMO**.
- You should find yourself at the **DNSTMO** item in the **TCPLIBM.MSG** file.
- Edit each item as described below, moving from item to item using the arrow keys
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu

NOTE These parameters are here mainly to make this manual complete. Under normal circumstances, you should never have to change these parameters except for fine-tuning purposes. The default values used here will work fine for the vast majority of installations. Please consult Vircom's technical support by E-mail if you wish to change something or have questions about certain values.

DNSTMO **DNS Query timeout in seconds**
10 If no responses are received after an interval of DNSTMO seconds, Major TCP/IP will automatically revert to the other name server. If no response is still received for the DNSTMO period, the query will fail. The value you can put here ranges from 5 to 60 seconds.

NBRES **Number of DNS resolution buffers**.
20 Each "hostname resolution buffer" takes about 818 bytes of extended memory. You can specify here how many resolution buffers should be defined. This controls the number of hostname resolution processes that can be active concurrently. You can allocate from 5 to 100 resolution buffers.

DSPINC **Record incoming IP address in audit trail.**
YES This option controls wether the IP address of Telnet callers is to be recorded in the audit trail. You may want to turn off this feature if most of your traffic comes from incoming Telnets, turning it on only if you want to trace someone who is causing you problems (hacking attempts for instance).

ECHGRP **Turn off echo of which channel group**
0 This allows you to turn echo off on a specific channel group. You can select channel groups 1 thru 16. Leave at 0 to disable.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

TCPTMO **TCP Level Inactivity Time Out in minutes (0=Disable).**
30 This is a low level inactivity timeout, it will terminate any _incoming_ TCP connection that will not have had activity on it after TCPTMO minutes. Set to 0 to disable. Maximum allowed time is 1000 minutes.

BANMODE **Use TCPSITES.BAN to list allowed sites**.
NO You can define a TCPSITES.BAN file to list of sites that are not allowed any connectivity with the BBS. Or you can set BANMODE to yes, and use the TCPSITES.BAN file to list the sites that CAN communicate with the BBS. If you do so, only the listed sites can have any sort of connectivity with the BBS. The TCPSITES.BAN file can be created with a simple text editor. On each line, put the IP address of the site you want to ban (BANMODE=NO) or allow (BANMODE=YES). This feature lets you stop hacking attempts from a particular IP if your system finds itself under attack. The TCPSITES.BAN file has to be located in your BBS directory (WGSERV/BBSV6).

TICKMS **Maximum duration of a TCP/IP tick (in milliseconds) (0 to disable)**
40 This is the maximum duration of a MajorTCP/IP Cycle, in (approximative) milliseconds. After MajorTCP/IP spends that much time servicing TCP/IP packets, control will be returned to next user needing service. (Enter 0 to disable). Should be at least 20 if set. Increasing TICKMS will favor the performance of your internet connectivity suite by penalizing general BBS performance. Consult technical support before changing this value.

LOCSPC **Should local incoming calls go to TELALT group?**
NO You can have MajorTCP/IP direct incoming Rlogin/Telnet calls that are originating from your LAN into a specialchannel group, TELALT (instead of TELNET). Setting LOCSPC to YES enables this option. This lets you isolate incoming telnets from a local unix box or terminal server from the calls coming in from the internet, for instance. This allows you to bill people who are using your local resources differently from those who Telnet in from the internet.
You can use LOCSPC with incoming FTP sessions as well with the new FTP Server.

LOCSPCM **Should calls from the BBS go in TELALT too?**
YES You may want to make an exception for Telnet/Rlogin calls that are coming _from_ the BBS, back into the BBS (users who are connected via SLIP/CSLIP/PPP for instance that Telnet back in using Worldgroup Manager). This allows you to decide if you want them to go into the normal TELNET channel group or in the TELALT channel group. **This option is visible only if LOCSPC is set to YES**. **You can use LOCSPCM with incoming FTP sessions as well with the new FTP Server.**

LOGWRT **Keep log file closed.**
YES Starting with v1.77-1 of MajorTCP/IP, MajorTCP/IP specific logs are grouped within one file. Each module has a toggle that can be used to enable or disable the log. Option LOGWRT defines if the LOG is always kept closed, with buffer flushed, or (for better speed), kept opened and buffer flushed only when the BBS is brought down. Note that if the file is always left open, you cannot view the log file while the BBS is up and operating using the SYSOP remote DOS function TYPE.

LOGPTHF **MajorTCP/IP log path and filename.**
tcplogf.log You enter here the path and filename for the MajorTCP/IP log file. If you leave this blank, logs are disabled. If no path is specified, the file will be saved in the BBS directory (WGSERV or BBSV6).

REDIRSUP **Enable handling of ICMP Redirect Packets?**
NO ICMP redirects are sent by routers, when dynamic routing changes have to inform the BBS that the path to a destination address changed. You only need this if you have _multiple_ routers on your LOCAL area network, and then again only in special cases. It is very safe (and reccomended) to leave this option at NO.

TCPMODDF **Default Module Text Variable**
<Empty> If you are using the TCP_RL_MOD text variable, you can use this option to specify which text variable will be used when a user is not in one of the modules that use TCP_RL_MOD. This would be used, for example, when you are using a module that display different module names when users are in different menu pages. **Warning: This option is currently experimental.**

TCPGLALS **Use GALALIAS for Internet Aliases in MajorTCP/IP**
NO Set **TCPGLALS to YES** if you want all of MajorTCP/IP's modules to use Galacticomm's GALALIAS module for aliases. This should only be set to YES if you're running WG2.0 or above.

NOTE: if you set this to YES, all of MajorTCP/IP's alias features are disabled and replaced by the ones in GALALIAS. RLogin USEMGI and MGIWRT and SMTP's USEALIAS settings will now be ignored. You should not use the RLogin "alias" sysop menu anymore.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

STEP 4:

Configure MajorTCP/IP to talk to the net

Last updated January 20th, 1997

- Added ESC command to scripting for the Modem dialup connections using the SLIP/CSLIP/PPP dialer connections. Lets the dialing script send a single escape character to the target system.

In this chapter, we will discuss five methods to establish your connection to the net:

- **Modem Dialup** connection using the internal **SLIP/CSLIP/PPP** dialer
- **Modem Dialup** connection using the **SLIPPER/CSLIPPER** drivers
- **Ethernet** connection using **TCP/IP packet drivers**
- **Novell network** using the **ODI packet drivers**
- Using a **secondary** Ethernet **card** with MajorTCP/IP
- Dedicated **serial hookup** through the internal **SLIP** dialer

Modem Dialup connection using the internal SLIP/CSLIP/PPP dialer

NOTE: Instead of constantly referring to the SLIP/CSLIP/PPP dialer, we will call the dialer simply the SLIP dialer. This is done simply to save paper bandwidth.

The automatic SLIP dialer emerged as an offshoot of our SLIP server that allows people to connect to your system via trumpet winsock and use client software such as Netscape, Mosaic, Free Agent and a myriad of other Windows-based clients. If the SLIP server was used to turn your BBS into a SLIP/CSLIP/PPP connectivity provider, why couldn't we adapt the module to serve the same function for your connection to your own provider? The SLIP server was modified to do just that.

Because you need the SLIP/CSLIP/PPP Server to use the built-in dialer**,** this feature is only available with the MajorTCP/IP combo version. Furthermore, the SLIP dialer was introduced with version 1.76-2 of MajorTCP/IP. Should you be using a version prior to that, the SLIP dialer function simply isn't available. The SLIP dialer replaces the old SLIPPER/CSLIPPER drivers, which required manual maintenance of the connection. If the SLIP dialer is unavailable to you, you can use these drivers to establish your connection instead.

Because of the introduction of PPP in version 1.81 as a connection protocol offered by the SLIP server, chances are that you will favor the PPP route to the SLIP or CSLIP route. Most of the instructions apply to all protocols. Differences will be noted in the rest of this section.

Because the SLIP dialer uses a modem from one of your modem channel groups, it uses up one of your licenses from a Galacticomm six-pack. The modem should be connected to a port that has a 16550 UART chip. Hardware flow control should be enabled for your particular brand of modem. Most Hayes-compatible modems use the &K3 in the initialisation string. You must also make sure that the cable connecting the modem to the port supports hardware flow control.

How the SLIP/CSLIP/PPP dialer works

- Dials up your provider using a modem in your modem pool.
- Sends your user name, password and any other text required via a script file. -OR- **if using PPP, assuming your provider supports PAP, you can do the same thing without a script file by configuring the PPPPAP, PPPUID and PPPPWD parameters.**
- Waits for the SLIP/CSLIP/PPP connection to be completed.
- Once the link is up, it monitors the connection constantly.
- Should the connection drop, it resets the modem and starts the process over.

NOTES about PPP

PPP is now supported by MajorTCP/IP. PPP stands for Point-to-Point protocol which is the new protocol kid on the block. Performance-wise, PPP is similar to CSLIP in terms of raw speed. However, PPP supports new features that make using it a breeze. Contrary to SLIP or CSLIP, you don't need a special script to establish the connection to your provider. PPP's big bonus comes from two new features added to this protocol:

Authentication Protocol (PAP): This feature is also supported in the PPP dialer, removing the need for any script to connect to your Internet Service Provider (I.S.P.). UserID and Password information is entered in CNF fields. If the I.S.P. doesn't support this feature, the traditionnal login script can be used instead.

Addresses negotiation: The IP and DNS addresses negotiation is also supported in the PPP dialer. This means that your BBS can now use a dynamic IP address, although this will essentially prevent anyone from reaching your BBS. (Imagine how easy it would be to reach someone randomly changing phone number.)

Using PPP as link with your provider - Summary

PPP is simpler to setup than SLIP or CSLIP. The procedure goes as follows and is detailled in the "Setting up the Internal SLIP/CSLIP/PPP dialer" section of this chapter.

- **Make sure that the SLIP/CSLIP/PPP server is enabled.** You need to verify if **SLIPENAB** in **TCPSLIP.MSG**, level 4 configuration is set to **YES.**

- **Make sure that the PPP features of the SLIP/CSLIP/PPP server are enabled**. This means making sure that **PPPENAB is set to YES** in **TCPSLIP.MSG**, level 4 configuration.

- **Configure TCPLIBM.MSG file**. This includes all of the parameters that are normally set for SLIP and CSLIP. The only difference is that you need to set **SLIPMOD to PPP**, and **if your provider allows PAP connections**, you have to set **PPPPAP to YES**, and input your **username (PPPUID)** and **password (PPPPWD)** used to login into your account at your provider's site**.**

- **If your provider does indeed provide PAP with his PPP connection:** you can omit creating a script file to connect to your provider**. If you're upgrading from an older version of MajorTCP/IP and already use a script file for a SLIP or CSLIP connection, you'll need to rename the TCPDIAL.SCR file to TCPDIAL.SCV file (delete the TCPDIAL.SCV file if it already exists before hand).**

- **If, on the other hand, your provider DOESN'T offer PAP connections, simply use the instructions here to create an appropriate script file.**

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Setting up the internal SLIP/CSLIP/PPP dialer

STEP	Description	Done
#1	Enable the SLIP/CSLIP/PPP Server	
#2	Configure the TCPLIBM.MSG file for the Internal SLIP/CSLIP/PPP Dialer	
#3	Edit the TCPDIAL.SCR script file to work with your provider's prompts if not using **PAP with PPP**.	

Enable the SLIP/CSLIP/PPP Server

To use the SLIP Dialer, we must first enable the SLIP/CSLIP/PPP Server. Simply follow these steps to bring the SLIP/CSLIP/PPP Server online for SLIP dialing.

- From the main configuration menu (CNF), select **F4 - Configuration Options**
- Press on **F8 - Search**, type **SLIPENAB.**
- You should find yourself at the **SLIPENAB** item (**TCPSLIP.MSG**) , set it to **YES**.
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu.

In addition, if you want to use PPP for your connection:

- From the main configuration menu (CNF), select **F4 - Configuration Options**
- Press on **F8 - Search**, type **PPPENAB.**
- You should find yourself at the **PPPENAB** item (**TCPSLIP.MSG**) , set it to **YES**.
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu.

Configure the TCPLIBM.MSG file for the Internal SLIP Dialer

Aside from basic IP information, some of the TCPLIBM.MSG parameters are used to program the behavior of the SLIP dialer. Below is the list of parameters to configure with explanations associated with each.

SLIP dialer Configuration

- From the main configuration menu (CNF), select **F1 - Hardware configuration.**
- Press on **F8 - Search**, type **SLIPINT**.
- The first item you should find is the **SLIPINT** parameter, in the **TCPLIBM.MSG** file.
- Edit each item as described below, moving from item to item using the arrow keys
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu

SLIPINT NO — This parameter tells MajorTCP/IP to use the internal SLIP Dialer. **By default, this option is set to NO**. Simply **change it to YES to enable the dialer**. Should the option be left to NO, all the other parameters associated with the SLIP dialer won't be visible. If you've been a long time owner of MajorTCP/IP and are simply activating the SLIP dialer in lieu of the SLIPPER/CSLIPPER serial port drivers, please remember to remove them from normal BBS activation.

SLIPMOD
SLIP

Slip dialer mode. This setting simply tells MajorTCP/IP which type of connection you will use with your provider. You should've obtained this information from your provider. **You can select either SLIP, CSLIP or PPP. PPP is the prefered connection method.** Check out **page 26** of this manual in the "what you need to know" section. **By default, this parameter is usually set to use SLIP. This parameter will not be visible if SLIPINT is set to NO.**

SLIPCH
0

Modem channel number used for the SLIP dialer. The SLIP dialer uses a a modem from one of your modem channel groups. If this parameter is set to the **default of 0**, MajorTCP/IP will not attempt to dial up your provider. This channel number is in hexadecimal the same way as they are defined in the Channel Group definition section of the BBSMAJOR.MSG file, and as seen on your system console. Ultimately, it's strongly suggested that you define a separate channel group for the modem you will be using to establish the connection to your provider. **This parameter will not be visible if SLIPINT is set to NO. This parameter applies for SLIP, CSLIP and PPP connections.**

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

SLIPDIAL
ATDT2222222

Dialing string. By default, this dialing string is set to **ATDT2222222,** simply change the 2's to the phone number noted down on **page 26 of this manual**. If you are using pulse lines to save money, simply change the ATDT command to ATDP. To dial our system locally here, we use the ATDT6872210 command. **This option will not be visible if SLIPINT is set to NO. This parameter applies for SLIP, CSLIP and PPP connections.**

SLIPWAIT
5

Redial delay in minutes. This value tells MajorTCP/IP to wait the specified number of minutes before redialing your provider after a disconnection. By default, the value is set to 5. It may be good to set this value to 1 for testing purposes. **This option will not be visible if SLIPINT is set to NO. This parameter applies for SLIP, CSLIP and PPP connections.**

SLIPCON
connect

Modem connect string. This tells MajorTCP/IP what connect string to expect when the connection is finally established. The default string is "**connec**t" (without the quotes). This string should work for most sites. **This option will not be visible if SLIPINT is set to NO. This parameter applies for SLIP, CSLIP and PPP connections.**

PPPPAP
YES

Use PAP to login to your provider.
The PPP dialer can login into your provider's PPP account in two ways. The first method is by using a script, the same way it would be done for a SLIP or CSLIP connection. The second is by using PAP, a PPP protocol that supports authentication. If you wish to use PAP (and your provider's system support it, see **page 26** if you did get confirmation of this fact), set **PPPPAP to YES. This option applies only for PPP connections, furthermore, this option is only visible if SLIPMOD is set to PPP.**

PPPUID
username

Enter UserID for PAP.
Enter the UserID for PAP. This is the userID you use to login into your PPP account on your provider's machine. If your provider cannot handle PAP, you should use the TCPDIAL.SCR script instead to send your username to his machine. **This option applies only for PPP connections, furthermore, this option is only visible if PPPPAP is set to YES.**

PPPPWD
password

Enter Password for PAP.
Enter the Password for PAP. This is the password you use to login into your PPP account on your provider's machine. If your provider cannot handle PAP, you should use the TCPDIAL.SCR script instead to send your username to his machine. **This option applies only for PPP connections, furthermore, this option is only visible if PPPPAP is set to YES.**

SLIPPING
0

Ping DNS how often (seconds) to keep link alive.
Some ISP (internet service providers) are stubborn and don't want to remove their inactivity timeouts on SLIP/CSLIP/PPP connections. This will make your link to your internet disconnect every so often, if there is no TCP/IP activity on your BBS. The re-dialer will reconnect, but this is still annoying. By setting SLIPPING to a number of seconds that is smaller than your provider's inactivity timeout, MajorTCP/IP will ping your primary DNS every SLIPPING seconds. As this is "activity", no timeout will be able to occur. Set SLIPPING to 0, to disable. **This option is visible only if SLIPINT is set to YES.**

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Edit the TCPDIAL.SCR script file to work with your provider's prompts

***NOTE* Ignore this step if you're using PPP with PAP.**

Once the TCPLIBM.MSG file is properly configured, the next step is to edit the **TCPDIAL.SCR** file located in your BBS directory. (usually \WGSERV or \BBSV6 depending on your setup). This file **MUST** be customized to work with your provider's screen prompts. The script language is very simple and consists of 4 commands.

DBUG Tells MajorTCP/IP to turn on script debugging. More information will be printed in the audit trail.

SEND <text> The SEND command tells MajorTCP/IP to send the characters specified to your modem. SEND adds a carriage return at the end of the <text> that you've specified. If you use SEND without any text, MajorTCP/IP will simply send a carriage return.

WAIT <text> The WAIT command waits up to 60 seconds for the case-sensitive <text> to be received from your modem. If the text is never received, the script will be aborted with a message in the audit trail. Otherwise, MajorTCP/IP proceeds to the next statement in the script file.

ESC The ESC command lets you send a single escape (ASCII character decimal 27) to the system you are attempting to connect to.

Any line that starts with the pound sign is used to add comments to the script file. Any text on that line following the pound sign will be ignored by MajorTCP/IP.

The TCPDIAL.SCR file contains a sample script used to login to a standard unix box. To find out exactly what your provider's prompts look like, you should use a terminal program like Telix or Procom and connect to your provider manually. It's a good idea to turn on the capture buffer and print out the file on paper afterwards. Here is a sample connect session to a typical provider and how we translate that to a functionning script file.

```
Welcome to the Widgets Unix system running Linux.
Login: JohnDoe
Password: Apassword4fun

SL/IP connection from 199.84.216.2 to 199.84.216.128 beginning ....
```

Here is the resulting script file:

```
DBUG
WAIT Login:
SEND JohnDoe
WAIT Password:
SEND Apassword4fun
WAIT beginning
```

Here is the same script file with commentary:

```
DBUG

# We tell MajorTCP/IP to log everything in the audit trail for debugging

WAIT Login:

# Wait for the login prompt.  Should the word at the wait statement be incorrect,
# MajorTCP/IP will timeout and will be indicated thus in the audit trail.
# Usually, this is caused by a typo at the wait statement.

SEND JohnDoe

# After receiving the Login: prompt, MajorTCP/IP is told to SEND the user name,
# in this case, JohnDoe.  Unix systems are usually case sensitive, so it's very important
# to send the user name exactly as it was given, including appropriate case.

WAIT Password:

# Wait for the Password prompt.  The same rules apply here as they do at the login prompt.

SEND Apassword4fun

# After receiving the Password: prompt, MajorTCP/IP is told to SEND the Apassword4fun
# password.  Again, because of the case-sensitivity of Unix systems, you should make sure
# that the password being sent is exactly the same as the one you chose, including the
# appropriate case of each character.

WAIT beginning

# Wait for an indication that we've made it thru the password request.  If the script gets
# to this point after execution, chances are that the connection is indeed working.  If for
# some reason, the script doesn't make it to this point, the culprit is usually an error in
# the previous two WAIT/SEND combinations.  Check your username and password if
# they've been properly entered
```

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Modem Dialup connection using the SLIPPER/CSLIPPER drivers

***NOTE* Skip this section if you're already using the internal SLIP dialer**.

Prior to the creation of the internal SLIP dialer, people used the SLIPPER.EXE and CSLIPPER.EXE serial TCP/IP packet drivers to establish a connection to their providers. Since then, most people today use the SLIP dialer. In some cases though, those who do not own the combo version (incoming or outgoing only versions of MajorTCP/IP) use this method to connect to their internet provider**. You cannot use SLIPPER and CSLIPPER for PPP connections.**

The advantages of using SLIPPER and CSLIPPER instead of the SLIP dialer:

- Does not use a hardware channel, meaning you don't lose a license from a six-pack.
- Because the 28.8k modem uses a non-hardware channel, it does not affect the polling rate.

The disadvantages of using SLIPPER and CSLIPPER over the SLIP dialer:

- Need to connect manually using a communications program (Telix, Procomm, ...)
- No way to detect a connection drop from the BBS to the provider.
- No way to re-establish the connection automatically if the carrier drops.
- The drivers eat up some of your low memory.
- For partial automation, necessary to write a script for the communication program used.
- Must use a modem on com 1 to com 4, cannot use other ports.
- Rebooting required after a disconnection.

As you can see, the disadvantages of using SLIPPER and CSLIPPER outweigh by far the few advantages gained. The only real advantage you gain is if you are using a 28.8k modem for your connection to your ISP, while you only have 14.4k modems for your user dial-ins. If your 28.8k modem was part of the defined channels, it would increase your polling rate by a factor of two, halfing your system's performance. This is only if you are restricted to slower modems on your normal channels. Since people are putting more and more 28.8k modems in their modem pools, this is rapidly becoming a non-issue.

The modem you will use for the SLIP/CSLIP connection to your provide MUST be connected to one of the four original com ports (ie: com1 to com4). In addition, the port used needs a 16550 UART chip. Hardware flow control should be enabled for your particular brand of modem. Most Hayes-compatible modems use the &K3 in the initialisation string, you may want to verify this by looking it up in your modem's manual. You must also make sure that the cable connecting the modem to the port supports hardware flow control (it has the CTS/RTS pins).

At **page 26 of this manual**, you should've noted down if your provider can let you use SLIP or CSLIP for your dialup connection. If you are using SLIP, the driver you will need is called SLIPPER.EXE. If your provider can offer you CSLIP instead, you can use the CSLIPPER.EXE which is functionally identical to SLIPPER.EXE. Internally, it uses Van Jacobson Header compression, which reduces much of the overhead associated with TCP/IP packets, increasing the efficiency of your link. CSLIP is thus preferable to use over SLIP. Note that these drivers are in the SLIPPR15.ZIP file that you find in your BBS directory once MajorTCP/IP is installed.

Setting up and using the SLIPPER/CSLIPPER drivers

STEP	Description	Done
#1	Cofigure the TCPLIBM.MSG file to use SLIPPER/CSLIPPER	
#2	Pace the SLIPPER.EXE/CSLIPPER.EXE driver where it can be found	
#3	Follow the standard connection procedure for SLIPPER/CSLIPPER	

Configure the TCPLIBM.MSG file to use SLIPPER/CSLIPPER

You need to make sure that MajorTCP/IP will be able to talk to the SLIPPER/CSLIPPER driver that will be loaded in memory later on. To do this, we must make certain that a pair of parameters are set correctly.

TCPLIBM.MSG configuration for SLIPPER/CSLIPPER

- From the main configuration menu (CNF), select **F1 - Hardware configuration**
- Press on **F8 - Search**, type **SLIPINT.**
- The first item you should find is the **SLIPINT** parameter.
- You should set **SLIPINT** to **NO**.
- Use the **down arrow** to find the item called **TCPINT**
- You should set **TCPINT** to **0**.
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu.

SLIPINT
NO — This parameter tells MajorTCP/IP to use the internal SLIP Dialer. **By default, this option is set to NO**. This is the proper setting for SLIPPER/CSLIPPER usage.

TCPINT
0 — **This is the software interrupt number** that will bind SLIPPER/CSLIPPER with MajorTCP/IP. If you leave it to 0, MajorTCP/IP will automatically find which interrupt number has been reserved by SLIPPER/CSLIPPER and will bind to it. Normally, the number ranges between 0x60 to 0x80 in hexadecimal. Should you forget to bring up SLIPPER/CSLIPPER, the system will catastro with a “Packet driver not found” message. In some cases, you may need to specify explicitely which Interrupt number you are using with SLIPPER and CSLIPPER. For instance, if you are using a local TCP/IP network but wish to get a 28.8k dialup connection to your provider. This means you’re going to have a TCP/IP packet driver on your machine while running SLIPPER or CSLIPPER, which could confuse MajorTCP/IP. To avoid this problem, you must tell MajorTCP/IP which interrupt number SLIPPER/CSLIPPER uses. **This option is visible only if SLIPINT is set to NO.**

Place the SLIPPER.EXE/CSLIPPER.EXE driver where it can be found

- Extract SLIPPER.EXE and CSLIPPER.EXE from the SLIPPR15.ZIP file. Zip files are compressed using Pkware’s PKZIP utility. To extract the programs from the zip file, simply type at the dos command prompt: **PKUNZIP SLIPPR15.ZIP. You can find the SLIPPR15.ZIP file in your BBS directory after you’ve installed MajorTCP/IP on your Hard disk.**

- Copy SLIPPER.EXE or CSLIPPER.EXE into your root directory OR simply place the current location where these are located in the PATH statement of your autoexec.bat. For instance, if you unzipped the SLIPPR15.ZIP file in the \WGSERV directory, you could add the directory to your PATH statement.

Follow the standard connection procedure for SLIPPER/CSLIPPER

Using SLIPPER or CSLIPPER to establish a connection to your provider is a fairly simple procedure. It requires the use of a communcations program like Telix, Procomm, Qmodem or any other terminal program available on the market. You could even automate the process by writing a script file for the communications program you use and call it up from the autoexec.bat file. This is left up to you. The procedure for a normal manual connection goes as follows:

1) **Start your communications program** with an init string that contains the switch to activate Hardware Flow Control known as CTS/DTS (&K3 on most Hayes-Compatible modems). The baud rate you use should be set between 19200 (if using a 14.4k modem) to 38400 (using a 28.8k modem).

2) Once connected, **login into your SLIP account**. Feed the system your username, password and any other procedure you need to do to login appropriately.

3) **Exit the terminal program without hanging up**. This step is important, do not confuse this with the shell out to dos command. The communications program must be totally removed from RAM.

4) **Start SLIPPER or CSLIPPER** (depending on your provider's available connection mode specified on **page 26** of this manual). Here is the parameter list that SLIPPER and CSLIPPER accept. The parameters can be entered in any order.

SLIPPER [com<digit 1-4>] [vec=<hex vector>] [baud=<speed>] [ether] [nohwhs] [?]

com<digit 1-4>	Which com port to use. If unspecified, defaults to com1 **com1** base=3F8, irq=4 **com2** base=2F8, irq=3 **com3** base=3E8, irq=4 **com4** base=2E8, irq=3
port=<hex port>	Override the com port setting (0000-FFFF)
irq=<hex digit>	Override the com irq setting (0-F)
vec=<hex vector>	The packet driver interrupt vector default is 60 (see **TCPINT**)
baud=<speed>	Baud rate of the connection, default is the current speed setting.
ether	Simulate ethernet board. (IP & ARP only) default is non-ethernet
nohwhs	Disable hardware handshakes.
keepalive	Enable a once per minute keep alive byte to be transmitted.
?	Display the commands.

Examples: SLIPPER com1 baud=38400
Tells slipper to use com1 at the 38400 baud rate (28.8k modem)

The parameters are exactly the same for CSLIPPER.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

When SLIPPER or CSLIPPER are loaded in memory, it should tell you if you are using a 16550 uart. If you aren't, or if your CTS/RTS (harware flow control) isn't turned on for the articular modem you are using, you will be getting **JUNK PACKETS** message in the audit trail.

5) **Start the BBS**.

It should be possible for you to automate the whole process by writing a script file for the communcations program you use. You can then put this in your autoexec.bat file. During the cleanup process, the BBS would then reboot and redial automatically. Unfortunately, if the connection fails at any point during the day, it's impossible for SLIPPER or CSLIPPER to detect the deconnection. This means that you should monitor regularly your connection.

Example of an autoexec.bat file modified to use a telix script and slipper:

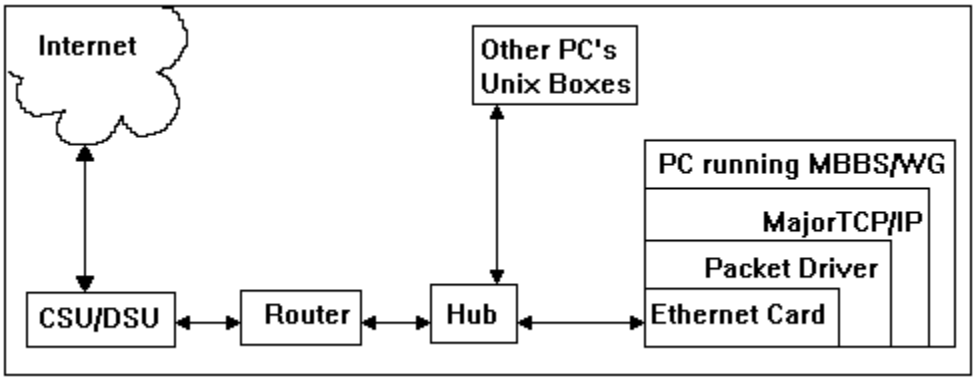
```
rem ------- Starting telix ----------------------------------------------------------------------------
rem start telix with a login script called login.slc that initialises the modem, establishes
rem the connection with the provider and automatically feeds the username, password and
rem other parameters to start up SLIP on his side.
TELIX SLOGIN.SLC
rem ------- Start slipper on com2, for a 28.8k modem. ------------------------------------------
slipper com2 baud=38400
rem ------- Start worldgroup immediately ------------------------------------------------------
cd \wgserv
wg go
```

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Ethernet connection using TCP/IP packet drivers

Most people who get a high-speed connection for the first time take this route because it's the simplest to setup. No file server required, no messy network softare to configure. All you need is the native TCP/IP packet driver that comes with your ethernet card.

Here is a typical connection diagram:



Your setup may differ slightly. Some people use a FRAD instead of a CSU/DSU. Some people have a device that incorporates the functionality of both a CSU/DSU and a router. Some setups utilise 10 base 2 coaxial loops to a single machine (the BBS) directly from the router to the PC using AUI transceivers to coax. Some have an ISDN bridge connecting the incoming ISDN line to a PC running Unix that acts as a router for the whole network. The possibilities are endless and are out of the scope of this manual. The best people to talk to concerning network architecture are your provider and a TCP/IP network specialist. They can point out to you the best hardware to purchase and the most economical architecture for your particular setup.

To make the BBS communicate to the internet whatever form the underlying architecture of the network takes, you must be able get MajorTCP/IP talking the ethernet card. As in the diagram, the packet driver serves as the bridge between the Ethernet Card and MajorTCP/IP.

90% of our current clients employ these three Ethernet cards and their associate driver:

Card name	Packet Driver	Parameters
3COM Etherlink III	3C5X9pd.com	[options] <packet_int_no> [id_port][io_port][board_number]
NE2000	ne2000pd.com	[options] <packet_int_no> <int_level> <io_addr>
SMC8000	pkt8000.com	[options] <packet_int_no> [<int_no> <io_addr> <mem_addr>]

Setting up and using an Ethernet packet driver for TCP/IP connectivity

STEP	Description	Done
#1	Configure the TCPLIBM.MSG file for the ethernet packet driver	
#2	Locate the packet driver on your ethernet card's diskette	
#3	Configure your Ethernet card	
#4	Put the packet driver in your AUTOEXEC.BAT file for loading	

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Configure the TCPLIBM.MSG file for use with an Ethernet Packet driver

You need to make sure that MajorTCP/IP will be able to talk to the Ethernet packet driver that will be loaded in memory later on. To do this, we must make certain that a pair of parameters are set correctly.

Configuration for an Ethernet type of connection via a TCP/IP network

- From the main configuration menu (CNF), select **F1 - Hardware configuration**
- Press on **F8 - Search**, type **SLIPINT.**
- The first item you should find is the **SLIPINT** parameter.
- You should set **SLIPINT** to **NO**.
- Use the **down arrow** to find the item called **TCPINT**
- You should set **TCPINT** to **0**.
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu.

SLIPINT NO — This parameter tells MajorTCP/IP to use the internal SLIP Dialer. **By default, this option is set to NO**. This is the proper setting if you intend to use an Ethernet packet driver.

TCPINT 0 — **This is the software interrupt number** that will bind the packet driver to MajorTCP/IP. If you leave it to 0, MajorTCP/IP will automatically find which interrupt number has been reserved and will bind to it. Normally, the number ranges between 0x60 to 0x80 in hexadecimal. Should you forget to bring up the appropriate packet driver, the system will catastro with a "Packet driver not found" message. **This option is visible only if SLIPINT is set to NO.**

Locate the packet driver on your ethernet card's diskette

You can usually find the packet driver for your particular card on the diskette that came with it. If you fail to find it, you should call up the manufacturer of the card to be pointed in the right direction. In any case, you may want to contact the manufacturer anyway to find out if you have the most recent version of the packet driver. You must specify that you need a **TCP/IP packet driver**, not to be confused with the NOVELL ODI drivers. Once you've located the packet driver, you should copy it in a directory that is searched by DOS thru the the **PATH** statement of your **AUTOEXEC.BAT** file.

Configure your Ethernet card.

You should make sure that your ethernet card is not in conflict with any other card if you are running a TCP/IP network thru the same hub. You should refer to your card's documentation to learn how to do this. Note down the appropriate configuration parameters.

Put the packet driver in your AUTOEXEC.BAT file for loading

You've found the packet driver, you've installed the card in your PC. It's time to load the packet driver in memory using the **AUTOEXEC.BAT** file. The packet driver should be loaded just before you start your MajorBBS/Worldgroup system. If you are using **QEMM or any other memory manager**, you should use the **EXCLUDE** statement (or the equivalent) to **prevent an overwrite** of the driver's loading adress. Here is an extract from an AUTOEXEC.BAT file containing a call for the SMC8000's packet driver (PKT8000.COM). Note that the parameters will vary from card to card. You should consult the card's documentation to find out which are needed. Once ready, boot up the system. MajorTCP/IP should be talking to your card now.

```
rem ------- Load the SMC8000 packet driver. ------------------------------------
pkt8000 0x7E 11 0x240 0xC800
rem  0x7E      Software interrupt for the packet driver (associated with TCPINT) in hex
rem  11        Interrupt number (IRQ) used by the card
rem  0x340     I/O adress in hexadecimal
rem  0xC800    Memory adress the packet driver will be loaded in
cd \wgserv
go
```

Novell network using the ODI packet drivers

Many people often go to the Novell Network route, where the incoming internet line hooks up into the system's hub. Basically, Novell and the internet are sharing the same wiring. The trick here is to disguise your standard ODI drivers used for ferrying traffic using the IPX/SPX protocols to act as a packet driver for MajorTCP/IP. You should use an Ethernet card with its ODI drivers installed in the same fashion as any other station on your Novell network. But what's different is what we will explain here.

Setting up for ODI Ethernet using both TCP/IP and ODI on the same board

STEP	Description	Done
#1	Configure the TCPLIBM.MSG file for the ethernet ODI packet driver	
#2	Locate the ODIPKT driver-shim	
#3	Modify your NET.CFG (Net Config) file	
#4	Modify your STARNET.BAT or AUTOEXEC.BAT files	

Configure the TCPLIBM.MSG file for the ethernet ODI packet driver.

You need to make sure that MajorTCP/IP will be able to talk to the ODI packet driver that will be loaded in memory later on. To do this, we must make certain that a pair of parameters are set correctly.

Configuration for an ODI Ethernet type of connection via a Novell network

- From the main configuration menu (CNF), select **F1 - Hardware configuration**
- Press on **F8 - Search**, type **SLIPINT.**
- The first item you should find is the **SLIPINT** parameter.
- You should set **SLIPINT** to **NO**.
- Use the **down arrow** to find the item called **TCPINT**
- You should set **TCPINT** to **0**.
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu.

SLIPINT
NO
This parameter tells MajorTCP/IP to use the internal SLIP Dialer. **By default, this option is set to NO**. This is the proper setting if you intend to use a Novell ODI packet driver.

TCPINT
0
This is the software interrupt number that will bind the packet driver to MajorTCP/IP. If you leave it to 0, MajorTCP/IP will automatically find which interrupt number has been reserved and will bind to it. Normally, the number ranges between 0x60 to 0x80 in hexadecimal. Should you forget to bring up the appropriate packet driver, the system will catastro with a "Packet driver not found" message. **This option is visible only if SLIPINT is set to NO**

Locate the ODIPKT driver-shim

The ODIPKT.COM driver shim is located in your BBS directory (WGSERV or BBSV6 depending on which program you are running). You should copy it either in your NWCLIENT directory (or any other directory where you keep your netware client drivers), or at least put it somewhere accessible by DOS via the PATH statement.

Modify your NET.CFG (Net Config) file

The first step is to prepare your NET.CFG to handle TCP/IP traffic. To do so, we need to add a few lines to it. We assume that you already have configured your machine to serve as an ordinary station on your network and have thus created a NET.CFG file for it. At the top of the NET.CFG file, you should add a Link Support section in the following fashion:

```
Link Support
        Buffers 6 1600
```

Note the indentation of the Buffers statement. That indentation should not be omitted. The program that parses the net.cfg file expects this. The buffering is required for proper TCP/IP packet handling.

As part of the Link Driver section, you should add two framing classes. These frame types are what lets your do TCP/IP over an IPX/SPX network.. They should appear as follows in the Link Driver section:

```
Link Driver XXXXXXXX        <-- this line is here only as a visual aid
        ... card configuration  <-- ditto here too
        ... other frame types   <-- and here
        Frame Ethernet_802.3
        Frame Ethernet_II
```

It's important to note the position of the **Frame Ethernet_II** framing class. In this example, it's the second frame in the frame list. It's possible that you have a few frames already (like Frame Ethernet_802.2 or Frame Ethernet_SNAPS). In the latter case then, frame Ethernet_II would then be the fourth frame in the list as in this example:

```
Link Driver XXXXXXXX        <-- this line is here only as a visual aid
        ... card configuration  <-- ditto here too
        Frame Ethernet_802.2
        Frame Ethernet_SNAPS
        Frame Ethernet_802.3
        Frame Ethernet_II
```

It's important to know the position of the Ethernet_II because ODIPKT needs to bind with this framing class. To do this, we tell ODIPKT to bind to the nth frame where n is the position -1 of the Ethernet_II frame. So in the STARTNET.BAT file or AUTOEXEC.BAT file, we would use **ODIPKT 3** if the latter example was true in our NET.CFG.

Modify your STARNET.BAT or AUTOEXEC.BAT files

You should now add ODIPKT.COM to your STARTNET.BAT or AUTOEXEC.BAT depending on which one you use to load your network drivers. Lets assume you're using STARTNET.BAT and that the NET.CFG file was configured exactly like in the last example of the previous section. (Frame Ethernet_II is the 4th frame). You should change directories to the appropriate one where STARTNET.BAT is located when it's called from the AUTOEXEC.BAT.

```
LSL
<MLID>          <-- Your ODI driver
IPXODI
NETX            <-- Or VLM depending on what version of Novell you are running
ODIPKT 3
```

Combined sample of NET.CFG and STARTNET.BAT

NET.CFG on C:\NWCLIENT

```
spx connections=127                 | Preliminary setup stuff for this network
show dots=on                        |

Link Support                        | Link support section that we added
    Buffers 6 1600                  | as per the instructions

Link Driver 3C59X                   | 3COM Etherlink III ODI driver
    FRAME Ethernet_802.3            | Load our first required frame
    FRAME Ethernet_II               | Load our second required frame

NetWare DOS Requester               | More stuff for this particular network
    FIRST NETWORK DRIVE = H         | Primary network drive is drive H
    NETWARE PROTOCOL = NDS BIND
    preferred server = olp
```

STARTNET.BAT on C:\NWCLIENT

```
SET NWLANGUAGE=ENGLISH              | Define the language used by netware
C:\NWCLIENT\LSL.COM                 | Load the LSL link support drivers
C:\NWCLIENT\3C5X9.COM               | Startup the ODI driver for the 3COM
C:\NWCLIENT\IPXODI.COM              | Load IPXODI
C:\NWCLIENT\VLM.EXE                 | Load VLM (Personnal Netware)
C:\NWCLIENT\ODIPKT 1                | Load ODIPKT, Frame Ethernet_II is the
H:LOGIN WG1                         |    second item, hence n = 1.
```

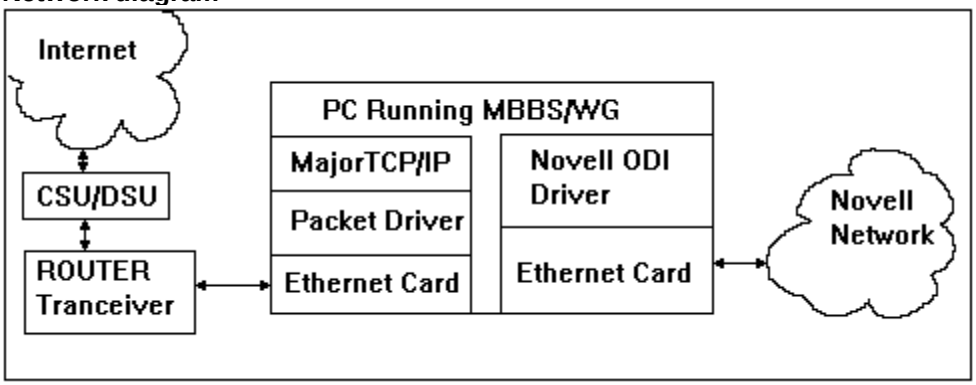
[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Using a secondary Ethernet card with MajorTCP/IP

Because MajorTCP/IP cannot talk to certain networks like Lantastic or Windows-based networks **unless these systems can emulate Novell by using the Novell ODI drivers**, a solution had to be found to make MajorTCP/IP work despite this limitation. Sometimes, even people running a Novell setup prefer to have the TCP/IP connections limited to only a few machines, while the IPX/SPX network stays isolated. This is often used as a security measure when the data on the network is sensitive in nature.

The solution is to simply install a second network card in your machine over the first. This way, the primary card acts as the connection to the local Lan, making it possible for the BBS to access the file server. The secondary card acts as the connection to the internet. Because both cards are doing totally unrelated things, there is no conflict. An interesting result of such a setup is that you effectively create a firewall between the internet and your local network. This means that, should you decide to isolate users on your local LAN by making the BBS the only machine connected to the TCP/IP link, nobody on the internet will be able to see your LAN. Not letting the rest of your LAN talk TCP/IP has one drawback: Users on the LAN will not be able to take advantage of the world-wide-web.

Network diagram



Please note that this example uses a NOVELL network combined with an independant internet connection. In fact, we could be running any sort of network. It doesn't matter. The point is that it's possible to have MajorTCP/IP talking to the internet independently from the LAN used, if we isolate this connection using a second network card.

To setup the secondary card requires an installation practically identical to setting up a single card for an Ethernet connections using the TCP/IP packet drivers. (**check out pages 49 to 50 in this manual**).

90% of our current clients employ these three Ethernet cards and their associate driver:

Card name	Packet Driver	Parameters
3COM Etherlink III	3C5X9pd.com	[options] <packet_int_no> [id_port][io_port][board_number]
NE2000	ne2000pd.com	[options] <packet_int_no> <int_level> <io_addr>
SMC8000	pkt8000.com	[options] <packet_int_no> [<int_no> <io_addr> <mem_addr>]

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Configuration of the secondary network card using the standard TCP/IP drivers

STEP	Description	Done
#1	Examine the current network configuration on the machine	
#2	Loate the packet driver on your ethernet card's diskette	
#3	Configure your Ethernet card	
#4	Modify your STARTNET.BAT or AUTOEXEC.BAT	
#5	Configure the TCPLIBM.MSG file for the secondary ethernet card's driver	

Examine the current network configuration on the machine.

Because there's an almost limitless number of network setups, it's best we just use the Novell example we started with earlier. For any kind of network though, it's safe to assume that the first card designated to talk to the Lan has it's drivers loaded from the **AUTOEXEC.BAT** file (or in the case of Novell, the **STARTNET.BAT** file). For this example, we'll be using the following Novell STARTNET.BAT file:

STARTNET.BAT on C:\NWCLIENT

SET NWLANGUAGE=ENGLISH	**| Define the language used by netware**
C:\NWCLIENT\LSL.COM	**| Load the LSL link support drivers**
C:\NWCLIENT\SMC8000.COM	**| Startup the ODI driver for SCM8000**
C:\NWCLIENT\IPXODI.COM	**| Load IPXODI**
C:\NWCLIENT\NETX.EXE	**| Load NETX Novell Client**
H:LOGIN WG1	**| Login to the H: drive**

Locate the packet driver on your ethernet card's diskette.

You can usually find the packet driver for your particular card on the diskette that came with it. If you fail to find it, you should call up the manufacturer of the card to be pointed in the right direction. In any case, you should contact the manufacturer to make sure you have the most recent version of their packet driver. You must specify that you need a **TCP/IP packet driver**, not to be confused with the NOVELL ODI drivers. Once you've located the packet driver, you should copy it ina directory that is searched by DOS thru the the **PATH** statement of your **AUTOEXEC.BAT** file.

Configure your Ethernet card.

You should make sure that your secondary ethernet card will not conflict with your primary card. It's also important to make sure that it will not conflict with any other piece of hardware that connects to the TCP/IP side of your network. You should refer to your card's documentation to learn how to do this. Note down the appropriate configuration parameters.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Modify your STARTNET.BAT or AUTOEXEC.BAT

You've found the packet driver, you've installed the card in your PC. It's time to load the packet driver in memory using either the **AUTOEXEC.BAT** or **STARNET.BAT** files. The packet driver should be loaded right after you loaded the primary card's set of drivers and before you start up your MajorBBS/Worldgroup system. If you are using **QEMM or any other memory manager**, you should use the **EXCLUDE** statement (or the equivalent) to **prevent an overwrite** of the driver's loading adress.

Using the Novell example defined earlier, we will modify the STARTNET.BAT to load up the packet driver for the secondary card, in this case, the SMC8000. Note that both the primary and secondary cards are identical. This is not a necessity. If using different cards, the parameters will vary accordingly. You should consult the card's documentation to find out which are needed.

STARTNET.BAT on C:\NWCLIENT

SET NWLANGUAGE=ENGLISH	**Define the language used by netware**
C:\NWCLIENT\LSL.COM	**Load the LSL link support drivers**
C:\NWCLIENT\SMC8000.COM	**Startup the ODI driver for SCM8000**
C:\NWCLIENT\IPXODI.COM	**Load IPXODI**
C:\NWCLIENT\NETX.EXE	**Load NETX Novell Client**
pkt8000 0x6A 11 0x240 0xC800	**Load the packet driver for second card.**
H:LOGIN WG1	**Login to the H: drive**

Notes about pkt8000 0x6A 11 0x340 0xc800

0x6A Software interrupt for the packet driver (associated with **TCPINT**) in hex.
11 Interrupt number (IRQ) used by the card.
0x340 I/O adress in hexadecimal
0xC800 Memory adress the packet driver will be loaded in

Each parameter specified above MUST be different from the ones specified for the primary card used for the Lan connection.

Configure the TCPLIBM.MSG file for the secondary ethernet card's driver

You need to make sure that MajorTCP/IP will be able to talk to the Ethernet packet driver that will be loaded in memory later on. A problem occurs though when we try to load drivers for two cards if the other card is also setup to talk TCP/IP. There's a possibility that MajorTCP/IP will bind to the primary card instead of the second card because the TCP/IP driver for the primary card is using one of the software interrupts between 0x60 and 0x80. So we must specify explicitely which software interrupt the secondary card's driver will use so MajorTCP/IP binds to the correct card. To do this, we must make certain that a pair of parameters are set correctly.

Configuration for an Ethernet type of connection via a TCP/IP network

- From the main configuration menu (CNF), select **F1 - Hardware configuration**
- Press on **F8 - Search**, type **SLIPINT.**
- The first item you should find is the **SLIPINT** parameter.
- You should set **SLIPINT** to **NO**.
- Use the **down arrow** to find the item called **TCPINT**
- You should set **TCPINT** to **0** unless the primary card also talks to a TCP/IP stack. If this is the case, **TCPINT** should have **the hexadecimal value selected for the software interrupt of the secondary card (in the example, we're going to use 6A).**
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu.

SLIPINT
NO

This parameter tells MajorTCP/IP to use the internal SLIP Dialer. **By default, this option is set to NO**. This is the proper setting if you intend to use an Ethernet packet driver.

TCPINT
0

This is the software interrupt number that will bind the packet driver to MajorTCP/IP. If you leave it to 0, MajorTCP/IP will automatically find which interrupt number has been reserved and will bind to it. Normally, the number ranges between 0x60 to 0x80 in hexadecimal. Should you forget to bring up the appropriate packet driver, the system will catastro with a "Packet driver not found" message. **In the case of a setup where we have more than one ethernet card in the machine AND both cards use a TCP/IP stack, we must specify which software interrupt to bind with. Because of this, we must specify explicitely which interrupt MajorTCP/IP must bind with. In the example, we're using 6A. This option is visible only if SLIPINT is set to NO.**

Booting the system at this point will load the drivers for the Lan connection. Additionally, MajorTCP/IP will now recognize the packet driver for the secondary card. Assuming everything is hooked up correctly, MajorTCP/IP will be able to talk to the internet while the BBS can use the Lan's file server. Each card functionning independently.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Dedicated serial hookup through the internal SLIP/CSLIP/PPP dialer

NOTE: Instead of constantly referring to the SLIP/CSLIP/PPP dialer, we will call the dialer simply the SLIP dialer. This is done simply to save paper bandwidth.

This is a new feature added to version 1.78-4 that lets you use the SLIP dialer to create serial SLIP/CSLIP/PPP connections to a unix box or a remote system. Some service providers are now offering ISDN hookups that connect directly to your serial port. The ISDN gateway/hookup can act a combined ISDN modem and router, converting the outgoing signal to SLIP/CSLIP or PPP.

Another use you can make of this capability is to setup a very no-frills network between your BBS and Unix box using SLIP/CSLIP/PPP as your communications protocol, and a serial null-modem connection as the hardware medium. You should read the section about normal SLIP Dialer usage to get a good idea about the procedure described here **(pages 38 to 43)**.

IMPORTANT Serial links, as opposed to ethernet links are tied to the BBS'es polling rate. This means that if you hook up to a 128k ISDN link thru a serial port, you will radically decrease the performance of your system. To give you a good idea, say your polling rate is equal to 1 unit with 28.8k modems. Adding a 128k link will QUADRUPLE the polling rate, meaning that the performance will go down by a factor of four. This is because you're using a hardware channel that is tied to the polling rate. Ethernet Cards used to connect to the internet do not affect the polling rate because they are non-hardware channels. Thus, you would be much better off to get an ISDN bridge that will convert the signal from ISDN to Ethernet, and put an Ethernet card in your machine instead. You can then follow the installation steps described earlier for TCP/IP packet drivers using ethernet cards. Another problem with serial links and high speed connections is the fact that Galacticomm limits the speed to 57600 bits per second. Should you connect a 64k ISDN or 128k ISDN connection thru your serial port, you'll lose 10% of your bandwidth in the first case, and over half your bandwidth in the second.

Since you need the SLIP Server to use the built-in SLIP dialer**,** this feature is only available with the MajorTCP/IP combo version. Furthermore, the serial capability of the SLIP dialer was introduced with version 1.78-4 of MajorTCP/IP. Should you be using a version prior to that, the serial SLIP mode of the dialer function simply isn't available.

Because of the introduction of PPP in version 1.81 as a connection protocol offered by the SLIP server, chances are that you will favor the PPP route to the SLIP or CSLIP route. Most of the instructions apply to all protocols. Differences will be noted in the rest of this section.

Instead of using a modem for our connection, we are simply connecting a serial device directly to your PC. Instead of using a MODEM channel group, we'll be using a SERIAL channel. In either case, this will use up a licence from a Galacticomm six-pack. The serial port should have a 16550 UART chip.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

How the SLIP/CSLIP/PPP dialer works over a serial link:

- Establishes a connection to your dedicated line via SERIAL channel
- Sends your user name, password and any other text required via a script file*. -OR- **if using PPP, assuming your provider supports PAP, you can do the same thing without a script file by configuring the PPPPAP, PPPUID and PPPPWD parameters.**
- Waits for the SLIP/CSLIP connection to be completed.
- Once the link is up, it monitors the connection constantly.
- Should the connection drop, it resets the modem and starts the process over.

*** If necessary. All you may require is an empty SEND statement.**

NOTES about PPP

PPP is now supported by MajorTCP/IP. PPP stands for Point-to-Point protocol which is the new protocol kid on the block. Performance-wise, PPP is similar to CSLIP in terms of raw speed. However, PPP supports new features that make using it a breeze. Contrary to SLIP or CSLIP, you don't need a special script to establish the connection to your provider. PPP's big bonus comes from two new features added to this protocol:

Authentication Protocol (PAP): This feature is also supported in the PPP dialer, removing the need for any script to connect to your Internet Service Provider (I.S.P.). UserID and Password information is entered in CNF fields. If the I.S.P. doesn't support this feature, the traditionnal login script can be used instead.

Addresses negotiation: The IP and DNS addresses negotiation is also supported in the PPP dialer. This means that your BBS can now use a dynamic IP address, although this will essentially prevent anyone from reaching your BBS. (Imagine how easy it would be to reach someone randomly changing phone number.)

Using PPP as link with your provider - Summary

PPP is simpler to setup than SLIP or CSLIP. The procedure goes as follows and is detailled in the "Setting up the Internal SLIP/CSLIP/PPP dialer" section of this chapter.

- **Make sure that the SLIP/CSLIP/PPP server is enabled.** You need to verify if **SLIPENAB** in **TCPSLIP.MSG**, level 4 configuration is set to **YES.**

- **Make sure that the PPP features of the SLIP/CSLIP/PPP server are enabled**. This means making sure that **PPPENAB is set to YES** in **TCPSLIP.MSG**, level 4 configuration.

- **Configure TCPLIBM.MSG file**. This includes all of the parameters that are normally set for SLIP and CSLIP. The only difference is that you need to set **SLIPMOD to PPP**, and **if your provider allows PAP connections**, you have to set **PPPPAP to YES**, and input your **username (PPPUID)** and **password (PPPPWD)** used to login into your account at your provider's site**.**

- **If your provider does indeed provide PAP with his PPP connection:** you can omit creating a script file to connect to your provider**. If you're upgrading from an older version of MajorTCP/IP and already use a script file for a SLIP or CSLIP connection, you'll need to rename the TCPDIAL.SCR file to TCPDIAL.SCV file (delete the TCPDIAL.SCV file if it already exists before hand).**

- **If, on the other hand, your provider DOESN'T offer PAP connections, simply use the instructions here to create an appropriate script file.**

Setting up the internal SLIP/CSLIP/PPP dialer for a direct serial link

STEP	Description	Done
#1	Enable the SLIP/CSLIP/PPP Server	
#2	Create a SERIAL channel in the BBSMAJOR.MSG file	
#3	Configure the TCPLIBM.MSG file for the Internal SLIP/CSLIP/PPP Dialer	
#4	Edit the TCPDIAL.SCR script file to work with your provider's prompts	

Enable the SLIP/CSLIP/PPP Server

To use the SLIP Dialer, we must first enable the SLIP/CSLIP/PPP Server. Simply follow these steps to bring the SLIP/CSLIP/PPP Server online for the SLIP serial connection.

- From the main configuration menu (CNF), select **F4 - Configuration Options**
- Press on **F8 - Search**, type **SLIPENAB.**
- You should find yourself at the **SLIPENAB** item (**TCPSLIP.MSG**) , set it to **YES**.
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu.

In addition, if you want to use PPP for your connection:

- From the main configuration menu (CNF), select **F4 - Configuration Options**
- Press on **F8 - Search**, type **PPPENAB.**
- You should find yourself at the **PPPENAB** item (**TCPSLIP.MSG**) , set it to **YES**.
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu.

Create a SERIAL channel in the BBSMAJOR.MSG file

You need to create at least ONE channel for a SERIAL type of connection.

Use the following procedure to add a serial channel group:

- From the main configuration menu (CNF), select **F1 - Hardware configuration**
- At this point, you should be editing the **BBSMAJOR.MSG** parameters.
- Use the **down arrow** key to get to next available channel group.
- Press **F2 - Pick one**
- From the Channel group type window, select **SERIAL**
- Starting channel number should be the **next one available** (per the last channel group)
- Number of channels, we suggest one, make sure you don't run out of six-pack licenses.
- I/O base adress ..... Per the COM port type.
- Maximum baud rate ..... Speed of the dedicated link
- Lock port at this baud rate ..... YES
- Echo keystrokes to this channel ..... NO
- Hardware type, if one of the normal ports, SINGLE, if not, MULTI
- Offset between channels ..... As per port offset
- Dialing string ..... Leave it blank.
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu

Configure the TCPLIBM.MSG file for the Internal SLIP Dialer

Aside from basic IP information, some of the TCPLIBM.MSG parameters are used to program the behavior of the SLIP dialer. Below is the list of parameters to configure with explanations associated with each. Only those parameters used over the serial connection are specified. Some parameters only apply to PPP links, these are also noted in each parameter.

SLIP dialer Configuration

- From the main configuration menu (CNF), select **F1 - Hardware configuration.**
- Press on **F8 - Search**, type **SLIPINT**.
- The first item you should find is the **SLIPINT** parameter, in the **TCPLIBM.MSG** file.
- Edit each item as described below, moving from item to item using the arrow keys
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu

SLIPINT
NO
This parameter tells MajorTCP/IP to use the internal SLIP Dialer. **By default, this option is set to NO**. Simply **change it to YES to enable the dialer**. Should the option be left to NO, all the other parameters associated with the SLIP dialer won't be visible. If you've been a long time owner of MajorTCP/IP and are simply activating the SLIP dialer in lieu of the SLIPPER/CSLIPPER serial port drivers, please remember to remove them from normal BBS activation.

SLIPMOD
SLIP
Slip dialer mode. This setting simply tells MajorTCP/IP which type of connection you will use with your provider. You should've obtained this information from your provider. **You can select either SLIP, CSLIP or PPP. PPP is the prefered connection method.** Check out **page 26** of this manual in the "what you need to know" section. **By default, this parameter is usually set to use SLIP. This parameter will not be visible if SLIPINT is set to NO.**

SLIPCH
0
Modem channel number used for the SLIP dialer. The SLIP dialer uses a one of your serial ports designated in one of your SERIAL channel groups. If this parameter is set to the **default of 0**, MajorTCP/IP will not attempt to talk to your dedicated link. This channel number is in hexadecimal the same way as they are defined in the Channel Group definition section of the BSMAJOR.MSG file, and as seen on your system console. Ultimately, it's strongly suggested that you define a separate channel group the SERIAL port you will be using to create the link to your provider. **This option is visible only if SLIPINT is set to YES.**
provider. **This parameter applies for SLIP, CSLIP and PPP connections.**

SLIPWAIT
5
Redial delay in minutes. This value tells MajorTCP/IP to wait the specified number of minutes before redialing your provider after a disconnection. By default, the value is set to 5. It may be good to set this value to 1 for testing purposes. **This option will not be visible if SLIPINT is set to NO. This parameter applies for SLIP, CSLIP and PPP connections.**

PPPPAP
YES
Use PAP to login to your provider.
The PPP dialer can login into your provider's PPP account in two ways. The first method is by using a script, the same way it would be done for a SLIP or CSLIP connection. The second is by using PAP, a PPP protocol that supports authentication. If you wish to use PAP (and your provider's system support it, see **page 26** if you did get confirmation of this fact), set **PPPPAP to YES. This option applies only for PPP connections, furthermore, this option is only visible if SLIPMOD is set to PPP.**

PPPUID **Enter UserID for PAP.**
username Enter the UserID for PAP. This is the userID you use to login into your PPP account on your provider's machine. If your provider cannot handle PAP, you should use the TCPDIAL.SCR script instead to send your username to his machine. **This option applies only for PPP connections, furthermore, this option is only visible if PPPPAP is set to YES.**

PPPPWD **Enter Password for PAP.**
password Enter the Password for PAP. This is the password you use to login into your PPP account on your provider's machine. If your provider cannot handle PAP, you should use the TCPDIAL.SCR script instead to send your username to his machine. **This option applies only for PPP connections, furthermore, this option is only visible if PPPPAP is set to YES.**

SLIPPING **Ping DNS how often (seconds) to keep link alive.**
0 Some ISP (internet service providers) are stubborn and don't want to remove their inactivity timeouts on SLIP/CSLIP/PPP connections. This will make your link to your internet disconnect every so often, if there is no TCP/IP activity on your BBS. The re-dialer will reconnect, but this is still annoying. By setting SLIPPING to a number of seconds that is smaller than your provider's inactivity timeout, MajorTCP/IP will ping your primary DNS every SLIPPING seconds. As this is "activity", no timeout will be able to occur. Set SLIPPING to 0, to disable. **This option is visible only if SLIPINT is set to YES.**

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Edit the TCPDIAL.SCR script file to work with your provider's prompts

***NOTE* Ignore this step if you're using PPP with PAP.**

Once the TCPLIBM.MSG file is properly configured, the next step is to edit the **TCPDIAL.SCR** file located in your BBS directory. (usually \WGSERV or \BBSV6 depending on your setup). This file **MUST** be customized to work with your provider's screen prompts. The script language is very simple and consists of 4 commands. For dedicated serial SLIP/CSLIP connections, all you may need is an empty script with one SEND command on an empty line. **However, if you're using a null-modem SLIP/CSLIP connection to a local unix box, you may still need some sort of login procedure. In any event, please refer to pages 43 and 44 of the manual for the sample case.**

DBUG Tells MajorTCP/IP to turn on script debugging. More information will be printed in the audit trail.

SEND <text> The SEND command tells MajorTCP/IP to send the characters specified to your modem. SEND adds a carriage return at the end of the <text> that you've specified. If you use SEND without any text, MajorTCP/IP will simply send a carriage return.

WAIT <text> The WAIT command waits up to 60 seconds for the case-sensitive <text> to be received from your modem. If the text is never received, the script will be aborted with a message in the audit trail. Otherwise, MajorTCP/IP proceeds to the next statement in the script file.

ESC The ESC command lets you send a single escape (ASCII character decimal 27) to the system you are attempting to connect to.

Any line that starts with the pound sign is used to add comments to the script file. Any text on that line following the pound sign will be ignored by MajorTCP/IP.

The TCPDIAL.SCR file contains a sample script used to login to a standard unix box. To find out exactly what your provider's prompts look like, you should use a terminal program like Telix or Procom and connect to your provider manually. It's a good idea to turn on the capture buffer and print out the file on paper afterwards. Here is a sample connect session to a typical provider and how we translate that to a functionning script file.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

STEP #5:

Configure the RLogin module

Last revised, September 16th 1996.

- Added **DMALANG** option for DMA Language mode selection upon connection to a remote DMA server using standard Rlogin strings.
- Added Option **TCPMODDF** in TCPLIBM.MSG, level 4 configuration. This option is used to display the location of the user when he is **not** in a MajorTCP/IP module. This is related to the **TCP_RL_MOD text variable** documented in the ***"Text Variables: Changing the /# command to display the Rlogin destination"*** section of this chapter.

RLogin Overview

Rlogin is a special "Remote Login" protocol that lets a user login to a Unix machine remotely. MajorTCP/IP's Rlogin mimics the native Unix Rlogin protocols thus enabling users on MajorBBS and Worldgroup to connect to Unix machines as if the BBS was in reality a Unix system. The number one use people make of Rlogin is to connect their MajorBBS/Worldgroup computer to a local Unix machine connected together via TCP/IP or Novell LAN. With this feature, you can then, from your unix box, offer services like Lynx (a text-based web browser), archie and gopher, or even run a MUD (Multi-User Dungeon).

***IMPORTANT NOTE* most of the modules are dependant on Rlogin for aliasing, so Rlogin MUST be in your menu tree. If not the other modules will not function properly**.

The advantages of running a Unix machine in addition to MajorTCP/IP are numerous:

More Services — There's a large number of services that are available exclusively on Unix systems that can be very useful or entertaining for your users. Services like: Gopher, Archie, Lynx, Newsreaders (tin, trn, nn), MUDs (Multi-User Dungeons) and their variants, Unix Databases, and even full Shell accounts.

Sharing the burden — In some cases, having MajorTCP/IP do everything from handling web pages to FTP sessions to the occasional Telnet or SLIP/CSLIP/PPP session can affect the general performance of your BBS. You can offload some of those Internet Services from the BBS system to the Unix machine. For instance, if you have very popular web pages, you could use a Unix-based web server instead of MajorTCP/IP's built-in web server freeing up your BBS for other things. Another example is the use of a Unix machine for Newsgroups. If you intend on carrying several hundred newsgroups, this will use up a lot of BBS disk space. By using the Unix machine as your news machine instead of MajorTCP/IP's NNTPD, you will save yourself some grief.

Security — If you offload some of the things you'd normally handle on MajorTCP/IP to the Unix machine like for instance, Web Server duty. The added redundancy gives you a Major advantage. Should the BBS go down, the web pages on the Unix machine will still be accessible. Should the Unix machine fail, you could temporarily run the MajorTCP/IP Web server while you get the Unix Machine up and running again

Flexibility — Some providers don't offer DNS services nor Sendmail Smarthost services. Running a Unix system lets you handle your own DNS list and Sendmail Smarthost. You are in control.

What's special about MajorTCP/IP's RLogin?

MajorTCP/IP's Rlogin has several characteristics that make it much more useful than straight Unix Rlogin. Rlogin (and Telnet) are the only modules that MUST be installed on your system no matter what final configuration you have because Rlogin handles more than just basic connections.

- Rlogin has the ability to pass the User ID of the current user to the Unix Host you are connecting to enabling you to automate the login process using pre-programmed module pages. In fact, Rlogin can respond to a large array of requests from a Unix machine. We call this the **Rlogin Plus protocol.**

- Rlogin can be used to maintain a database of aliases. One of the problems about MajorBBS/Worldgroup .vs. the internet is the fact that ordinary ID's on the BBS can have up to 29 characters and are comprised of characters that aren't "legal" on the net. You can only use 16 character user names, with a fairly restricted number of valid characters. Rlogin will let you use and maintain the Rlogin alias file **TCPUIDS.DAT**. This file is shared by many modules including Rlogin.

- Rlogin can also be used to function with the MG/I alias file if you previously installed Major Gateway Internet. The setup is similar to a normal alias file. It only requires the setting of a pair of extra parameters.

How does it differ from Telnet?

Telnet's function is slightly different from Rlogin's. Telnet is mainly used to establish connections with application servers, somewhat akin to a terminal program on a PC connecting to a BBS. The BBS software is an application that offers some services over the modems. It doesn't give total access to the host machine. In other words, it's a connection inasmuch as the host machine responds to requests, but it isn't as "intimate" as Rlogin's capability to remotely access the target machine's operating system. RLogin is somewhat similar to products called PC Anywhere or Carbon Copy in the MS-DOS world. But this is only an analogy ... it isn't perfect. Sometimes, you can use Telnet to login to shell accounts as well as Rlogin. It really depends on how the target Unix system is setup.

How do I use MajorTCP/IP's implementation of RLogin?

You can use Rlogin for several tasks:

- **As a generic "Rlogin" page**. This lets you do a manual Rlogin to any site on your Local net or on the internet. This capability is fairly dangerous and should **NEVER** be given to the public. It isn't that Rlogins on the internet are dangerous, it's mostly because people who have accounts on your system could Rlogin into your Unix machine (assuming one is there) without any kind of security checking if the Unix machine is setup to bypass password requests for local Rlogin users.

- **Provide access through pre-programmed "Rlogin" pages**. This is usually how you would offer Rlogin to your users, by giving them access to Unix services via a pre-programmed Rlogin page. This usually requires a special setup on the Unix machine. This lets your users connect to your Unix host transparently. You can create a script on your Unix machine (consult a Unix guru) that will automatically start-up the desired Unix applications right after the user is connected. Rlogin will answer special information inquiries from the Unix hosts, depending on the Rlogin command string.

- **Rlogin as an alias request page.** You can create an Rlogin page that will let your users select a valid E-mail alias for internet E-mail. This can work with the TCPUIDS.DAT file (the native alias file for Rlogin) or the GALGWI.DAT file (the alias file used with MG/I). Special settings are required if you wish to use the latter. You need this page for proper E-mail delivery and replies.

- **Rlogin as an alias maintenance page.** Finally, you can create a "SYSOP" page that lets you edit the alias file (Rlogin or MG/I file). You can search by User ID, Internet ID and delete. You need this page if you use the Rlogin alias request page.

Using the RLogin module

Here are the various questions the Rlogin module will prompt you for with an explanation of each if you attempt to use Rlogin manually from a "Generic" Rlogin page. In fact, you already created one when you installed the core modules (TCPLIBM, Rlogin and Telnet) in the menu tree. All you need to do is perhaps modify the Rlogin page to allow the /go command. Note that the order in which each query is made is the same as the one you will use for the automated command string. **[Note: each command string item is explained within a note block like this]**

You type in /go Rlogin (or you select it from a menu somewhere).

What Protocol: R(L)ogin or R(S)h>

Selecting **L** lets you start an Rlogin session. You'll be able to pass some parameters to a script file that will intercept the data on the Unix machine. Of course, a Unix script has to be written to intercept and interpret the data given.

Selecting **S** lets you start an Remote Shell session. You'll be able to supply to the Unix host a command to be executed at the shell level. You can type in the command directly from the MajorTCP/IP Rlogin.

Typing the word **SYSOP** at this prompt (and assuming you have the **SYSKEY**) will bring up the SYSOP functions, include alias file maintenance.

Typing the word **ALIAS** at this prompt lets the person using Rlogin enter an internet alias if the user doesn't have one.

[Note: On the command string you'll use, you simply put the letter L or S, with a second letter indicating what kind of special commands you will be accepting separated by a slash '/'. The special commands are explained later in this section, see the "create pre-programmed Rlogin pages" section]

You type in L to do a normal RLogin

Enter Host IP address>

This is where you type in the target Unix system's Host name or IP address.

[Note: On an automated command string, you can only use the numeric IP address. If you specify a Host name, it will not work. Use the DNS resolver to find out what's the IP address of a given site]

You type in your Unix machine's name: some.widgets.com

Enter the local login name>

Part of the normal Rlogin protocol is the need to tell the system you are calling what your ID is on the local system (your BBS). This is either your BBS user ID or the internet user ID associated with your BBS user ID.

[Note: On the automated command string, you can have MajorTCP/IP feed the local login name automatically. You can use these variables: %u = Internet user ID, %ul = Internet user ID in lower case. %ud = Internet user ID with creation. %ud will force Rlogin to query the user automatically if he doesn't have an internet user ID. Once selected, the user will not be querried for one if he tries Rlogin again].

You type in your internet user ID, that is Johndoe.

Enter your login name on the host>

At this prompt, you type in the user ID you have on the remote host. This ID must be valid on the internet (ie: 16 characters, no special punctuation except periods and underscores).

[Note: The User ID can be that of a generic account (which is used by everyone on your system, you can use the special commands to send the user to the desired service on the Unix machine) or a specific account. You can use %u, %ul and %ud. Usually the latter.[

You type in your internet user ID again, Johndoe.

Enter your terminal type (ansi)> (Rlogin Only)

Appears only if you selected R(L)ogin at the first prompt. Here, you specify a terminal mode to connect in on your Unix system. This terminal mode must be valid (i.e.: defined in your termcap or terminfo database). Note that in addition to this terminal type, Rlogin also sends your screen width and length to the remote host. Make sure they are set properly in your MajorBBS account. **The most common termtypes are vt100 and ansi.**

[Note: On the automated command string, you simply put in the termtype in long form. vt100 or ansi usually does the job fine.]

You type in vt100.

Enter parameter to RSh> (Remote Shell only)

This prompt appears only if you specified the R(S)h option at the protocol prompt. This lets you feed the remote system's shell a typical shell command. Like ls <filename> for instance.

[Note: This lets you start commands on the Unix machine and displays the result on the screen. For instance, more <filename> on the Unix machine would display a filename page per page. Rsh has limited application.]

Enter extra parameter to the shell> (Rlogin only)

This prompt lets you specify extra parameters that you want a shell script to be able to query on the Unix machine. This can be used to create menu options on the BBS that will send the user directly into applications on the Unix system.

[Note: in other words, you can create menu options like [E]nter the Widgets MUD that would Rlogin the user to the Unix system and startup the MUD automatically]

You type in <enter> to skip this step. You're now logged into the Unix system.

RLogin sessions and their effects on TCP Handles

Each incoming our outgoing RLogin uses up one TCP Handle. For more details about TCP Handles, check out NBTCP (**page 32 of this manual**). DNS and Finger requests do not use up any of your Galacticomm licenses off of your six-packs

Installation procedure for the RLogin module

Step by Step installation procedure for the RLogin module

STEP	Description	Done
#1	Configure the TCPRLGN.MSG file for RLogin operations	
#2	Create a generic Rlogin page (for Sysop only)	
#3	Create an Rlogin alias creation page (Highly recommended)	
#4	Create an Rlogin alias maintenance page (Highly recommended)	
#5	Create an Rlogin pre-programmed page (optional)	

Configure the TCPRLGN.MSG file for RLogin operations

Level 3 - Security and Accounting configuration

- From the main configuration menu (CNF), select **F3 - Accounting and Security**
- Press on **F8 - Search**, type **TCPRLGN.MSG**
- The first item you should find is the **SYSKEY** parameter.
- Edit each item as described below, moving from item to item using the arrow keys.
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu.

SYSKEY **Key for Rlogin sysop access.**
MASTER There is a hidden sysop menu in Rlogin, you access it by typing SYSOP at the *"What Protocol: R(L)ogin or R(S)h"* prompt. This key controls who should have access to that menu. This **menu includes the ability to change entries in the alias files**. Only SYSOPs should have this key. Your generic Rlogin page should be protected by the SYSKEY.

SURKEY **Key to be surcharged even when exempt**.
<empty> If a monthly, credit-exempt, user owns this key, Rlogin will apply the appropriate surcharge for the connection manually. Leave blank to disable this feature. Note that Rlogin will never surcharge anyone with the master key. In other words, this key lets you charge people who are normally credit-exempt for Rlogin services. Useful if you charge a flat fee for local BBS usage but you want to charge by the credit for internet services. The surcharge itself is **defined in TCPLIBM.MSG, level 3 accounting and security. (SUROLOC and SUROREM, page 34 and 35 of this manual).**

NSURKEY **Key that will exempt from any surcharges.**
<empty> This key exempts a user from any form of surcharge in the usage of Rlogin. In other words, this is a surcharge override.

Level 4 - System options configuration

- From the main configuration menu (CNF), select **F4 - Configuration options**
- Press on **F8 - Search**, type **TCPRLGN.MSG**
- The first item you should find is the **RLGPORT** parameter.
- Edit each item as described below, moving from item to item using the arrow keys.
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu

RLGPORT **Definition of the well-known Rlogin port.**
513 RLogin will make calls to the RLGPORT port number when trying to establish a Rlogin session. You should not change it. It defines what's called the well-known-port to use when establishing an Rlogin call. This is a BSD protocol standard. It's included just in case you need to change it for a very special application.

RSHPORT **Definition of the well-known RSH port.**
514 RSh will make calls to the RSHPORT port number when trying to establish a remote shell session. You should not change it. Like the RLGPORT, this is a BSD protocol standard and shouldn't be altered unless you need to change it for a very special application.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

MINSUID **Minimum size of Internet-UserIDs.**
4 RLogin supports an Internet UserID database. You can define here the minimum length of the User ID's your users will be able to use. This User ID should match the requirements of the Unix host you want to connect to.

MAXSUID **Maximum size of Internet-UserIDs.**
16 RLogin supports an Internet UserID database. You can define here the maximum length of the User ID's your users will be able to use. This User ID should match the requirements of the Unix host you want to connect to.

DISCHR **Disconnect Character.**
! In an Rlogin connection, this character, typed 3 times with a delay of 3 or more seconds afterwards will close the connection. Enter '!' to disable this option. By default, you can't disconnect from an Rlogin this way, but you can use the X command however, unless the connection is already established and you are logged in.

USEMGI **Use the Major Gateway/Internet alias file.**
NO Instead of maintaining yet another alias file, you can tell Rlogin to use the alias file created by the Major Gateway/Internet from Galacticomm. Rlogin will never write to that file but will get Internet aliases from it **unless you toggle MGIWRT to YES.**

MGIWRT **Add/Write to MG/I alias file.**
NO This parameter tells MajorTCP/IP to write to the MG/I alias file, when a user picks a new alias. **This option will not appear if USEMGI is set to NO.**

SPCPWD **Allow Rlogin Plus to send passwords.**
NO You can enable Rlogin Plus to answer the 0x9b special command by sending the current user's password. Be sure to know what you're doing if you are enabling this, as if you configure it improperly, people might be able to grab your user's password. Check out the **"Create an Rlogin pre-programmed page"** section for details about the Rlogin Plus protocol.

SPCPWDT **Password to send if queried**.
DISABLED If you prevent Rlogin Plus from sending passwords, you can define a string that will be sent in it's place if queried by the 0x9b special command. This option is visible only if SPCPWD is set to NO. Check out the **"Create an Rlogin pre-programmed page"** section for details about the Rlogin Plus protocol.

SPCCHR **Special Characters Allowed.**
<empty> By default, RLogin does not allow users to enter any non alphabetic characters in the internet-userid. You can enter in the next option a list of characters you want to accept. Leave blank to accept none. Example: Enter ._! to accept the "."."_" and "!" characters.

DMALANG **Always pretend to be using language 1**
NO It's possible that DMA servers and Master BBSes don't share the same language options, or that they are not mapped to the same numbers. When you connect to a DMA server that is not matching your language, you can force all of your users to appear as if they are using the first language of the DMA server.

Create a generic Rlogin page (for Sysop only).

This page will let you Rlogin anywhere, as long as you have an IP address or a host name to Rlogin to. In general, you'll use Rlogin mostly to communicate with your own Unix machine. To use the page, check out the **"How do I use MajorTCP/IP's implementation of Rlogin"** section. During the installation process of the MajorTCP/IP core modules RLogin/Telnet and TCPLIB), you already created a generic RLogin page although in this case, the page was created as a floating page detached from the main menu tree.

To create a generic RLogin page associated to a "Sysop Menu" (because access to this page should be restricted to authorized people only), simply follow these instructions. Note that this menu is used solely as an example. Simply substitute it for the menu you want to associate Rlogin to. Only users who have the **SYSKEY** should have access to this page.

Use the following procedure to create a generic sysop-only RLogin page

- From the main configuration menu (CNF), select **F2 - Design Menu Tree**
- Make sure that the menu item cursor is located on **your Sysop Menu page**
- Select **F2 Edit** to change the Sysop Menu page
- Go to the menu options area and **add a new option**, say [L] to R(L)ogin to another site
- In the **EDIT OPTION** window ...
    - Short Description .....could be "R[L]ogin to another site"
    - Key required for this option..... **SYSOP or MASTER key**.
    - Destination page..... could be called **GRLOGIN**
    - **Save the menu**. A new page in the menu tree should've been created.
- Move the cursor to the new page called **GRLOGIN.**
- Press **F2 Edit** to configure this module page.
    - Allow go to this page ..... should be set to **YES**
    - Key required ..... **SYSOP or MASTER key.**
    - Select module window, you should chose the **RLogin Module**
    - Display header ..... should be set to **YES**
    - **The command string should be left empty**
    - Save the resulting page.
- That's it!

When you select the R[L]ogin option from the Sysop Menu, this should bring you to the **"What Protocol: R(L)ogin or R(S)h>"** prompt. Type **SYSOP** at the prompt will bring you the Internet alias maintenance screen.

Create an Rlogin alias creation page (Highly recommended).

The process is almost exactly the same as the Generic Rlogin page except for a couple of items: You need to put the word **ALIAS** at the command string, and you can make the Rlogin module accessible to all the users with internet services privileges. We assume you have some sort of "Internet Services" menu. This is what we use in our example. Follow this procedure:

Use the following procedure to create an Rlogin internet alias creation page

- From the main configuration menu (CNF), select **F2 - Design Menu Tree**
- Make sure that the menu item cursor is located on **your Internet Services page**
- Select **F2 Edit** to change the Internet Services page
- Go to the menu options area and **add a new option**, say [R] for Register for Internet E-mail.
- In the **EDIT OPTION** window ...
    - Short Description .....could be “Register for Internet E-mail”
    - Key required for this option..... **The key your users own for internet access.**
    - Destination page..... could be called **ALIAS.**
    - **Save the menu**. A new page in the menu tree should’ve been created.
- Move the cursor to the new page called **ALIAS.**
- Press **F2 Edit** to configure this module page.
    - Allow go to this page ..... should be set to **YES**
    - Key required ..... **The key your users own for internet access.**
    - Select module window, you should chose the **RLogin Module**
    - Display header ..... should be set to **YES**
    - **Command String ..... ALIAS**
    - Save the resulting page.
- That’s it!

Please note that the word **ALIAS** must be in CAPS.

Setting the USEALIAS parameter

We need to set **USEALIAS** (in TCPSMTP.MSG, level 4 Configuration options) to **YES**
This tells SMTP (*Simple Mail Transfer Protocol*) to use the ALIAS file instead of doing a simple conversion on the normal User ID. Once configured, MajorTCP/IP will always convert normal User ID’s to the equivalent internet alias stored in the **TCPUIDS.DAT** file unless you’ve decided to use the MG/I file instead.

- From the main configuration menu (CNF), select **F4 - Configuration options**
- Press on **F8 - Search**, type **USEALIAS.** When found, set it to **YES.**
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu.

Setting the USEMGI and MGIWRT parameters for MG/I alias file usage

If you had MG/I installed on your system and would like to use the MG/I alias file (GALGWI.DAT) file, you must set USEMGI and MGIWRT in TCPRLGN.MSG to YES. (**See the “Configure the TCPRLGN.MSG file for Rlogin operations” section**). **IGNORE THIS SECTION IF YOU NEVER USED MG/I.**

- OR - follow these quick instructions:

- From the main configuration menu (CNF), select **F4 - Configuration options**
- Press on **F8 - Search**, type **USEMGI.** When found, set it to **YES.**
- Press on **F8 - Search,** type **MGIWRT.** When found, set it to **YES.**
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu.

[Vircom Inc’s MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

What the user sees when calling up the Rlogin alias creation page

When the user selects (as in the example) the Register for Internet E-mail option that we created, this is what he will see. Note that instead of getting the "**What Protocol: R(L)ogin or R(S)h>"** prompt, the user will get this message instead:

> **You must now choose an Internet userid name that must not exceed 16 characters in length and must be at least 4 characters. The userid name will be converted to lowercase and can include only letters (a-z).**
>
> **Enter your Internet Userid >**

All the user needs to do is to type in his or her desired interned ID at the prompt. If the user ID given is valid, the user will see this message:

> **Okay, your Internet userid has been recorded. We will attempt to establish the connection you have requested. However, if it doesn't work (if you are stuck at a password prompt), send an E-mail to your Sysop asking him to validate your Internet account.**

Should the user enter an ID that already exists, this is the resulting message:

> **This Internet userid is already in use. You must pick an userid that is not the same as any userid on your BBS or Internet userid of your BBS.**

If the user tries to get an Internet user ID and already has one, this is the resulting message:

> **You already have an internet userid. If you want to change or delete it, you'll have to ask your SYSOP about it.**

In any event, if the user wants to change his or her User ID, the Sysop has to use the Alias Maintenance page to search for the alias in question (by BBS User ID or Internet User ID), and delete the offending name to be able to change it.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Create an Rlogin alias maintenance page (Highly recommended).

The process is exactly the same as creating the **Rlogin alias creation page**. The only difference is the menu you attach it to and the command string to use. We assume you have some sort of "Sysop" menu. This is what we use in our example.

Use the following procedure to create an Rlogin internet alias maintenance page

- From the main configuration menu (CNF), select **F2 - Design Menu Tree**
- Make sure that the menu item cursor is located on **your Sysop menu page**
- Select **F2 Edit** to change the Sysop Menu page
- Go to the menu options area and **add a new option**, say [E] for Edit internet aliases.
- In the **EDIT OPTION** window ...
    - Short Description .....could be "Edit internet aliases."
    - Key required for this option..... **SYSOP or MASTER key.**
    - Destination page..... could be called **EDALIAS**
    - **Save the menu**. A new page in the menu tree should've been created.
- Move the cursor to the new page called **EDALIAS.**
- Press **F2 Edit** to configure this module page.
    - Allow go to this page ..... should be set to **YES.**
    - Key required ..... **The SYSOP or MASTER key.**
    - Select module window, you should chose the **RLogin Module**
    - Display header ..... should be set to **YES.**
    - **Command String ..... SYSOP**
    - Save the resulting page.
- That's it!

Please note that the word **SYSOP** must be in CAPS. When a normal user with simple internet access uses the Rlogin module set for alias creation,

What the sysop should see after invoking the internet alias maintenance page.

When the sysop selects the Edit internet aliases option in the Sysop Menu we created, this is what he will see. Note that instead of getting the "**What Protocol: R(L)ogin or R(S)h>"** prompt, the sysop will get this menu instead:

RLogin Sysop Menu
==========

V - View the Internet Alias of a user.
D - Delete the Internet Alias for a user.
I - Find who is using a specific Internet Alias

X - Exit Rlogin

To search for an internet Alias directly, use the **V** option.
To search for an internet Alias using the BBS User ID, use the **I** option.
To delete the alias found, press on **D**.

If a user wants to change his/her internet User ID, simply use the search function to find it, then use the delete function to erase the entry. All the user needs to do is go back to the **alias creation page** (Register for internet E-mail in our example) and get a new one.

Create an Rlogin pre-programmed page (optional).

Rlogin pre-programmed pages are a little different in that you need to have something on the Unix machine to prepare for the incoming connection. For Unix scripting, you should consult a local Unix-guru or be prepared to learn how to do it yourself. Basically, pre-programmed Rlogin pages can let you offer Unix services to your users with pre-defined menu options. The process involves two sides: the BBS machine and the Unix Host. Rlogin will only work if you enable it on your UNIX host and adjust your security file accordingly. You can do a "man" on rlogin, rhosts and host.allow to find out how you can use this with your particular UNIX system.

The Unix Host, what you need.

- You need to create a **.rhosts** file that will prevent the Unix machine from asking the user a password. What you need to put in the file is the internet address of the calling system, or in this case, your BBS's name (i.e.: Combined HOSTNAME and DOMNAME in TCPLIBM.MSG, level 1 hardware configuration). For instance, bbs.widgets.com is a valid address for the .rhosts file.

- You need to either a) **use generic user accounts** or b) create a script file that **will create accounts** for each individual user, with a home directory, **.rhosts** file and **application launching script file.**

A script file that will query MajorTCP/IP's Rlogin for a parameter that will specify which application to launch on the Unix side. For instance: You use Rlogin with the word "lynx" in the "**Enter extra parameter to the shell"** field. The Script on the Unix Machine should be able to pick this word up and start up the Lynx text-based web browser on it's side. We use MajorTCP/IP's Rlogin extended commands to accomplish this.

The BBS machine, what you need.

Basically, you need to create an appropriate pre-programmed Rlogin module page. The process is similar to the previous pages defined for alias creation and maintenance. What really changes is the command string. We use the concatenated commands. Here's how to do it:

Use the following procedure to create an Rlogin pre-programmed module page

- From the main configuration menu (CNF), select **F2 - Design Menu Tree**
- Make sure that the menu item cursor is located on **your Internet Services menu**
- Select **F2 Edit** to change the Internet Services page
- Go to the menu options area and **add a new option**, say [Y] to start up Lynx.
- In the **EDIT OPTION** window ...
    - Short Description .....could be "Start up Lynx"
    - Key required for this option..... **The key required for normal internet use.**
    - Destination page..... could be called **LYNX**
    - **Save the menu**. A new page in the menu tree should've been created.
- Move the cursor to the new page called **LYNX.**
- Press **F2 Edit** to configure this module page.
    - Allow go to this page ..... should be set to **YES.**
    - Key required ..... **The key required for normal internet use.**
    - Select module window, you should chose the **RLogin Module**
    - Display header ..... should be set to **YES.**
    - **Command String ..... See Below "Create the command string"**
- Save the resulting page and that's it!

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Creating the command string

The command string you use follows the input sequence described in the **"How do I use MajorTCP/IP's implementation of Rlogin?" section of this step.** The command string usually takes these formats:

<R(L)ogin/(ext)> <IP address> <Local user ID> <Host user ID> <Term Type> <Parameters>
<R(S)hell> <IP address> <Local user ID> <Host user ID> <Shell Command>

<R(L)ogin/(ext)> Means to invoke the Rlogin module in Rlogin mode. The extension is simply the command that activates the **special commands.** On the command string, this item takes the following forms:

L Use the Rlogin module for a standard R(L)ogin connection.
L/S Use the Rlogin module while enabling the special commands. You need to enable special commands if you want the Unix system to query the BBS for the user's UserID. That way, login is automatic. The Unix machine won't ask for a password if the **.rhosts** file is correctly set.
L/SD Use the Rlogin module, enable special commands and have the user create a new internet user ID if he doesn't have one. The same as using the ALIAS command.
L/K Same as L/S except there is no screen echo. The person doesn't see the login process. He only sees that at some point, he's been brought directly into the desired application. You can also add the letter **D** to force account creation on the BBS.

<R(S)hell> Invokes Rlogin to issue a Remote shell command specified in **<Shell Command>**. You can't use any of the extended commands. The special commands are automatically used solely to pick up the <Local user ID> and <Host user ID> fields. You use the letter **S** to invoke Remote Shell commands. Once the command is executed, the result is displayed on the screen.

<IP address> The IP address of the Unix machine.

<Local user ID> & **<Host user ID>** The internet user ID used on the BBS. This can be specified explicitly (if you are doing an Rlogin connection into a generic account that all your users will use) or indirectly using the user ID variables. Generally, the BBS internet user ID should be the same as the one you'll be using on the Unix system **<Host user ID>.**

The explicit form implies that an account has already been created on the Unix machine. For instance, a generic Lynx account could be called **Lynx_user**. The user ID doesn't need to really exist on the BBS in this case. You just want to fool the Unix system into thinking that such an ID exists on the calling system. If you have accounts for individual users:

%u The user's Internet ID.
%ul The user's Internet ID converted to lower case.
%ud The user's Internet ID. If the user doesn't have an Internet ID, Rlogin will ask the user for one. This is the same as explicitly asking the user to get an Internet ID using an Rlogin ALIAS creation page.

<Term Type> The terminal type to use upon login. Usually vt100 or ansi, depending if these are defined in the termcap or terminfo database on the Unix machine.

<Parameters> These are optional parameters you want to make available to the Unix machine. For instance, you could put the word Lynx (in a non-generic account setting) to tell the script file on the Unix machine to start up Lynx for the user. The Unix script needs to use the **0x9a special command** (defined later in more detail) to capture the data in this field.

Sample Command Strings

L/S 199.84.216.1 Lynx_User Lynx_User ansi

This command string does the following things:

- Opens an Rlogin session with special commands activated (so that the username gets read)
- Connects to a Unix machine at the address 199.84.216.1
- Logs into a generic account called Lynx_User. When Rlogin gets to this point, it waits for the Unix machine to send the 0x81 or 0x82 bytes. When Rlogin receives them, it sends to the host machine the "Lynx_User" string in both querries. 0x81 is the Unix machine's way to tell Rlogin "what's the user's name on your system. 0x82 is the same thing, but also asks to convert the ID to lowercase. If there's no **.rhosts** file in the home directory of Lynx_User, it will query the user for a password.
- Tells the Unix machine to use the **ansi** term type.
- Once the person is connected, your Script file should immediately call up Lynx.

L/KD 199.84.216.1 %ud %ud vt100 lynx

This command string does the following things:

- Opens an Rlogin session with special commands activated and no screen echo with automatic account creation if the user has no Internet User ID on the BBS.
- Connects to a Unix machine at the address 199.84.216.1
- Logs into an account corresponding to the current user's Internet username if it exists on the Unix machine. If it doesn't, you may need to create a page that calls up a generic account with an auto-login Script designed to create specific accounts. Check out SCRIPTS.ZIP for sample scripts that do just that. When the machine receives the 0x81 or 0x82 commands, it feeds the Unix host the user's Internet ID. If there's no **.rhosts** file in the user's home directory, it will query the user for a password.
- Tells the machine to use the **vt100** term type.
- Waits for the machine to read the "lynx" string. When the Unix machine sends the 0x9a code (feed me your Rlogin extra shell parameter), Rlogin will transmit the word "Lynx". It's up to the script file on the Unix side to know what to do if it receives that word. (if the extra parameter = lynx, execute the lynx program).

S 199.84.216.1 generic generic more condition

This command string does the following things:

- Opens a remote Shell session that will execute a quick command and display it on the user's screen.
- Connects to a Unix machine at the address 199.84.216.1
- Feeds it the user name "generic". If the **.rhosts** file is correctly set, no password is required.
- Tells the Unix machine to do a "more condition". more is a text-file viewer. "condition" is the name of the text file to view. Once the person has finished reading the text-file and quits from the viewer, the connection ceases immediately.

Rlogin special commands for Unix Scripting

The special commands are enabled when you use the slash '/' character when invoking the Rlogin module to do a normal Rlogin. You can also use the '*' asterix character that enables the special extended commands. In both cases, these commands are issued by the Unix machine using the codes below. Rlogin simply takes care of forming the appropriate response.

/S **Enables special commands.** You need to enable special commands if you want the Unix system to query the BBS for the user's UserID. That way, login is automatic. The Unix machine won't ask for a password if the **.rhosts** file is correctly set.

/SD Enable special commands **and have the user create a new internet user ID** if he doesn't have one. The same as using the ALIAS command.

/K **Same as /S with no screen echo**. The person doesn't see the login process. He only sees that at some point, he's been brought directly into the desired application.

/KD **Same as /SD with no screen echo.**

***** **Same as using the slash, except that it activates the extended special commands.**

When you use a slashed command (L/S, L/SD ...), Rlogin watches the flow of characters FROM the remote host and will automatically send values/reply strings to the remote system depending on the "special byte" or code received.

You have three types of commands:

One Shot commands

These commands can only be used once. Rlogin stops monitoring the line for these one-shot commands once one of them is received and processed.

Multiple use commands

These special commands can be used any number of times you want. You must turn them off once you're finished with them. If you don't, a hacker who is knowledgeable about MajorTCP/IP could use them to change some of his credit rates for instance. Use the command 0x9f to turn them off.

Extended Special commands

These are two-bytes sequences starting with 0x96 followed with the appropriate extended command then 0x97 to terminate the command. For instance, if you want to find out if a user owns the "TEST" key, the unix script should proceed something like this: echo "\x96TEST\x97". Rlogin should return 1<enter> if the user owns the TEST key or 0<enter> if he does not. All return values are terminated by an <enter>, making them easy to be processed. On the BBS side, use the * instead of the / to use these.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Table of special commands

Byte received	Rlogin sends in reply ...	Type of command
0x81	Internet UserID	One shot
0x82	Internet UserID lowercase	One shot
0x91	Internet UserID	Multiple use
0x92	Internet UserID, lowercase	Multiple use
0x93	User's alias from Internet alias database or *N/A* none	Multiple use
0x94	Full name of user	Multiple use
0x95	Returns the "ansi flag" variable (1-3 Ansi ON, 0-2 Ansi Off)	Multiple use
0x96	Start recording incoming character in buffer **OR** indicate that an Extended Rlogin Special command is coming up.	Multiple use
0x97	Stop recording, and see if the user owns the key that is in the buffer. Returns 1 if he does, 0 if he doesn't.	Multiple use
0x98	Indicate that the following numeric characters (up to the following 0x99) will define a new surcharge for this connection. Added to the current connection credit rate. (SUROREM/SUROLOC)	Multiple use
0x99	Start the surcharge based on the numeric value between 0x98 and 0x99	Multiple use
0x9a	Return the "Extra Shell Parameter". This parameter is usually coming from a parameter string entered in the menu page.	Multiple use
0x9b	Send the password of the current user if you enabled this with SPCPWD or send the default password entered in SPCPWDT	Multiple use
0x9c	Resume output to the user.	Multiple use
0x9d	Stop output to the user until 0x9c or 0x9f is encountered.	Multiple use
0x9e	The first time 0x9e is encountered, Rlogin returns "new", the subsequent times, Rlogin returns "Y"	Multiple use
0x9f	Stop special command interpretation.	Multiple use
0x80	The current user will be disconnected from the BBS upon return from this Rogin connection. It's up to you (or your script) to inform the user of that fact and of the reason for it.	Extended
0x81	Start Recording in buffer (and erase buffer)	Extended
0x82	End Recording in buffer (32 characters maximum)	Extended
0x83	Send buffer to Rlogin connection. Buffer is not erased and can be sent multiple times. A carriage return is appended to the string in the buffer.	Extended
0x84	Same as 0x83, but no carriage return at the end, unless you recorded one.	Extended
0x85	Evaluate buffer as if it was a text variable for the current user. Return string, with a carriage return appended to the end.	Extended
0x86	Generate an encoded generic password. This password is generated based on the string you have entered for SPCPWDT and the UserID. A carriage return is also added to the string at the end.	Extended
0x87	Returns the user ID that has been entered in the command string.	Extended
0x9f	Terminate interpretation of Extended Special Commands. Send the string 0x96 0x9f 0x9f to terminate all special commands when in "Extended" mode.	Extended

Sample: getting a text variable value on the BBS from a unix machine

Lets say you wanted to know what channel number the person was logged in from. The text variable we want to check on the BBS is “CHANNEL”. To do this, we need to open the buffer, type in the channel text variable we want info on, close the buffer, then send the buffer back to the BBS. Note that text variables need to be preceded by a justification indicator (L, C or R) and a length format indicator. (Check the Worldgroup Manual).

The commands on the unix machine would look like this:

```
printf “\x96\x81”          // Extended Rlogin special command, start recording
printf”L=CHANNEL”          // Send CHANNEL text variable, Justification L
printf”\x96\x82”           // Extended Rlogin special command, stop recording
printf”\x96\x83”           // Send Buffer to Rlogin (BBS)
```

The BBS would return the content of the CHANNEL text variable.

[Vircom Inc’s MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Text Variables: Changing the /# command to display the Rlogin destination

These are the two text variables available

TCP_RL_IUID

Defined to return the Internet UserId the user selected. It will use the built-in User-ID mangling mechanism if the person hasn't selected an internet alias. (example: someone with the BBS User ID of **Charles Darwin** would be **Charles.Darwin** on the internet -- note the period).

TCP_RL_MOD and **TCP_RL_MOD2**

This is used to change the output of our /# or # global commands so that instead of showing "Rlogin", you can display predefined text. Example: If the user is using PINE for Internet E-mail, you could have that displayed as "Pine" or "Internet_Mail" in your online users list.

To do that, you enter, as the last word of the Rlogin command string passed to Rlogin, #<word> where <word> is what you want to appear in your online users listing. You must also modify the proper message blocks used by your globals package to display the variable "TCP_RL_MOD" to show the module a user is into. For the standard MajorBBS /# display, you would change the ULSLIN text block.

TCP_RL_MOD and MOD2 only differ in the file indexes they use. If you want to find out which one works, simply setup your globals package with one of the variables, if it works, then you've got it. If not, try the other variable.

Notes about the TCPMODDF in TCPLIBM.MSG, level 4 configuration.

If you are using the TCP_RL_MOD or MOD2 text variables, you can use this option to specify which text variable will be used when a user is not in one of the modules that use TCP_RL_MOD. This would be used, for example, when you are using a module that display different module names when users are in different menu pages. **Warning: This option is currently experimental.**

Modifying the /# command to display destination of Rlogin: Detailed Procedure

- At then end of your Rlogin pre-programmed page command string, add the desired caption. This is defined by adding a pound sign followed by the caption like so: #Caption . Note that Rlogin will know that this isn't part of the Rlogin Extra shell command. Here is a real-world example: **L/S 199.84.216.1 Lynx_User Lynx_User ansi #Using_Lynx**
- From the main configuration menu (CNF), select **F6 - Edit text block**
- Press on **F8 - Search**, type **ULSLIN.**
- Press on **F2 - Edit, you'll be brought into a text editor window.**
- Move your cursor to the point where you want to substitute the last parameter with the text variable. You can write over the last parameter of the string. (it starts with a % symbol)
- Press on **Alt-V** to add a server text variable. Select **TCP_RL_MOD.**
- Press on **Alt-S** to save and go to the normal CNF screen.
- Press on **F10 Save and Exit** to go back to the main configuration menu

Pseudo Key: Forcing the user to select an internet alias

_TCP_RL_HIUID

has been defined so that it is granted to a user when he has selected an Internet UserId.

This key is very usefull in that, it allows us to create an automatic selection of an alias the first time a user tries to go into the E-mail menu. The procedure is fairly simple, follow these steps:

1. Startup the system and go into your menu tree.

- From the CNF menu, pick option #2, Design Menu Tree

2. Create the EMAIL2 module page

- Move the cursor to the TOP menu item.
- Press **F5-Add**. When asked for the Module name, type in **EMAIL2.**
- Move the cursor to the Free-Floating EMAIL2 page and press **ENTER**.
- When asked for which type of page, select **Module** page.
    - Allow go to this module ..... Should be set to **NO**.
    - Module name ..... Select "**Electronic Mail**"
    - Display module page header ..... Should be set to **YES**.
    - Command string ..... Should be left blank.
    - Return to menu tree? ..... Select **YES**.
- At this point, you have properly configured the E-MAIL2 page.

3. Modify the EMAIL page.

- Move the cursor to the EMAIL page and press **ENTER**.
- Press on the up-arrow, when asked for the type of page, select **Menu Page.**
- Allow "go" to this menu ..... Should be set to **YES**.
- Key required for "go" ..... Key that all valid users own (**NORMAL**).
- Is this an "auto-select" menu? ..... Should be set to **YES**.
- **Press on E to create an E-mail option**.
    - Short Description ..... **Electronic Mail.**
    - Key Required ..... **_TCP_RL_HIUID**
    - Destination page ..... **EMAIL2.**
- **Select the move option, since EMAIL2 exists.**
- Save this option ..... **YES**.
- **Press on P to create an Alias Picking option.**
    - Short Description ..... **Pick an internet alias.**
    - Key Required ..... Key that all valid users own (**NORMAL**).
    - Destination page ..... **ALIAS. (See Rlogin ALIAS page, p.75)**
    - Save this option ..... **YES**.
- That's it!

4. Create an Rlogin alias page.

Simply follow the instructions on **page 75**. Instead of creating the ALIAS page as per instructions, simply edit it because we created it in the previous step as a menu page.
All you need to do is follow the steps stipulated on page 75.

How it all works:

When a first time user goes to the E-mail menu, the auto-select will find the first item which the user has the key for (in this case, the Pick an Alias option) and will automatically call up the Rlogin Alias page. Once the person has selected an Alias, he is automatically attributed the _TCP_RL_HIUID key.

If the person subsequently choses the E-mail menu, because he has the key for the first option now (_TCP_RL_HIUID), the auto-select E-mail menu will bring the user to the EMAIL2 page that calls up the E-mail functions of MajorBBS/Worldgroup.

Simple, and it works.

STEP #6:

Configure the Telnet module

Telnet Overview

Telnet is a set of protocols that regulate how computer systems talk to one another without actually being logged into the target machine. On the server side (the system you are trying to call), an application must be listening to the port you are trying to connect to. Once connection occurs, a common protocol is established. This is usually either ASCII, Binary or 8 bit. You can even force a protocol negotiation if you don't know which one the other system expects.

Once connected, you are using the listening application's user interface which is functioning through that port. A simple analogy is the relationship between say, your standard Terminal Program for the PC to that of a BBS. You can't use that terminal program to get into the PC's operating system. You need some sort of application at the other side to provide a service over the modem, like a BBS for instance. The BBS gives you a limited number of options, there's only so many things you can do with this application. The relationship between Telnet and a computer system on the internet is similar to that of terminal programs like Telix or Procomm versus the BBS computer system waiting for a modem call. You can't do anything other than use applications that have been designed to talk over the modem. Telnet can only talk to applications that work with Telnet, so to speak.

How does it differ to Rlogin?

Rlogin is different in that, it lets you do a Remote Login. You can log-on to a remote computer and use that computer as if you were on the machine locally. If we use the same analogy, Rlogin is more akin to those control programs like PC-Anywhere or Carbon Copy. It lets you login directly into the operating system and use the machine as if it were on your desk. You can use programs that weren't designed to talk over a modem for instance. That's because as far as the host system is concerned, you're just like any local user. This is the principal reason why access to Rlogin must be restricted to pre-programmed Rlogin sites. It's too dangerous to leave in the hands of just anybody because of the potential for mischief.

How do I use MajorTCP/IP's implementation of Telnet?

You have three methods to use MajorTCP/IP's Telnet:

The Normal or "Generic" method

This is the method by which users can specify an IP address or internet address they want to connect to including the port number and protocol. People who want to use this feature need the **NORKEY** defined later in this section. To provide such access to your users, you need to create a generic Telnet page for them. The process of creating a generic Telnet page is also explained later in this section.

The pre-programmed menu pages method

This is the prefered method used to create pre-defined Telnet sites. Like a "Generic" telnet page, you make it possible for your user to select a menu option or /go statement that sends them to a Telnet module page. From there, a command in the "command string" section of the module page automatically establishes the connection to a pre-defined site. All this is done transparently. This gives you the ability to offer services such as MUDs, Internet-capable BBSes and so on. The command used on the module page's command string takes the form of O <IP address> <Port> <Mode A/B or 8>.

The pre-programmed connection list method

This method lets you create a list of up to 20 different Telnet sites, each with it's own short identifier, a long description, individual access keys and so on and so forth. Like the previous method, you need to create a Telnet module page that is called from some sort of menu, each module page calling up one of the pre-defined connections. Instead of the O <IP> <Port> <Mode> command at the command string, you simply put the *<connection name> command instead.

There are no advantages associated with this method over the previous one. The pre-programmed connection list is an artifact of previous versions of MajorTCP/IP that has been left in place for long-time owners of the product. It's generally preferable to use the second method over this one.

A simple reason why is the ability to change the IP adress on the fly. If you have a product like **Menu Magician**, you could alter the module page's command string, making it possible for you to change the IP adress (or any other parameter) **while the system is running.**

In the pre-programmed connection list method, each Telnet site is defined in the message files. Hence, you need to take the system down to change any parameter.

Using the Telnet module

You've defined your Generic Telnet page, you've associated it to a menu option somewhere. Now it's time to use Telnet.

*Example: The user selects "**[T] Telnet to another site**" from an "**Internet Services**" Menu.*

Enter Host Name or IP address (ie: 199.84.216.1)>

The user simply types in the Host Name (bbs.widgets.com) or an IP address here. If the user types in a host name, the DNS resolver will convert the address to an IP address. If for some reason conversion does not occur, you might want to verify your PRIDNS setting in level 1 hardware config, in the TCPLIBM.MSG message file. If the Host Name/IP adress is invalid or isn't resolved, Telnet will simply ask the question again. Typing X here will abort the Telnet session.

So the user types 199.84.216.2 and presses enter. (This is the Vircom BBS system).

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Enter Port address (ie: 23)>

The Port number corresponds to the target system's point of entry. Usually, the commonly known telnet port is 23. In some cases though, like (MUDs for instance), the port number can be radically different, like 4000. You should find out what port number to use by consulting the party that operates the site. If a user presses <enter> without specifying a port #, the system will use port 23 by default.

The user hits <enter> knowing that he'll be using port 23 by default.

Open connection in (A)scii, (B)inary or (8) Binary 8 bits mode or (H)elp>

Telnet can connect in 3 modes. (A)scii, (B)inary or (8) bits binary.

(A)scii mode is used to communicate almost exclusively with MUDs (Multi-User Dungeons). In this mode, the information you type will be sent to the application server (the Telnet site) only when you press the <enter> key. An advantage of this mode is that you have full access to all MajorBBS Global Commands. This way, you can add MUDs to your game pages in such a way that will let them believe that they are playing a game like any other MajorBBS game.

(B)inary mode is used to connect to most services. Keystrokes are processed immediately as they are typed and sent to the target system, meaning you can use control characters. The only drawback of Binary mode is the inability to use X/Y/Z modem file transfers.

(8) bits binary is perfect if you wish to do full file transfers. Unfortunately, some Unix machines cannot handle 8 bit transmissions. If you are connecting to a MajorBBS/Worldgroup system, 8 bit is the way to go if you intend to use the file libraries. Else, use (B)inary mode to be on the safe side.

(AN) mode is simply ASCII mode that addditionnally disables the **X** and **X NOW** commands. This special connection mode is used mostly in pre-programmed Telnet pages.

(AD, BD or 8D) mode: same as A, B or 8, however it shows option negociation.

(AC, AL, BC or BL) mode: same as A or B, but uses different CR/LF translation.

Note: Some systems do automatic protocol negotiation thus overiding your selection.

The user types in 8 to login into full 8 bit binary, that way he'll be able to get the most recent version of MajorTCP/IP by downloading it via Zmodem.

Telnet sessions and their effects on TCP Handles

Each incoming or outgoing Telnet uses up one TCP Handle. For more details about TCP Handles, check out NBTCP (**page 32 of this manual**). DNS and Finger requests do not use up any of your Galacticomm licenses off of your six-packs

Installation procedure for the Telnet module

Simply follow these instructions to activate the Telnet module. Don't forget that during the installation of the Core Modules (Telnet/RLogin the TCPLIB), we already installed Telnet in the menu Tree. We will repeat the installation process here simply to make the manual consistent and complete. Setting up the Telnet module should be a fairly straight-forward process.

Step by Step installation procedure for the Telnet module

STEP	Description	Done
#1	Configure the TCPTELNT.MSG file for Telnet operations	
#2	Create a generic Telnet page	
#3	Create a pre-programmed Telnet page (optional)	

Configure the TCPTELNT.MSG file for Telnet operations

Level 3 - Security and Accounting configuration

- From the main configuration menu (CNF), select **F3 - Accounting and Security**
- Press on **F8 - Search**, type **TCPTELNT.MSG**
- The first item you should find is the **SYSKEY** parameter.
- Edit each item as described below, moving from item to item using the arrow keys.
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu.

SYSKEY **Key to enter module's menu.**
MASTER or SYSOP — This is the key that a user must have in order to be able to enter the module and get the "supervisory" menu which lets you view the programmed connections. Use a key that only you and your operators can own.

DIRKEY **Key to enter module with param string.**
NORMAL — This is the key required to enter the module using a menu system parameter string. In other words, if you want your users to be able to access your pre-defined Telnet pages, they should have the key assigned to this item. By default, anybody with the **NORMAL** key can use **pre-programmed Telnet pages** that use a parameter string to define where to Telnet to.

NORKEY **Key to enter module at IP question.**
NORMAL — This is the key required for a normal user to be able to enter the module without a paramater string from the menu system. Users will be sent to the (O)pen connection choice of the telnet menu, unless they have **SYSKEY**. You can use this to limit access to the "Generic" Telnet page. By default, users with the **NORMAL** key can use this option. Because a person can go anywhere with this type of Telnet connection, it might be wise to limit this option unless your users have specific Telnet sites in mind. In other words, this key controls who can get to specify where they want to connect.

SURKEY **Key to be surcharged even when exempt.**
<empty> If a monthly, credit-exempt, user owns this key, MajorTCP/IP will apply the appropriate surcharge for the connection manually. Leave blank to disable this feature. **Note that telnet will never surcharge anyone with the MASTER key.** This key is used to charge people who have unlimited local access to the BBS (ie: are credit-exempt) but have to be charged for internet services. **The amount of the surcharge is defined in TCPLIBM.MSG, level 3 accounting and security. The name of the parameters are SUROLOC and SUROREM. Check out page 34 and 35 of this manual.**

NSURKEY **Key that will exempt from any surcharges.**
<empty> This key tells MajorTCP/IP to exempt the user from any surcharges due to usage of Telnet if everybody is normally affected by the surcharges **defined in TCPLIBM.MSG, level 3 accounting and security. (SUROLOC and SUROREM, page 34 and 35 of this manual).**

PRIVKEY **Key to telnet to privileged ports.**
<empty> This key will be required for any telnets to privileged ports (0-1023 except 23). If you leave it blank, then no special key will be required for telnets to privileged ports. This key is used only to prevent people from telnetting out to ports other than port 23 or ports over 1023. This is because most essential ports like SMTP, or NNTP are between 0 and 1023 and you do not wish to have your users mucking about with other people's servers via Telnet.

Level 4 - System options configuration

- From the main configuration menu (CNF), select **F4 - Configuration options**
- Press on **F8 - Search**, type **TCPTELNT.MSG**
- The first item you should find is the **DISCHR** parameter.
- Edit each item as described below, moving from item to item using the arrow keys.
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu

DISCHR **Disconnect Character.**
= Pressing the disconnect character key three times, with a delay of 3 or more seconds lets the user close the Telnet session. This is exactly the same as Unix-based Telnets that tells you to type ^] to close the connection. This option functions only In a binary mode connections. To disable this capability, enter an '!' exclamation point.

Note about pre-programmed connections: This feature has been superceeded by the programmed telnet pages where you can define directly on the module page's command string the location you with to automatically telnet to. The pre-programmed Telnet connection list is still supported simply to remain compatible with older sites who are still using this mode of automated Telnet connections. If you are installing MajorTCP/IP for the first time, it's suggested that you ignore the following parameter definitions of this section. If you insist on using this feature, check out the "About pre-programmed connections" section.

NBCON **Number of Connections defined**.
20 This parameter tells MajorTCP/IP the number of pre-programmed connections In the connections list specified below. The value **can range between 0 and 20**. Leave NBCON to 0 if you will not use this feature (very likely). The way to access each connection is thru a pre-programmed menu option that calls up a module page that uses the Telnet module. In the command string, you would then use the concatenated command *<name> where <name> is the connection name defined in **CONnCD. For each CONnXX parameter, n represents the n-th element of the list. XX represents what this element is. Check out section called "About the pre-programmed connections list" later in this section.**

CONnCD **Name of the Connection.**
<empty> This parameter defines the name of each connection. This name cannot be left blank because it serves as the key when the *<name> command is invoked from a Telnet module page's command string. The name of the connection cannot be more than 15 characters in length.

CONnDC **Connection's Long Name.**
<empty> This parameter defines the long name of the connection displayed to the user when the connection actually occurs. This is simply a more detailed description of the CONnCD parameter. This description can be up to 40 characters in length.

CONnNA **Internet Address of Connection**.
<empty> This is where you specify the actual IP Address of the Telnet site associated with this connection. This address can only take the numeric form. (ie: 199.84.216.2 for instance).

CONnPT **Port number to connect to.**
0 This tells MajorTCP/IP on which port Telnet should connect to on the target site. Usually, this is port #23 but it often changes depending on the service. This corresponds to the Unix ending socket number).

CONnKY **Supplemental key required to enter connection**.
<empty> Key required to have access to this connection. This lets you put in place extra keys if you want to restrict particular Telnet sites and not others. To sum up, if the user doesn't have this key, he will not have access to this connection.

CONnNK **Key that will deny access**.
<emtpy> Give the user this key and he won't be able to use this connection. This is the reverse of the **CONnKY.** Use this key if you want to give selective denied acces to each individual site. To sum up, if the user doesn't have this key, he will have access to this connection.

CONnSU **Surcharge in credits per minute for hourly users of this connection.**
0 This surcharge is in addition to the one **defined in TCPLIBM.MSG, level 3 accounting and security. (SUROLOC and SUROREM, page 34 and 35 of this manual).**

CONnMO **Mode for this connection.**
A This parameter specifies which connection mode Telnet will utilize for this particular connection. Use A for ASCII, B for MBBS Binary, and 8 for Full Binary mode.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

CONnXN **Allow X Now to exit and trap "X"**
YES ASCII mode connections normally return the message "type X NOW if you really want to exit" when the user types X alone in a connection. If you set the following option to NO this feature and the interpretation of X NOW will be disabled. In other words, use this parameter to Enable/Disable the X and X NOW commands.

Create a generic Telnet page

The generic telnet page lets your users Telnet to any telnet site as long as the IP adddess or internet address is known to them. During the installation process of the MajorTCP/IP core modules (RLogin/Telnet and TCPLIB), you already created a generic Telnet page although in this case, the page was created as a floating page detached from the main menu tree.

To create a generic Telnet page associated to a “Internet Services Menu”, simply follow these instructions. Note that this menu is used solely as an example. Simply substitute it for the menu you want to associate Telnet to. Only users who have the **NORKEY** should have access to this page.

Use the following procedure to create a generic telnet page

- From the main configuration menu (CNF), select **F2 - Design Menu Tree**
- Make sure that the menu item cursor is located on **your Internet Services page**
- Select **F2 Edit** to change the Internet Services menu
- Go to the menu options area and **add a new option**, say [T] to Telnet to another site
- In the **EDIT OPTION** window ...
    - Short Description .....could be “Telnet to another site”
    - Key required for this option..... the key you give to internet users.
    - Destination page..... could be called **GENTEL**
    - **Save the menu**. A new page in the menu tree should’ve been created.
- Move the cursor to the new page called **GENTEL.**
- Press **F2 Edit** to configure this module page.
    - Allow go to this page ..... should be set to **YES**
    - Key required ..... should be the internet key you give to your users
    - Select module window, you should chose the **Telnet Module**
    - Display header ..... should be set to **YES**
    - **The command string should be left empty**
    - Save the resulting page.
- That’s it!

Create a pre-programmed Telnet page (optional)

To create pre-programmed Telnet pages, you basically go through the same process as above, with one exception. Instead of leaving the command string empty, you can put in a scripted command that opens a connection to a specific IP address. Should you have a large number of interesting Telnet sites (like MUDs for instance), you should consider creating a Sub-menu linked to your main “Internet Services” Menu. That way, users can find all of them at the same place. Pages that make use of pre-programmed command strings should be restricted to users who own the **DIRKEY**. Don’t forget to change the destination page of each menu option. Each page must be unique. The format of the command string is thus: **O <IP address> <Port> <Mode>**

O stands for Open, and the **<IP address>** is the numeric IP address of the target Telnet site. If you don’t know the numeric IP address of the site, you can use the generic Telnet page to Telnet to the internet address instead, jotting down the number given by the DNS resolver when it does the Telnet connection.

[Vircom Inc’s MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

<Port> stands for the port number or "socket" to connect to. By default, the port to use is port #23 although this changes from site to site. For instance, to connect to some MUSES (Multi-User Simulation Environments), you have to connect to a port between 3000 and 4000 (specified by those who offer the service).

<Mode> Stands for the connection type. A for ASCII, B for MBBS Binary and 8 for 8 bit Binary. There's also a mode called "AN" that disables the X and X NOW command while maintaining an ASCII connection.

Example at the module page window, the command string field: **O 199.84.216.2 23 B**

This would open a Telnet session at the 199.84.216.2 site automatically, Port 23 in MBBS Binary mode. 199.84.216.2 happens to be our Support BBS IP adress. The BBS works off of port #23 (the default port of most Telnet sites), and is running MajorBBS.

At the end of the command string, you can now add a small description that indicates where the Telnet is going to. This description will appear in the "/#" list when you want to find out who'se online and what are the users doing. We need to add a text variable (see the Rlogin section) to the display format of that list called **TCP_RL_MOD.**

Modifying the /# command to display destination of Telnet: Detailed Procedure

- At then end of your Telnet pre-programmed page command string, add the desired caption. This is defined by adding a pound sign followed by the caption like so: #Caption . Note that Telnet will know that this isn't part of the normal Telnet string. Here is a real-world example:
- **O 199.84.216.2 23 B #Battletech**
- From the main configuration menu (CNF), select **F6 - Edit text block**
- Press on **F8 - Search**, type **ULSLIN.**
- Press on **F2 - Edit, you'll be brought into a text editor window.**
- Move your cursor to the point where you want to substitute the last parameter with the text variable. You can write over the last parameter of the string. (it starts with a % symbol)
- Press on **Alt-V** to add a server text variable. Select **TCP_RL_MOD.**
- Press on **Alt-S** to save and go to the normal CNF screen.
- Press on **F10 Save and Exit** to go back to the main configuration menu

About the pre-programmed connections list

Pre-programmed telnet connections must be defined in the TCPTELNT.MSG message file.
Lets say for the sake of argument, that we define a sample system in the Telnet connections.
The system used as an example is what's called a MUSE (Multi-User Simulated Environment). Do not try this site as the connection has likely moved elsewhere. These are the settings we will use:

Parameter	Description	Contents
NBCON	Number of programmed connections	1
CON0CD	Name of the 1st connection	Battletech
CON0DC	Detailed name of the 1st connection	Battletech Muse 3056
CON0NA	Internet address of the 1st connection	198.69.186.38
CON0PT	Connection port number	3056
CON0KY	Supplemental key required to enter connection	NORMAL
CON0NK	Key that will deny access	NOBTECH
CON0SU	Surcharge	0
CON0MO	Connection Mode (A)scii, (B)inary (8)bit	A
CONOXN	Allow X Now to exit	YES

The way you would make this particular system available to your users using the sample setup here is by simply creating a Telnet module page in the same fashion you would do for a pre-programmed Telnet page. The only thing that changes is the command string. As in this sample, the command string parameter would be: *Battletech.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

STEP #7

Configure the FTP module

Last revised, July 30th 1996.

- Added “bin” abbreviation for the “binary” command.

FTP Overview

The FTP module gives you the ability to provide your users access to the thousands of FTP archive sites around the world over the internet. You can offer your users either a generic FTP page where people specify which FTP site they wish to access, or you can create menu-ized FTP pages where you can offer pre-defined selections of FTP sites, making life easier for your users.

You can use FTP in two modes: manually and automatically.

Manual FTP: This mode works directly off of a menu option without any type of programmed command string. This means that the users must select the FTP site they wish to contact. Afterwards, the person must login with a user name and password. Usually, this means entering the word “anonymous” as login name, and the password is expected to be the user’s internet E-mail address (JohnDoe@bbs.widgets.com for instance).

Automatic FTP: This mode of operations is used when the sysop created pre-defined menu options with various pre-selected FTP sites to chose from. All the user has to do is to select the menu option corresponding to the FTP site they want to access. FTP takes care of establishing the connection, and logging-on automatically as an anonymous user, with the password being automatically derived from the user’s internet alias.

Using FTP, a typical session

Once connected (Manually or Automatically), the user can perform all of the standard FTP operations. FTP’s command set was based loosely on the Unix operating system file manipulation commands. People who are already familiar with MS-DOS will make the transition to FTP fairly easily. However, people who have never been exposed to operating systems with command line interfaces will find it a little bit more difficult to master. It’s suggested that sysops create some sort of step-by-step text-file explaining the usage of FTP.

Here’s how a person would go about using FTP manually

- Person selects the appropriate menu option that calls up the FTP module.
- At the “Enter Host Name or IP address (or ?)>“ prompt, the person types in the **internet address of the target FTP site** they wish to access. **Note that at any time during the FTP session, the user can type in “?” or “help” to get the list of commands supported by the FTP module.**

[Vircom Inc’s MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

- If the connection is successful, the person is asked to Enter a login name or type “anonymous”. Then there’s usually a request for a password. All the user has to type is his or her internet E-mail address.

- The person can navigate the various directories by type the command “**cd**” - Change directory just like in DOS, using slashes “/” instead of backslashes “\” as delimiters. They can type “**dir**” to see the content of the directory, or even “**ls**” which is the UNIX equivalent.

- Once the user found the file desired, they have to specify what transfer mode to use. They simply need to type the words “**binary**” or “**ascii**” at the prompt. Usually though, it’s preferable to always choose “**binary**”. The user can type **“bin”** instead of “binary”. It’s an abbreviation.

- The user can initiate the transfer from the target system to your machine by issuing a “**get <filename>“** command or in the case of multiple files, **“mget <filespec>“** where filespec can be any kind of spec like *.* (every file in the directory) or foo* (every file that starts with the word foo).

- The file or files are swiftly transmitted to your system in a temporary storage area. As soon as they are received, the person is prompted to see if they wish to download them to their own computer via all the protocols available to users who go into your file libraries. The user can either download them right now, or tag them for later retrieval before logoff. If the person doesn’t download them at that time, the files are deleted from temporary storage.

- The user can QUIT from the FTP session by typing “**QUIT**” or “**X**” at the prompt.

FTP Module Help Menu

cd <directory>	Change to a new directory.
pwd	Indicate the current directory.
dir	List the contents of the current directory
dir <filespec>	List the files matching the specified <filespec> that are in the directory.
get <filename>	Get a file from FTP archive site.
put <filename>	Put (upload) a file to FTP archive site.
get <fname> <fname2>	Same as get, but 'filename' will be called 'filename2' on your computer.
mget <filespec>	Get multiple files at the same time
autoprot <c>	Set your automatic download protocol to <c>
prompt	Toggle prompting between files in a mget operation.
binary	Switch FTP file transfer mode into BINARY mode
bin	Abbreviation of the binary command.
ascii	Switch FTP file transfer mode into ASCII mode
QUIT	Close (normally) this FTP session.
quote <cmd...>	Send <cmd...> directly to server. Use carefully.
verbose	Show all commands sent to server
del <filename>	Delete File.
rd <path>	Delete Directory.
md <path>	Make Directory.
X	Abort this FTP session.
help or ?	Display the help menu.

FTP and its effect on TCP Handles

Each FTP session uses up one TCP handle for the connection. In addition, when transfer from the FTP site to the BBS occurs, the FTP module uses another TCP Handle for the incoming stream of data. Check out NBTCP (**page 32 of this manual**). FTP sessions do not use up any of your Galacticomm licenses off of your six-packs.

Installation procedure for the FTP module

Setting up the FTP module is a fairly straight-forward process. We will concern ourselves strictly with the essential parameters that require appropriate data to function with your system correctly.

Step by Step installation procedure for the FTP module

STEP	Description	Done
#1	Configure the TCPFTP.MSG file for FTP operations	
#2	Create a generic FTP page	
#3	Create a pre-programmed FTP page (optional)	

Configure the TCPFTP.MSG file for FTP operations

Level 3 - Security and Accounting configuration

- From the main configuration menu (CNF), select **F3 - Accounting and Security**
- Press on **F8 - Search**, type **TCPFTP.MSG**
- The first item you should find is the **SYSKEY** parameter.
- Edit each item as described below, moving from item to item using the arrow keys.
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu.

SYSKEY **Key to enter module's menu**.
MASTER or SYSOP — This is the key that a user must have in order to be able to enter the module and get the "supervisory" menu. Use a key that only YOUR OPERATORS can have. Note that the supervisor module is not implemented yet but will be when we code the FTP server.

FTPRAT **FTP surcharge Rate (in credits per minute)**
0 — This is a surcharge in credits/minute that you wish to apply to your FTP users. This charge is added to the primary surcharge defined in TCPLIBM.MSG, level 3 config called **SUROLOC** and **SUROREM** (**page 34 and 35 of the manual**). This surcharge can also be applied to people who are normally credit exempt with the **SURKEY** defined below.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

SURKEY **Key to enforce the FTPRAT surcharge on credit exempt users.**
EXCHARGE If a monthly, credit-exempt, user owns the following key, FTP will apply the appropriate surcharge for the connection manually. Leave blank to disable this feature. Note that FTP will never surcharge anyone with the master key. The use of this surcharge is simple: You want people who have unlimited access otherwise to be charged only when they use FTP services. The default name of the Key is **EXCHARGE**, but you can modify it at your discretion.

NSURKEY **Key to exempt from any surcharges.**
<empty> This key can be used for classes which have unlimited monthly access to the internet for instance. In this case this key will exempt the user from any surcharges due to usage of FTP.

GETKEY **Keys to allow FTP transfers.**
MGETKEY This key lets you define who can actually execute transfers and who can't. This
PUTKEY feature lets you open up FTP to general usage for instance, people can browse
NORMAL the FTP sites they wish, but if they don't have this key, they can't use the GET/MGET commands to download software. This is a good key to use for demo accounts with limited internet access. They'll be able to connect to the FTP site, look around, but not download files. This lets you create an FTP teaser. The **PUTKEY** key does the same thing, except it limits uploads instead of downloads. A reason why you would want to limit the **MGETKEY** is the fact that MGET lets you get multiple files, which could tie up your bandwidth quite nicely if abused by your user.

Level 4 - System options configuration

- From the main configuration menu (CNF), select **F4 - Configuration options**
- Press on **F8 - Search**, type **TCPFTP.MSG**
- The first item you should find is the **DIRPATH** parameter.
- Edit each item as described below, moving from item to item using the arrow keys.
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu.

DIRPATH **Temporary directory path**.
.\TCPFTP.DIR Files transferred with Major FTP have to be kept into a temporary directory. Here you can specify the full path of that temporary directory. Do not put a trailing '\'. For instance, C:\FTP is acceptable. C:\FTP\ is not.

DEFEMLA **Default E-mail Address**
<empty> This is where you specify the default E-mail address that will be added to the password when the remote FTP site asks for it after entering the "anonymous" user name. This adress should be just the Host's domain name, in other words, everything AFTER the at (@) symbol. Example: If you set DEFEMLA to be bbs.widgets.com and the user 's ID is JohnDoe, the password FTP will send Is JohnDoe@bbs.widgets.com.

DSLOW1 **Minimum disk space available for FTP in megabytes.**
0 When the amount of available disk space reaches the defined number for DSLOW1, no new FTP requests will be allowed to start. (This number is in MEGABYTES). Set to 0 to disable. This number should be a multiple of DSLOW2.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

DSLOW2 **Minimum disk space available for FTP in megabytes.**
2 When the amount of available disk space reaches the defined number for DSLOW2, all current FTP sessions will be terminated (abruptly) and all files in the DIRPATH will be deleted. Set to 0 to disable. This number is in MEGABYTES. If you use this feature, this number _MUST_ be higher than the maximum amount of data that can be transferred in a minute at maximum throughput. This would be 1MB on a 56K and less and 10MB on a T1.

FTPMSS **Maximum segment size for FTP-Data in bytes**.
1024 You can define the largest size of packets sent by the remote FTP using this configuration variable. A smaller number reduces the load of FTP against interactive sessions, but also reduces the maximum throughput of FTP. If you set this number to 0 or to more than what you've defined for the **MSS** value (**TCPLIBM.MSG, level 1 Hardware config**), FTPMSS will assume the value of the MSS. **See the MSS parameter on page 31 for a detailed description of the effects of various segment sizes.**

Create a generic FTP page

When we say “create a generic FTP page”, what is really meant by that is to simply add the FTP module to the menu tree, preferably as part of another menu. Most of our clients create a generic “Internet Services” menu. So we’ll use that as our example to explain the process.

Use the following procedure to add the FTP module to the menu tree:

- From the main configuration menu (CNF), select **F2 - Design Menu Tree**
- Make sure that the menu item cursor is located on **your Internet Services page**
- Select **F2 Edit** to change the Internet Services menu
- Go to the menu options area and **add a new option**, say [F] go to the FTP module
- In the **EDIT OPTION** window ...
    - Short Description .....could be “go to the FTP module”
    - Key required for this option..... the key you give to internet users.
    - Destination page..... could be called **FTPOUT**
    - **Save the menu**. A new page in the menu tree should’ve been created.
- Move the cursor to the new page called **FTPOUT.**
- Press **F2 Edit** to configure this module page.
    - Allow go to this page ..... should be set to **YES**
    - Key required ..... should be the internet key you give to your users
    - Select module window, you should chose the **FTP module**
    - Display header ..... should be set to **YES**
    - **The command string should be left empty**
    - Save the resulting page.
- That’s it!

From this hypothetical menu called Internet Services, people will be able to select option F, described as “go to the FTP module” and call up the FTP module, letting them do a manual FTP session.

Create a pre-programmed FTP page (optional)

Creating pre-programmed FTP pages is a snap. You basically go through the same process as above, with one exception. Instead of leaving the command string empty, you can put in a scripted command that opens a connection to a specific IP address. Should you create a large number of pre-programmed FTP connections, it's suggested that you make them part of an "Interesting FTP-sites" sub-menu, off of the main "Internet Services Menu". Don't forget to change the destination page of each menu option. Each page must be unique.

The format of the command string is thus: **O <IP address>**

O stands for Open, and the <IP address> is the numeric IP address of the target FTP site. If you don't know the numeric IP address of the site, you can try to Telnet to the internet address instead, jotting down the number given by the DNS resolver when it does the Telnet connection.

Example at the module page window, the command string field: **O 199.84.216.2**

This would open an FTP session at the 199.84.216.2 site automatically. In fact, FTP when prompted will give the site the **anonymous** user name with the password being your **user's E-mail address**. All this transparently.

STEP #8:

Configure the Domain Name and Finger Servers

Module Overview

Both the Domain Name resolver and the Finger Client/Server are part of the module called TCPMISC.DLL. Because both functions are small in extent, it was decided early on to create a catch-all module that would contain all the smaller functions needed to provide internet services. Eventually, other internet services will be added to this module.

Each part of the module is distinguished by a character you specify in a module page. Basically, by putting that character in the command string section of the module page, you will invoke the corresponding service.

Letter	Function
D	Triggers the DNS resolver
F	Triggers the Finger Client

Domain Name resolver overview

You already use the DNS resolver each time you invoke a textual internet address (domain name) of the site instead of the numeric IP address. DNS will work even though it may not be present in the menu tree in the form of a TCPMISC page. What the TCPMISC module provides you is the ability to invoke the DNS as a global command. This will be only of limited use to your users, **but will make your life easier as a Sysop if you enjoy creating pre-defined Telnet, RLogin and FTP module pages**.

Example: Say you want to create a module page for an FTP site called **sunsite.unc.edu**. All you need to type at the menu prompt anywhere on the BBS is a command like **/DNS sunsite.unc.edu** allowing you to get the IP address you'll need for your module page.

Finger Client and Server overview

Finger was originally a UNIX function that was ported to MajorTCP/IP using the standard finger protocols that lets you find out who is currently on-line on a remote system both globally by fingering the site itself or particularly by fingering a specific user on the system. It also lets people elsewhere find out who is on your system at the moment. The Finger portion of the TCPMISC module is separated into two parts: **Client and Server**.

You can now invoke the finger command via the /finger global command. Note that you need to create a FINGER page as per the instructions in this chapter for this global command to work.

Finger information server

The Finger information server or more commonly called, the Finger Server is the portion of the TCPMISC module that lets people find out who is currently on your system. **You do not need to put the TCPMISC module in the menu tree** to activate this feature. All you need to do is to **Enable the Finger Server by setting the appropriate parameter** in the configuration options (described later in this section).

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

By default, the finger server gives exactly the same information as the global /# command that lets local users find out who is currently on-line. If someone fingers a specific user on your system, the only information given out is the presence of the user on the system at the moment.
You can change the information given in both instances by changing text blocks, described in the installation portion of this section using text variables.

An interesting feature of MajorTCP/IP's Finger Server is the ability to create up to five "dummy" accounts that lets you turn your Finger Server into an information server. What this means is that someone could finger these particular accounts like any other, but instead of returning standard user information, it can return an entire text-file as a reply. One of the uses made of this feature by many of our clients is to describe the services they offer to prospective users, with the going rates and contacts to gain membership. All you need to do is tell MajorTCP/IP what "dummy" account names will be used, and where to find the information on your disk (in the form of a filename).

Finger information Client

The Finger information Client or more commonly called the Finger Client lets your users find out who is currently logged-in on a remote system. They can also specify if a particular user is logged-in or not. When your users Finger a particular person on a Unix machine, the information returned contains stuff like: the last time the person was connected, if the person read his e-mail or not, where to contact the person voice (if specified) and so on and so forth. **You need to put the TCPMISC module in the menu tree to offer Finger Client capability.**

Finger and DNS and their effects on TCP Handles

Each Finger or DNS request for information uses up one TCP Handle. For more details about TCP Handles, check out NBTCP (**page 32 of this manual**). DNS and Finger requests do not use up any of your Galacticomm licenses off of your six-packs.

Installation procedure for the TCPMISC module

Installing the TCPMISC is fairly easy. Described below is the series of steps required to activate all of the features contained therein. In fact, here's a small summary of what you need to configure to offer each TCPMISC service:

Service	Need
DNS resolver	TCPMISC.MSG & module page invoking it with "D" in the command string
Global DNS	TCPMISC.MSG properly configured
Finger Client	TCPMISC.MSG & module page invoking it with "F" in the command string
Finger Server	TCPMISC.MSG properly configured with appropriate text blocs / text files.

Step by Step installation procedure for the TCPMISC module

STEP	Description	Done
#1	Configure the TCPMISC.MSG file	
#2	Create the DNS Resolver page (optional)	
#3	Create the Finger Information Client page (optional)	

Configure the TCPMISC.MSG file

Each parameter of the TCPMISC.MSG file applies only to specific functions of the module. To make your life easier, we will note which function these parameters are associated with. You can thus ignore those configuration parameters that you will not make any use of.

Level 3 - Security and Accounting configuration

- From the main configuration menu (CNF), select **F3 - Accounting and Security**
- Press on **F8 - Search**, type **TCPMISC.MSG**
- The first item you should find is the **DNSKEY** parameter.
- Edit each item as described below, moving from item to item using the arrow keys.
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu.

DNSKEY **Key for DNS Lookups**. Required for **DNS Resolver page** and **Global DNS**.
<empty> This key is required to permit users to use the DNS Resolver explicitly. It is Not required for general DNS usage by Rlogin, Telnet, FTP and other modules.

FINKEY **Key for Finger requests.** Required for the **Finger Client page** only.
<empty> This key is required to permit users to use the Finger Client. It is not required for the Finger information server.

Level 4 - System options configuration

- From the main configuration menu (CNF), select **F4 - Configuration options**
- Press on **F8 - Search**, type **TCPMISC.MSG**
- The first item you should find is the **DNSGLOB** parameter.
- Edit each item as described below, moving from item to item using the arrow keys.
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu.

DNSGLOB **Global DNS lookup command**. Required only for **Global DNS** requests.
/DNS This is the parameter you use to define which command people can use to invoke the Global DNS Resolver. **Clear it to disable this function**.

FINCGLOB **Global Finger Command.**
/FINGER This is the global command for Finger Queries. **Clear to disable**. **Only users that have the FINKEY will be able to use the global.**

Note: in order to use this global command, you must havedefined a FINGER page that is accessible through the /GO command. Make sure this page is working by doing /GO FINGER. Doing the /FINGER command is the equivalent of /GO FINGER <parameter>. (The FINGER page can be an orphan page).

FINENAB **Finger Server activation**. Required for **the Finger Information page and the**
NO **Finger Server.** Setting **FINENAB to YES** lets people on the BBS issues finger requests. It also lets people from the outside world find out who is online at the moment. You can disable outside requests while maintaining Finger Information Client capability by setting **ENABF1 and ENABF2 to NO** (described later in this section).

FINMAX **Maximum concurrent Finger Server users.** Required for the **Finger Server**.
3 Tells MajorTCP/IP how many finger requests your system will accept from the outside world at any given time simultaneously. Each finger request eats up one TCP Handle from your NBTCP count. (Located in level 1 Hardware configuration in the TCPLIBM.MSG message file. **Check out page 32 of this manual**.) **This option is visible only when FINENAB is set to YES.**

FINTRL **Display finger requests in the audit trail.** Not required but useful for both
NO Finger Client/Server modes. If enabled, any kind of finger request is logged in the audit trail. At first, it may not be obvious why you would want to log this information. In fact, there is one major reason: Excessive usage of finger may mean that your system is under hacker attack. Because someone can find out who is logged in on your system via finger requests, a hacker can at least get account user-IDs that way. All he needs to do then is to crack the passwords. If your users select "Standard" passwords, this may be all too easy to do for even a mildly skilled hacker. Passwords such as their first or last names, common swear-words or sexually explicit words are often used as passwords. Hackers know this, so it's important for you to educate your users about password selection. **This option is visible only when FINENAB is set to YES.**

ENABF1 **Enable finger to return the list of on-line users**. Needed only for the **Finger**
NO **information Server**. When someone attempts to finger @yoursystem.com, the system returns information as specified in the TXTF10 to TXTF12 messages under level 6 Message text blocks configuration. Check out the Galacticomm MajorBBS or Worldgroup manuals for more information about text blocks and text variables. You can use the default TXT file settings. The information given out is limited to the same information given out by the /# global command. **You can turn on/off ENABF1 by setting it to YES or NO. This is useful if you wish to provide Finger information Client services without letting people in the outside world looking into your own system. This option is visible only when FINENAB is set to YES.**

ENABF2 **Enable finger to return information on a user.** Needed only for the **Finger**
NO **information Server.** When someone attempts to finger a particular user with the finger someuser@yoursystem.com on their system, MajorTCP/IP returns the information as described using the format specified in the TXTF20, 21,2D and 2E message blocks. The information returned is limited to the presence or absence of the user on the system at the moment. **Like ENABF1, you can turn on/off ENABF2 by setting it to YES or NO. Useful if you wish to provide Client services without letting outsiders peek into your system. This option is visible only when FINENAB is set to YES.**

FINGEN **Enable generic accounts for finger.** This turns on the **Finger information**
NO **Server's special functions** that let you create up to 5 generic finger accounts with associated text files to provide finger infromation services to the outside world. If set to YES, you should be able to set FINGnU and FINGnT to the desired values. (n is a digit from 1 to 5).

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

FINGnU **Generic Account for Finger**. Only used with the **Finger information server.**
<empty> These fields (FING1U to FING5U) let you define up to five generic or "dummy" accounts that will refer to a text-block or text file that will be sent to the person doing the fingering. The messages are specified in the FINGnT parameters. Note that the user ID specified here should be a valid internet name thus subject to the limitations of internet names (no spaces, no punctuation except the underscore, etc ...). **This option is visible only when FINGEN is set to YES.**

FINGnT **Text block refered by the Generic Account.** Only used with the **Finger**
<empty> **information server**. (FING1T to FING5T) These are the text blocks that will be returned when the Finger Server is queried about the previously defined generic user. Text Variables work here and you can also point to a file by entering **$path\filename.ext**. Nothing else should be in the text block if you're pointing to a file. **This option is visible only when FINGEN is set to YES.**

Create the DNS Resolver page (optional)

- From the main configuration menu (CNF), select **F2 - Design Menu Tree**
- Make sure that the menu item cursor is located on **your Internet Services page**
- Select **F2 Edit** to change the Internet Services menu
- Go to the menu options area and **add a new option**, say **[D] resolve an internet adress**.
- In the **EDIT OPTION** window ...
    - Short Description .....could be "resolve an internet adress"
    - Key required for this option..... the key you give to internet users.
    - Destination page..... could be called **DNSRES**
    - **Save the menu**. A new page in the menu tree should've been created.
- Move the cursor to the new page called **DNSRES**
- Press **F2 Edit** to configure this module page.
    - Allow go to this page ..... should be set to **YES**
    - Key required ..... should be the internet key you give to your users
    - Select module window, you should chose the **TCPMISC** Module
    - Display header ..... should be set to **YES**
    - The command string should have the letter **D**
- Save the resulting page.
- Done.

Create the Finger Information Client page (optional)

- From the main configuration menu (CNF), select **F2 - Design Menu Tree**
- Make sure that the menu item cursor is located on **your Internet Services page**
- Select **F2 Edit** to change the Internet Services menu
- Go to the menu options area and **add a new option**, say **[F]inger someone over the net**.
- In the **EDIT OPTION** window ...
    - Short Description .....could be “[F]inger someone over the net”
    - Key required for this option..... the key you give to internet users.
    - Destination page..... could be called **FINGER**
- **Save the menu**. A new page in the menu tree should’ve been created.
- Move the cursor to the new page called **FINGER**
- Press **F2 Edit** to configure this module page.
    - Allow go to this page ..... should be set to **YES**
    - Key required ..... should be the internet key you give to your users
    - Select module window, you should chose the **TCPMISC** Module
    - Display header ..... should be set to **YES**
    - The command string should have the letter **F**
    - Save the resulting page.
- Done.

[Vircom Inc’s MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

STEP #9:

Configure the World-Wide-Web Server

Last Revised January 20th 1997.

- Added new configuration option **SECONL** in CNF level 3, accounting and security. This option lets you decide to prompt a user you know comes from your BBS for a user ID and password when accessing protected pages on your server.
- Added new configuration option **OBUFSIZ** in CNF level 4, configuration options. Similar parameters were added to other modules and their effect are discussed in the **Performance Optimization chapter in the annex**.
- If you are upgrading from the TCPWWW module to the new TCPWEB2 module, dropping the old web server program, read the section at the end of this chapter called **"Moving over to the new web server, some tips".**
- Added some details about protecting subdirectories with the ACCESS.CTL file and other features.
- Now accepts internet aliases as a substitute to the standard UserID if a person, when queried to enter his username and password to see a page. This assumes of course that you use the internet alias file.
- Added application/pdf to **TCPMCTYP.TXT** file.

Module Overview

The World-Wide-Web is the most recognizable aspect of the Internet that is usually associated with the media's insatiable desire to talk about the "information superhighway". The WWW is in fact the aggregate result of a huge number of Web servers that all talk a common language called HTML or Hyper-Text Markup Language. **Our Web server lets you put up your own web pages**.

HTML lets you combine, text, sounds and graphics all in one integrated document. HTML is simple to use and learn, and once mastered, can let you create an awesome variety of hyper-text documents, referring to other resources all over the net including those on your own system.

The World-Wide-Web servers are but one aspect of the whole web. To be able to see these HTML documents, users must use Web Browsers. The most commonly known of these are Lynx (on the Unix platforms), Netscape, Microsoft Internet Explorer and Mosaic (on the PC platforms).

Basically, a Web Browser makes a request for a page to the server, and the server obliges. It doesn't need to know HTML, all it needs to know is how to respond to URL (Universal Resource Locators) requests which is basically the Web Browsers way of asking for a given page of information, where information can take different forms. Most of the work of interpreting the HTML document is done by the Browser.

The World-Wide-Web Server, what's new?

Aside from the cut-and-pasted intro. here, just about everything has changed with the new web server. This is a major revamping of the original TCPWWW module. In fact, the new web server is a totally NEW module that will replace your TCPWWW module. You can deactivate the old web server module or you can run both the TCPWWW and TCPWEB2 modules side by side by assigning a different port number to the TCPWEB2 server module. Of course, why someone would want to do this is left as an exercise to the reader.

New Web Server features:

- **WG 2.0 compatibility:** The new web server is compatible with Worldgroup 2.0 and the WG 2.0 Netscape plug-in. All you need to do to install the plug-in is follow the instructions specified by the WG 2.0 manual. They apply both for the WG2.0 web server and the MajorTCP/IP web server.

- **HTTP 1.0 Compatibility:** Our new web server is now fully compatible with the HTTP 1.0 standard. This means that AOL members surfing the net will be able to view your pages. The original web server included with MajorTCP/IP only supported HTTP 0.9 which created some problems with people that didn't have backwards-compatible browsers like the folks using the AOL web browser.

- **Doesn't use user-count licenses:** To continue with the tradition of alleviating the need to use six packs, MajorTCP/IP's web server does not use any user-count licenses. This is important because even a single user connecting via Netscape generates 4 simultaneous web hits. That's four licenses off of a six pack. If you intend to operate a high-traffic website, this feature can save you hundreds of dollars simply because you don't need to purchase extra six-packs.

- **Clickable Image Maps:** The web server now supports images maps. If you're not familiar with the World-Wide-Web, an image map is simply a picture with various "hotspots" that bring the user to another location. That means you can draw various pictures with buttons and icons on them that will scoot the user off to a desired location, on your web server or out on the World-Wide-Web..

- **Form to File Support:** We now fully support the FORM GET method. You can now specify a file where the data submitted in the form will be saved to. This is different from the old method with the TCPWWW module where everything would wind up in the TCPWWW.LOG file.

- **Form to Email support**: In addition to the standard Form-to-File support, the New Web server is capable of sending any data entered thru a form to an E-mail using the same legible format used by the Form-To-File system. You can even have the person filling out the form put in something in the "Subject:" line, and the "Mail From:" line.

- **True Subdirectory Redirection:** The original web server that came with MajorTCP/IP had an annoying problem. If someone on the world-wide-web tried to refer to a sub-directory without referring to the index page therein, the browser would find the index.htm from that page, however all references within that **index.htm** page had to be absolute because the browser didn't know we had changed directories.

  Say someone did **http://www.widget.com/somedir** and **somedir** is a subdirectory. The browser would return the following page: **http://www.widget.com/somedir/index.htm** which is essentially correct.

  However, if **index.htm** made references to relative URLs, say, a picture in the same directory as **index.htm** called **picture.gif,** the web browser would try to access **http://www.widget.com/somedirpicture.gif.** A slash is missing between **somedir** and **picture.gif**.

This problem has been fixed in the new web server. Because of this, it will be possible to have folks refer to a subdirectory instead of the index page of that subdirectory. The **index.htm** file will be loaded automatically, and any file or object referenced by this **index.htm** page will be fetched appropriately.

So, basically, instead of having to do: **http://www.widget.com/kevin/index.htm,** people can now do **http://www.widget.com/kevin** and **index.htm** will be loaded automatically. Any reference to other documents within the index page will be accessed properly.

- **Page protection by Key or IP Address:** Password security is now possible with Vircom's new web server. You can create web pages that are only accessible by users of the BBS via their username and password using specific access keys for each of your pages. Only the key owners will be able to access those pages after typing in a proper username and password. You can also restrict access to a block of IP addresses, or a combination of both.

- **Combined Log Format:** The MajorTCP/IP Web Server is now compatible with the log format standard used by the majority of web servers on the market. This means that statistical packages like Web-Trends will be able to read your server activity log and use the data to create statistical reports.

- **Account information**: It is now possible for users to find out the status of their account on the BBS via the world-wide-web by simply accessing a special URL.

- **VRML, JavaScript and Java Compatibility:** The new web server is capable of handling VRML documents, JAVA scripts and Java Applets (not fully tested yet, since the applets that are out there use long file names. Since MajorBBS/Worldgroup runs under DOS , that causes a problem).

The New World-Wide-Web server and its effect on TCP Handles

Each user that generates a “Web Hit” (access a page) uses up one TCP Handle (NBTCP) and one file handle (defined in your CONFIG.SYS). The WEB2MAX value described in this section specifies the maximum number of hits allowed (ie: the number of people who are getting a page or graphic from your server simultaneously). Netscape (and other web browsers) by default generate four simultaneous web hits. Because of this, if you want to handle more than a couple of users connected to your web server simultaneously, you should increase WEB2MAX at 4 units per user. You will **want to increase your FILES statement in the CONFIG.SYS file by the same number.** For the details about NBTCP, check out **page 32 of the installation manual**.

Installation procedure for the TCPWEB2 module

Configure the TCPWEB2.MSG file

Level 3 - Accounting and Security

- From the main configuration menu (CNF), select **F3 - Accounting and Security**
- Press on **F8 - Search**, type **TCPWEB2.MSG**
- The first item you should find is the **SECFIL** parameter.
- Edit each item as described below, moving from item to item using the arrow keys.
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu.

SECFILName of access control file.

access.ctl — You can define an access control file that can be used to restrict access to WWW pages to users that have an account on your BBS and a specific key. The format of that file is:

<files/filename.ext> <KEY>
<files/filename.ext> <IP-address>

files/test.zip normal -> Restricts files/test.zip to NORMAL key owners
files/test.zip 199.84.216.* -> Restricts files/test.zip to people from 199.84.216.1 to 199.84.216.255.

SECLTIM **How often should access.ctl be checked for changes (in minutes).**

1 — This tells MajorTCP/IP how long to wait between reloads of the access file in minutes. Set to 0 to disable reloading, or a value between 1 to 60 minutes..

SECONL **Prompt users for password if we know who they are.**

NO — When a page is protected by key, Web2 will usually make the browser prompt the user for a userid/password. However, when a user is connected to the BBS using SLIP/CSLIP/PPP or RADIUS, we already know (from the IP address) who the user is and which key he has. When SECONL is set to NO, we will use this information instead of prompting the user.

Level 4 - System options configuration

- From the main configuration menu (CNF), select **F4 - Configuration options**
- Press on **F8 - Search**, type **TCPWEB2.MSG**
- The first item you should find is the **WEB2ENAB** parameter.
- Edit each item as described below, moving from item to item using the arrow keys.
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

WEB2ENAB **Enable WWW Server.**
YES This parameter tells MajorTCP/IP if you wish to activate the Web Server or not. Simply set it to YES to activate it. If it's set to NO, many of the TCPWEB2 parameters will remain invisible.

WEB2MAX **Maximum concurrent WWW Server users.**
10 This tells MajorTCP/IP how many incoming simultaneous "web-hits" you will accept for your BBS. Each incoming connection uses up one TCP Handle (NBTCP) and one File Handle. This means that for a WEB2MAX of 10, you should increase the FILES statement in CONFIG.SYS by 10. Setting this value to 0 actually sets WEB2MAX to a default value of 40. **NBTCP refers to the TCPLIBM.MSG parameter in level 1 hardware config, on page 32 of the installation manual. WEB2MAX is visible only if WEB2ENAB is set to YES.**

WEB2HOST **Base Host Name.**
<Empty> For redirection purposes, WEB2 must know what is the host name it's known under. If your Web2 server is called as www.yourdomain.com, then enter this in WEB2HOST. If WEB2HOST is left blank, then we'll be using the combinaison of hostname.domname as defined in TCPLIBM.MSG, level 1 hardware configuration.

As to the "why?" of this option ... when you do subdirectory redirection or image map redirection, MajorTCP/IP must send the hostname of the web2 server in the redirection packet. MajorTCP/IP was using hostname.domname, but some sysops have an alias pointing at the BBS (like www.theirdomain.com) and they don't want the HOSTNAME/DOMNAME to show (like theirdomain.com. This will do it.

WEB2MSS **Maximum Segment size of WWW Server Connections.**
512 You can change this value to alter the performance of your system. The smaller the packet size, the less impact WWW transfers will have on your other services. However, WWW Server throughput will be reduced. Leave to 0, to use the default, system-wide MSS. If WEB2MSS is larger than the system-wide MSS, MajorTCP/IP will use the system-wide MSS as the default. For more information concerning MSS, **check out page 31 of the installation manual describing the system's MSS. WEB2MSS is visible only if WEB2ENAB is set to YES**.

WEB2PORT **Port number for incoming Web contact.**
80 The normal WWW port used by browsers and servers is port 80. This option allows you to change the port number used by this WWW server to listen for WWW calls on. If you change it to 8000, then WWW browsers can be told to use this port using the following syntax in an URL:

http://www.domain.com:8000/whatever page.

Typically the alternative port number often seen for web server is 8000.

AXSFILLog all attempts to access your web.
YES You can log all attempts to access your web site. Choose YES to log all attempts. his log follows the "combined log format" used by other WWW Servers (unix and NT based). You can then analyze this log file using standard WWW log file analyzers. **This parameter is visible only if WEB2MAX is non-zero.**

AXSFILN **Access log filename.**
webaccess.log This is the file where all access attempts are logged to. This file resides in the <WEBPATH> (usually TCPWEB2) directory. **This parameter is visible only if AXSFIL is set to YES.**

AGTFIL **Log all client versions in a separate file.**
NO You can log all user-agents (e.g. Netscape) connecting to your Web server in a. separate file. Choose YES to enable this option. The data will be stored in the file specified in the AGTFILN parameter, in addition to logging everything in the combined log (AXSFILN). Since this duplicates the information recorded in the AXSFILN log, chances are you will not activate this option. Choose **This parameter is visible only if WEB2MAX is non zero.**

AGTFILN **Agent log filename.**
webagent.log All agents connecting to your World-Wide Web site will be logged to this file. This file resides in the <WEBPATH> (usually TCPWEB2) directory. **This option is visible only if AGTFIL is set to YES.**

ERAFIL **Log all error attempts to access your web.**
YES You can log all erroneous attempts to access your web site. Choose YES to log all error attempts. **This option is visible if WEB2MAX is non zero.**

ERAFILN **Error log filename.**
weberror.log All erroneous attempts to access your World-Wide Web server will be logged to this file. This file resides in the <WEBPATH> (usually TCPWEB2) directory. **This option is visible only if ERAFIL is set to YES.**

INTMOUT **WWW Server Timeout (minutes).**
2 This is the timeout for incoming WWW server connections. This timeout will be triggered after n minutes waiting for a WWW request or waiting for a block of data sent to be acknowledged.

OBUFSIZ **WWW output socket buffer size.**
2048 This sets the size of the output buffer for WWW sockets. The larger the buffer, the better the performance of the WWW server. However, this also increase the amount of memory taken for each WWW socket. **Check out the Performance Optimization section in the annex for further details.**

WEBPATH **Master WWW Directory.**
TCPWEB2 WEBPATH defines the master directory where all other WWW directories, log and work files will be located. The webpages will always be coming from a subdirectory called WEBPAGES, and the imagemap files will be coming from a subdirectory called IMAGEMAP. **This option is visible only if WEB2MAX is non zero.**

IMGPFIX **URL prefix for Image maps.**
imagemap URL path prefix you will use for your clickable image maps referenced in your HTML pages. Example: if this option is set to "imagemap", you might have the following clickable image in an HTML file:

<A HREF="http://company.com/imagemap/photo.map">
<IMG SRC="http://company.com/photo.gif" ISMAP> </A>

Then, assuming WEBPATH is set to TCPWEB2, the file TCPWEB2\IMAGEMAP\PHOTO.MAP would have the list of clickable regions and destination URL's. The file TCPWEB2\WEBPAGES\PHOTO.GIF would have the image itself. **This option is visible only if WEB2MAX is non zero**.

DFTFIL **Default "/" page for WWW Server**
INDEX.HTM This is the default HTML page that will be sent when a WWW client sends the GET / request. **This option is visible only if WEB2MAX is non zero**.

FLROOT **FORMS-TO-FILE directory.**
FORMFILE This is the directory where to store forms-to-file information received from Web browsers. The names of the files in this directory are specified in the URLs of the ACTION attribute in the FORM element of your HTML pages. Those URLs must use the prefix specified in FFLPFIX (see next option).

Note that this directory will be under the directory you have defined above in <WEBPATH.>

For example, <FORM ACTION="http://www.yourcompany.com/formfile/litreq.txt"> can specify that filled-in form information should go into C:\WGSERV\TCPWEB2\FORMFILE\LITREQ.TXT (assuming FFLROOT=FORMFILE and FFLPFIX=formfile and WEBPATH=TCPWEB2).

FFLROOT is the PHYSICAL location where the form files will be stored.

FFLPFIX **FORMS-TO-FILE URL prefix.**
formfile This is the URL prefix for the ACTION attribute in the FORM element of your HTML, for forms you wish to be handled by Forms-to-file. This comes after your host name and before the form file name.

For example, <FORM ACTION="http://www.yourcompany.com/formfile/litreq.txt"> can specify that filled-in form information should go into C:\WGSERV\TCPWEB2\FORMFILE\LITREQ.TXT (assuming FFLROOT=FORMFILE and FFLPFIX=formfile and WEBPATH=TCPWEB2).

FFLPFIX is the LOGICAL location, or URL used to indicate that the file is a form file. When the browser performs a SUBMIT, MajorTCP/IP knows that the file after the FFLPFX statement will be stored in the FFLROOT directory.

FFLMAX **Maximum size of forms recording files.**
1000000 This is a limit on the total number of bytes to be stored in the FFLROOT directory. This directory contains the files where all Forms-to-file data will be stored. Usually this data comes from Web users who fill in forms supplied by your Web server (but this cannot be completely verified). This limit can protect your hard disk from getting filled up with Forms-to-file data.

FFLCRE **Create Form Response file if not there.**
NO You may not want people to start creating form response files other than the one you specifically created. Set FFLCRE to NO, and TCPWEB2 will not create a form response file, it will just append to an existing one. If you set to YES, the possibility exist that malicious WWW surfers could start creating lots of dummy files in the formfile directory.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

IMGLOC **Get image maps from the WEBPAGES hierarchy.**
NO The IMAGEMAPS are usually retrieved from the <WEBPATH>\IMAGEMAP directory. If you set this option to YES, they will be retrieved from the <WEBPATH>\WEBPAGES directory (or any sub-directory of WEBPAGES). In other words, it lets you override the normal IMAGEMAP directory and store the image map files anywhere in webpages hierarchy.

LOGLOC **Write Access log into the WEBPAGES directory.**
NO The Access Log file is usually recorded in the <WEBPATH> directory. If you set this option to YES, it will be recorded in the <WEBPATH>\WEBPAGES directory (or any subdirectory of WEBPAGES). Note that this means that anyone can retrieve the file, unless you protect it with a key in the access.ctl file. In other words, it lets you override the normal IMAGEMAP directory and store the image map files anywhere in webpages hierarchy.

FEMPFX **Forms-to-e-mail URL prefix.**
frmemail This is the prefix the web server will check for to know it is dealing with a forms-to-e-mail web page. For example, if the HTML file contains:

<FORM ACTION="/frmemail/user@domain.org">
Then this module will recognize the form as one it should handle. (As you can see, the destination e-mail address is also specified in the ACTION URL.) Note that only SMTP Internet Emails can be sent.

FBKTO **Fallback to address.**
Sysop If the form's ACTION URL contains a missing or invalid-mail address, the Email message with the form responses will be sent to the e-mail address you specify here.

FBKFRM **Fallback from address.**
Sysop If the form contains a "From Address" field, for example:

<INPUT TYPE="hidden" NAME="From Address" VALUE="user@domain.com”>
<INPUT NAME="From Address" SIZE=50 MAXLENGTH=50>

Then the e-mail message with the form responses will be identified as having come from that e-mail address. (The From Address field may be hidden, or the user may have entered it.) If the form does NOT contain a "From Address" field, however, the address you specify in the FBKFRM item is used instead. (in this case, sysop)

FBKTPC **Fallback Topic.**
Form Response If the form contains a field named "Topic", for example:

<INPUT TYPE="hidden" NAME="Topic" VALUE="Some Topic”>
<INPUT NAME=“Topic” SIZE=50 MAXLENGTH=50>

The e-mail message with the form responses will use that value as the topic of the message. (The Topic field may be hidden or the user may have entered it.) If the form does NOT contain a "Topic" field, however, the topic you specify here is used instead.

STSPFX **Account Status URL prefix**
acctstat The account status URL allows users to have a look at their account's information, like which class they are in, how many credits are left. This is configured in text block (level 6) STSTXT. This is the prefix that must be at the beginning of the URL to activate the account status module.

http://www.test.com/acctstat/

Will show the status of the user's account. If we don't know who is the user yet, we'll authenticate him automatically. To disable, clear STSPFX.

STSKEY **Key to be able to see account status.**
<empty> A user must have this key in order to see it's account status over the WWW. Clear to allow everyone to see it.

STSNKEY **Key to disable account status.**
<empty> If a user has this key, he won't be able to see his account status over the WWW. Clear to allow everyone to see it.

Notes about using the web server

Once the server is up and running, there are a few questions that need to be answered.

How do I give MY users access to my web pages?

You need to run the SLIP/CSLIP/PPP server to do that. The SLIP/CSLIP/PPP server provides your users with SLIP, CSLIP or PPP connectivity. They need to run a program called Trumpet Winsock (or any other winsock-compatible TCP/IP stack) or Win95 with it's built-in TCP/IP capability and a windows-based Web Browser like Netscape or Mosaic. From that point, they can go and visit your web pages, or any other page on the internet.

How do I provide home-page services to my users?

There are now third party products on the market that are much better at managing home-pages than using this kludge that are truly maintenance free. You are advised to log-on to our support BBS to find out from us or other sysops.

One way to offer home-page services is to use a method that is relatively maintenance-free for you, that is, using individualized software libraries to give users the facilities necessary to add and remove pages from their home-page directory.

- Create a subdirectory of the directory specified in the **<WEBPATH>\WEBPAGES** directory.
- Create a new file library pointing at the sub-directory previously created.
- Provide access to this Library solely to the owner of the home page area using a custom key.
- Provide the user with a generic **INDEX.HTM** that will serve as his default/index page.

Create a subdirectory of the directory specified in <WEBPATH>\WEBPAGES

Lets assume that the directory specified in **<WEBPATH> is TCPWEB2**. The webpage directory is thus TCPWEB2\WEBPAGES. All you need to do in John Doe's case (our hypthetical home-page user) is create a directory called say, JOHNDOE. We wind up with at sub-directory called **TCPWEB2\WEBPAGES\JOHNDOE.**

Create a new file library pointing at the sub-directory previously created.

Use the MajorBBS/Worldgroup facilities to create a new File Library for our generic home-page user called John Doe.

- Log-on to your BBS as Sysop (or user with Sysop keys)
- Menu option (L) ..... Go into the Libraries area
- Menu option (O) .... Go into the Operations menu
- Menu option (C) ..... Create a new file Library
- Name of Library ..... John Doe's home pages
- DOS-ONLY ..... should be set to NO
- Short Description.... Whatever suits you or your user John Doe.
- Long Description ... Whatever suits you or your user John Doe.
- Alternate File Path should be **TCPWEB2\WEBPAGES\JOHNDOE**
- Hidden Library ..... set to NO
- Copy from CD ..... set to NO
- Read/Only ..... set to NO
- Record in Audit ..... set to YES both for Uploads and Downloads
- Stop Connect ..... Depends on how you do your billing
- Charge per File ..... Depends on how you do your billing
- Charge per K ..... Depends on how you do your billing
- Max num of Files .. Whatever you find suitable
- Max num of Bytes.. Depends how much area you wish to give per user
- Max size of File ..... Whatever you find suitable
- Keys ..... **JOHNDOE** (We will create it later)
- Primary Lib-Op..... John Doe
- Save or Quit ..... Select SAVE.

We're done. You now have a file Library only accessible by John Doe (once we create the JOHNDOE key of course) that refers to the TCPWEB2\WEBPAGES\JOHNDOE directory where all his pages will be stored. This means that John Doe will be able to maintain his own directory without your intervention. In addition, the File Libraries provide you with the perfect means to charge your user (Charge per File or per Kilobyte) and limit how much resources he or she takes (limit on the disk space used).

Give access to this Library to the owner of the home page area using a custom key

We've created John Doe's Library which points to his home-page directory. We made it so that only people with the JOHNDOE key can access this Library. We need to go and create a key called **JOHNDOE** for our user John Doe.

- Log-on to your BBS as Sysop (or user with Sysop keys)
- Menu option (S)..... Remote Sysop functions
- Menu option ACCOUNT .... Accounting functions sub-menu
- Menu option EDIT ..... Edit a user's individual keys
- Edit keys for which user? .. Enter the User ID, in this case, **John Doe**
- Enter a key name (...) ..... Type in his unique key, **JOHNDOE**

John Doe now owns the key required to access the File Library system to maintain his home-pages.

Provide the user with a generic INDEX.HTM that will serve as his default/index page

Sub-directories can have their own INDEX.HTM page that will be called up automatically if someone tries to browse the directory without specifying any page. This is the perfect place for you to create a generic home-page called INDEX.HTM that could have a built-in link to your main INDEX.HTM page in the **TCPWEB2\WEBPAGES** root directory. Your user could use it as the basis to create an index to his own pages for instance. You have our permission to use the Widgets BBS demo pages as a basis to create an INDEX.HTM for yourself or for your users.

How does someone access pages on my system?

For the sake of this example, lets say our friend John Doe creates a page called **HOBBIES.HTM** and **RESUME.HTM** that are **linked to his own INDEX.HTM** page using local URLs. These are stored in the **TCPWEB2\WEBPAGES\JOHNDOE** directory with his INDEX.HTM page

Here is how someone using Netscape would get to John Doe's pages:

http://bbs.widgets.com/johndoe/	Fetches his INDEX.HTM page by default.
http://bbs.widgets.com/johndoe/resume.htm	Fetches his resume page.
http://bbs.widgets.com/johndoe/hobbies.htm	Fetches his hobbies page.

Note that you do not need to specify the TCPWEB2\WEBPAGES directory. That's because it's defined as the root directory for the web pages. As far as it's concerned, TCPWEB2\WEBPAGES is actually just the the \ directory. You can't go higher than that in the directory hierarchy. This has the side-effect of protecting the rest of your hard disk from unwanted intrusion.

Where do I find out how to do my own web pages?

To create HTML documents, you should find a good book about the subject in any well-stocked computer book store. One book we've used is the HTML Sourcebook by Ian S.Graham (ISBN 0 471-11849-4) which gives you a detailed run-down of everything that has to do with HTML, HTTP and other World-Wide-Web features. This in no way means that the book is the THE authoritative source for HTML information, but it's a good start.

One handy little product we've found is an HTML quick-reference card produced by SSC (Specialized Systems Consultants) which can be contacted at these phone numbers:
(206) FOR-UNIX / (206) 782-7733, FAX (206) 782-7191 and E-mail at sales@ssc.com.
Ask for their HTML Quick Reference.

Other documents you can check out on the world-wide-web itself were actually created by those who built it in the first place. You can check out these URLs:

http://www.ncsa.uiuc.edu/demoweb/html-primer.html
This is an HTML primer written by the same workgroup that brought us the world-wide-web in the first place. It's very complete and includes working examples of each feature you can use in basic HTML documents. And it's free.

http://www.hwg.org/
This is the HTML writer's guild homepage. It contains information about standards, tips and techniques used by people who do web pages for a living. They are a very good source of information for both the experienced webmaster and the webnewbie alike.

http://www.tucows.com/
The TUCOWS site (or The Ultimate Collection of Winsock Software) has a comprehensive list of all the popular PC-based HTML editors, most of them windows-based. Each editor is reviewed and scored against one another (A five "cow" products is way better than a product with two and a half cows) and include links to the FTP sites where these can be downloaded from directly at the click of a mouse.

http://www.yahoo.com/Computers_and_Internet/Internet/World_Wide_Web/
The Yahoo pages offer directory services to over 50000 web sites on the internet covering almost as many subjects of interest. This URL points to the Yahoo directory of Web Resources that include pointers to HTML Primers, Editors, standards and other neat stuff about the Web. It's suggested that you browse those pages because there are several gems contained therein.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Creating a simple web page

This section is only meant to give you a taste of what HTML is all about. You can do HTML with any kind of text editor on the market, but ultimately, should you start making large amounts of HTML pages, you should find a good HTML editor to work with.

HTML stands for Hyper Text Markup Language, which is used to create multi-media documents combining text, images, sounds and even animation in some circumstances. HTML was created with one goal in mind: to create the means to connect information together that does not require any programming skills. HTML uses what are called "tags" to tell the client's Web Browser how to display the various information on the client's screen. The gruntwork is done by the client's machine.

We will create the **SAMPLE.HTM** page which will contain the name of your computer system, and a paragraph of information about it.

Notes about HTML tags

First, what is a tag? A tag is an element of HTML that tells the Web Browser that is reading the file how to display information. Tags start with a less-than "<" sign and end with a greater-than ">" sign. What's in between are the commands to the browser.

You've got two major types of tags: Open-Ended tags or "empty" tags, and Paired or "non-empty" tags. Open-Ended tags are tags that can appear anywhere in a document. Paired tags indicate the start and ending of a section that is affected by a given formatting command. Note that HTML is case insensitive. That means that there is no difference between using <p> or <P>.

Open-Ended: <p> anywhere is a document indicates a paragraph break.
Paired Tags: text indicates that the text in between and will be in **bold**

The HTML tags we will use

These tags delimit the document. Seperating it from normal text.

<html></html>	Indicates the beginning and end of an HTML document.
<body> </body>	Indicates the actual body of the document (excludes header and title)

These tags indicate the document's name and purpose. The information encapsulated by these tags is not usually displayed by the web browser. But should you register your page with one of the large north-american reference services like the Yahoo Pages, they will use the information contained in these fields to create your entry.

<head></head>	Indicates the header of the document, usually including the title.
<title></title>	Title of the document.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

These tags are used to do special text formatting. Please note that anything typed other than tags will be concatenated into one long paragraph and reformatted to fit the person's screeen. When you type something like ordinary text, the places where you put carriage-returns will not necessarely be the same as what is going to appear on your client's screen.

	Indicates the beginning and end of a level 1 header.
	Indicates the beginning and end of a level 2 header.
	Indicates the beginning and end of a section of text in **Bold.**
<I> </I>	Indicates the beginning and end of a section of text in *Italics.*
	Indicates the beginning and end of a list of items, combine with
	Put in front of an item of the list so that formatting will occur.
<p>	Place a paragraph break here.
<hr>	Place a horizontal line here.
<a> 	Indicates an anchor point referring to another resource, document

Creating the SAMPLE.HTM document

- Using a text editor, type in these following lines and save the document as **SAMPLE.HTM**.
- Afterwards, copy that file to the **TCPWEB2\WEBPAGES** directory.
- Have a friend on the internet browse to your website using the following URL: **http://yourdomain.com/sample.htm**. Substitute **yourdomain.com** with your BBS real **hostname.domname.**

```
<html>
<head>
<title>Widgets BBS Info Page</title>
</head>
<body>
<h1>Welcome to Widgets BBS!</h1>
<hr>
Widgets BBS has been operating since 1994 running MajorBBS version 6.25 upgrading later to
Worldgroup. We have been offering a very complete list of services including <b>full internet
connectivity</b> since October 95.
<p>
<h2>The list of internet services we offer are:</h2>
<p>
<ul>
<li> Internet E-mail
<li> Usenet Newsgroups
<li> FTP, IRC and Telnet services
<li> MUDs (Multi-User Dungeons)
<li> SLIP/CSLIP/PPP connectivity
<li> And much much more!
</ul>
<hr>
For more information about the services we offer, send us E-mail at <i>sysop@bbs.widgets.com</i>.
</body>
</html>
```

What it should look like on a Web Browser
(a user types http://yourdomain.com/sample.htm on his Web Browser)

Welcome to Widgets BBS!

Widgets BBS has been operating since 1994 running MajorBBS version 6.25 upgrading later to Worldgroup. We have been offering a very complete list of services including **full internet connectivity** since October 95.

The list of internet services we offer are:

- Internet E-mail
- Usenet Newsgroups
- FTP, IRC and Telnet services
- MUDs (Multi-User Dungeons)
- SLIP/CSLIP/PPP connectivity
- And much much more!

For more information about the services we offer, send us E-mail at *sysop@bbs.widgets.com*.

How do I use all the new features of the web server?

A sample set of web-pages was provided with the new server. Assuming you installed the web server using the default directories and prefixes, these pages will function as-is. If you did change the defaults, you will need to modify the pages yourself to make them work. The "Widgets BBS" web pages demonstrate the various aspects of the new Web Server.

Web page	Demonstrates
tcpweb2\webpages\widget\index.htm tcpweb2\imagemap\widget.map (mapfile)	Image Maps, Background Sounds
tcpweb2\webpages\widget\wdgnew.htm tcpweb2\access.ctl (access control file)	Subdirectory Redirection, Password protection of a page and links to other widget pages
tcpweb2\webpages\widget\wdgstats.htm	A hit counter, and sample statistics calculated from the combined log format (Web-Trends sample)
tcpweb2\webpages\widget\wdgstaff.htm tcpweb2\formfile\formtest.txt (form file)	Form-To-File capability
tcpweb2\webpages\widget\wdgreg.htm	Form-To-Email capability

The structure of directories (default) looks like this:

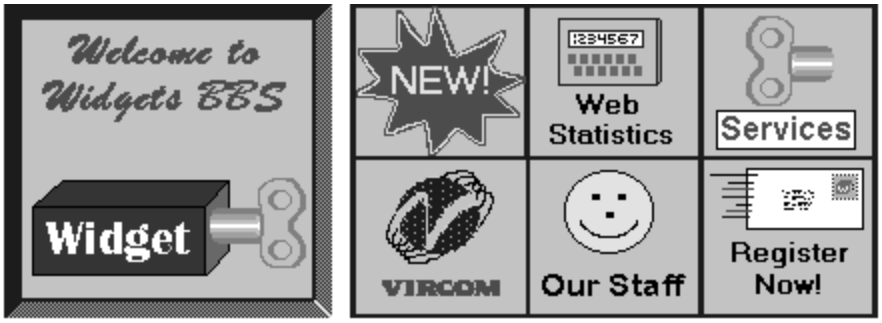
tcpweb2	Master Web Server directory (defined in **WEBPATH*).**
tcpweb2\webpages	Directory where all webpages are stored
tcpweb2\imagemap	Directory where all image maps are stored (defined in **IMGPFIX***)
tcpweb2\formfile	Directory where form files are stored (defined in **FFLROOT*** & **FLPFIX***)

* The parameters are in TCPWEB2.MSG, level 4 configuration options.

Image Maps

Before you start making image maps, you'll need a program that will let you generate a mapfile. The mapfile describes which part of the picture will point to what URL. You can find mapedit at this URL: **http://www.boutell.com/mapedit/**. We're going to use the example of an image map in the widget.htm page. So, to create an image map, follow these steps:

(a) Use a graphics package to create a gif or jpg file that will represent your graphical map.

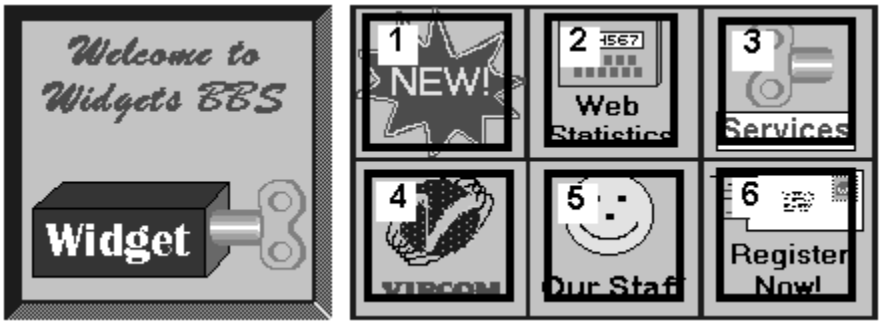


This particular picture is saved as **widget.gif** in the **tcpweb2\webpages\widget** directory.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

(b) Use MapEdit to identify the sections of the image map and generate the mapfile.

1	New!	will point to the /widget/wdgnew.htm page
2	Web Statistics	will point to the /widget/wdgstats.htm page
3	Web Services	will point to the /widget/wdgserv.htm page
4	Vircom	will point to http://www.vircom.com
5	Our Staff	will point to the /widget/wdgstaff.htm page
6	Register Now!	will point to the /widget/wdgreg.htm page



When using MapEdit to Identify the sections of the picture that will be clickable, you can use different shapes. Rectangles, Circles, Polygons, so on and so forth. In the case of this picture, it's best to use rectangles since the clickable items are rectangular. For each item, you can immediately associate a URL. The file MAPEDIT will generate will look like this:

```
rect /widget/wdgnew.htm 176,1 260,76
rect /widget/wdgstats.htm 265,1 347,75
rect /widget/wdgserv.htm 351,2 434,76
rect http://www.vircom.com/ 176,78 263,155
rect /widget/wdgstaff.htm 266,79 346,157
rect /widget/wdgreg.htm 351,79 435,155
```

As you can see, the format is fairly simple. For each graphical object that you isolate, you get an entry that includes: <shape> <URL> <coordinates>. The format of the coordinates will vary depending on the type of shape you use.

Once it's done, the file is saved as **widget.map** (to correspond with the graphic image. Of course, you can call it whatever you want. The file should be copied to the **tcpweb2\imagemap** directory.

(c) Place the image map in your web page.

Finally, you need to link the mapfile with the graphical image on your webpage. In the case of the widget.htm page (and the widget.gif with the widget.map file), the tags will look like this:

```
<A HREF="/IMAGEMAP/widget.map">
    <IMG SRC="widget.gif" ALT="[Widgets Menu]" ISMAP>
</A>
```

That's it. Once the web browser hits this particular tag, it brings up the widget.gif image, and then the person can click on one of the items that were isolated earlier and codified in the widget.map file. If the person clicks say, on the square corresponding to the "Our Staff" box, he or she will be brought to the /wdgstaff.htm page.

Background Sounds

Automatic background sounds are only supported by Microsoft's Internet explorer at the moment, although this could change in a few months. To create a background sound, all you need is to put the following tag:

```
<BGSOUND SRC="NOISE.WAV">
```

NOISE.WAV can be found in the **tcpweb2/widget/webpages** directory. You can put any .wav file there, and there are literally thousands of sounds to chose from on the world-wide-web. Our noise is a simple trumpet call for the Widgets page. If you want to hear the noise but can't because you're not running internet explorer ... you can create a simple reference link:

```
<A HREF="NOISE.WAV">Click Here to play the entrance trumpet</A>
```

It will work only if you have configured a "viewer" on your web browser that will run a .wav player when the file being referenced begins with .wav

Controlling access to a page.

To control access to a page, you need to create a security file (whose name is defined in the level 3 accounting and security section of TCPWEB2.MSG. The parameter is called SECFIL. The file can contain these different lines: (Anything starting by a # is a remark). By default, the file name looked for is **access.ctl**

This line protects the main index.htm page with the normal key. If someone tries to hit the
protected page, he or she will be asked a user ID and password. If the person doesn't have an
account on the BBS or the person has an account but doesn't have the normal key, access will
be blocked.

```
index.htm normal
```

This line protects the same index.htm page by IP address. Any user that tries to get the page
from an IP address outside from the one defined will not be able to access the page. This is
is good if you want to limit access to people on your local net, without restricting via password # the content.

```
index.htm 199.84.216.*
```

The following line protects the pages of an entire subdirectory including any directory under
that subdirectory. The wildcard character is '*', and must be at the **end** of the url. In this
example, any page under the subdir directory and any subdirectory of that directory will be
protected with the normal key.

```
subdir/* normal
```

Lines are scanned in sequential order. The first line that results with the user being given access will stop the scanning. You can have multiple lines that restrict the same page. The above example will give access to the index.htm page to either a user that has the proper key (force login) or comes from the proper IP address. If an IP address is checked and it matches, the user will not be asked to login.

This file can have as many line as you want. Filename is defined in level 3 accounting and security of the TCPWEB2.MSG message file. The parameter is called SECFIL. The SECLTIM parameter controls how often TCPWEB2 checks to see if this file has changed. If it did change, it is reloaded. All scanning is done in memory, so it's relatively fast, although you do not want to do too many key checks.

NOTE about protecting a subdirectory:

Lets say you have the WIDGET directory under the TCPWEB2\WEBPAGES directory. As far as the web server is concerned, the \TCPWEB2\WEBPAGES directory is the ROOT directory. therefore, to protect a subdirectory of the TCPWEB2\WEBPAGES directory, all you need to
add is a line in the ACCESS.CTL file that will protect all the files of that subdirectory. In our example, the TCPWEB2\WEBPAGES\WIDGET directory, the entry you would add in the ACCESS.CTL file would be <subdir>/* <key required>. This is how you would type it:

widget/* NORMAL This will protect all pages under the widget subdirectory. A username and password will be asked for any page there and the person will need the NORMAL key to use them.

Form-to-file capability

This is an example of a form that will output the information to a file. In this case, it's better to go line by line in the **wdgstaff.htm** file (Our Staff survey form).

The complete form in HTML

```
<FORM METHOD=GET ACTION="/FORMFILE/FORMTEST.TXT">

<PRE>
    Name: <INPUT NAME=NameSIZE=50 MAXLENGTH=50>
   Phone: <INPUT NAME=Voice SIZE=15 MAXLENGTH=15>
   E-mail: <INPUT NAME=Email SIZE=50 MAXLENGTH=50>
</PRE>

<P>
Comments: <TEXTAREA NAME=Comment COLS=40 ROWS=5></TEXTAREA>

<P>
<INPUT TYPE=SUBMIT NAME=SUBMIT VALUE="SUBMIT">
<INPUT TYPE=RESET VALUE="CLEAR">

</FORM>

<P>
```

And now, the nitty gritty:

```
<FORM METHOD=GET ACTION="/FORMFILE/FORMTEST.TXT">
```

Here, we define the method as being the GET METHOD (for MAILTO: type of forms, you use the POST method). The ACTION=<URL> is where we locate the formfile. Normally, form files should always be written to the same directory, in this case FORMFILE. The file that stores the data is FORMTEST.TXT. Unless FFLCRE in TCPWEB2.MSG, level 4 config is set to YES, you have to make sure there's at least a zero-byte file by that name. If the file doesn't exist, no data will be saved and an error message will occur. The FORMFILE directory is in the TCPWEB2 directory.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

```
<PRE>
   Name: <INPUT NAME=NameSIZE=50 MAXLENGTH=50>
  Phone: <INPUT NAME=Voice SIZE=15 MAXLENGTH=15>
  E-mail: <INPUT NAME=Email SIZE=50 MAXLENGTH=50>
</PRE>

<P>
Comments: <TEXTAREA NAME=Comment COLS=40 ROWS=5></TEXTAREA>
```

Here we tell the form how to input data. <INPUT> tags are used to define fixed-length fields. In that tag, you can define the NAME of the item, the physical SIZE on the screen, and the MAXIMUM LENGTH (if you type in more data than the size of the field on screen, the content will scroll to the left until you reach MAXLENGTH). The TEXTAREA invokes a multiple line Box of COLS columns wide and ROWS columns long.

```
<P>
<INPUT TYPE=SUBMIT NAME=SUBMIT VALUE="SUBMIT">
<INPUT TYPE=RESET VALUE="CLEAR">

</FORM>
```

The <INPUT TYPE=SUBMIT> Brings up a clickable button that, when clicked, will output the data into the formtest file in the tcpweb2/formfile directory. The <INPUT TYPE=RESET> simply clears the form for data entry.

Form-to-Email capability

Form-to-Email is very simular to Form-to-File. The only difference is that response will be sent to a pre-determined mailbox. Four parameters where added that allows you to send “beautified” mail responses.

FEMPFX: Form-to-Email URL prefix. By default, the value taken is **frmemail**
The prefix means that instead of using the ACTION=“MAILTO:user@domain.com”, you would use instead the ACTION=“/freemail/user@domain.com”. The big difference with this new way to generate an E-mail form response is that the mail received will be formatted by the Web Server using the same output format as the one used in the Form-To-File system, which is far more readable than the output generated by mail-capable web browsers.

The “freemail” in the ACTION statement actually tells the server that this form, once submitted, will need to be processed by the web server.

FBKTO: Fallback to address. By default, the value taken is **sysop**
If the e-mail address specified in ACTION=“/freemail/user@domain.com” doesn’t work, any submitted data will wind up in the mailbox specified in FBKTO. This is simply to have a fallback address if one of your clients puts up a web page and they make an error in the destination address.

FBKFRM: Fallback from address. By default, the value taken is **sysop**
This parameter lets you specify a default address that the From: field in the e-mail will contain. Usually, you’ll use a data entry field like: E-mail address <INPUT NAME="From Address" SIZE=50 MAXLENGTH=50>. This field will wait for the user to type in his E-mail address and will show in the From: field of the recepient of the form response. Should the person’s address be invalid, the default value will be used (in this case, sysop).

FBKTCP: Fallback topic of response. By default, the value taken is Form **Response**
This parameter lets you specify a default topic that the Subject: field in the e-mail will contain. Usually, you'll use a data entry field like: E-mail address <INPUT NAME="Topic" SIZE=50 MAXLENGTH=50>. This field will wait for the user to type in the topic and will show in the Subject: field of the recepient of the form response. The default value is used if none is specified.

Example: (integrated)

```
<FORM METHOD=GET ACTION="/frmemail/majortcpip@vircom.com">

<INPUT TYPE="checkbox" NAME="Terminal Mode" VALUE="Yes">
   I want to use this system in terminal mode.<BR>
<INPUT TYPE="checkbox" NAME="Client/Server Mode" VALUE="Yes">
 I want to use this system in Client/Server mode.<BR>

<PRE>
    Topic: <INPUT NAME="Topic" SIZE=50 MAXLENGTH=50>
    Email: <INPUT NAME="From Address" SIZE=50 MAXLENGTH=50>
    Name: <INPUT NAME=NAME  SIZE=50 MAXLENGTH=50>
   Phone: <INPUT NAME=VOICE SIZE=15 MAXLENGTH=15>
</PRE>

<INPUT TYPE=SUBMIT NAME=SUBMIT VALUE="Send E-Mail">
<INPUT TYPE=RESET VALUE="Clear Form">

</FORM>
```

Example: (explained)

```
<FORM METHOD=GET ACTION="/frmemail/majortcpip@vircom.com">
```

This indicates the beginning of the form, using the GET method. The frmemail URL in the ACTION method indicates that the Form should be processed by the Web Server, sending a form response to majortcpip@vircom.com.

```
<INPUT TYPE="checkbox" NAME="Terminal Mode" VALUE="Yes">
   I want to use this system in terminal mode.<BR>
<INPUT TYPE="checkbox" NAME="Client/Server Mode" VALUE="Yes">
 I want to use this system in Client/Server mode.<BR>
```

Checkboxes.

```
<PRE>
    Topic: <INPUT NAME="Topic" SIZE=50 MAXLENGTH=50>
```

Input topic that will be placed in the subject header of the E-mail. If the data entered is empty, the value sent will assume the default value specified in **FBKTCP**.

```
Email: <INPUT NAME="From Address" SIZE=50 MAXLENGTH=50>
```

Ask user his or her E-mail address to indicate in the form response that the client will read where the mail came from:. If left blank, the default entry specified in **FBKTO** will be used.

```
    Name: <INPUT NAME=NAME  SIZE=50 MAXLENGTH=50>
   Phone: <INPUT NAME=VOICE SIZE=15 MAXLENGTH=15>
</PRE>

<INPUT TYPE=SUBMIT NAME=SUBMIT VALUE="Send E-Mail">
<INPUT TYPE=RESET VALUE="Clear Form">

</FORM>
```

Input the rest of the fields and allow user to click on SUBMIT to send the form response to the address specified at the beginning. RESET will clear anything typed in the fields and allow the person to enter new data.

Form-to-Email capability using the MAILTO:user@domain.com method

Form to E-mail is almost totally identical to the form-to-file. The only thing that changes is the initial <FORM> element.

```
<FORM METHOD=POST ACTION=MAILTO:majortcpip@vircom.com>
```

To turn a Form-To-File into a Form-To-E-mail, you simply substitute the METHOD to a POST method instead of a GET method. In the ACTION, you specify the E-mail address to E-mail to form's contents once submitted. As you can see, the syntax is ACTION=MAILTO:user@domain.com. When the person who fills out the form clicks on the SUBMIT button, the data entered will be automatically E-mailed to the person specified in the MAILTO parameter.

Although this command is supported by most web browsers, not all web browsers have E-mail capability. Furthermore, the resulting E-mail looks like a CGI string and is barely readable. The output is generated by the web browser. It's better to use ther previous option to this one.

Access to account information from the world-wide-web

Users on your system can now find their account status directly from the World-Wide-Web simply by accessing a special URL. This URL is defined in the **STSPFX** option in **TCPWEB2, level 4 configuration**. By default, the value suggested is **acctstat**, but it can be anything you want. Whatever the name the option carries, the data is displayed as per the **STSTXT** text block (in level 6 configuration). You can alter the latter as you wish.

Example: To find out about his account, John Doe does an **http://www.widget.com/acctstat/** (note the trailing slash, it must be there for this URL to work correctly). His web browser on the other hand will ask him his username and password on the BBS. If he enters them correctly, the textblock **STSTXT** is loaded and sent over the WWW as a web page with the fields filled-in with the user's data. You can modify the text block as you wish, but you should keep the text variables there. In this example, this is what John Doe should see on his web browser:

ACCOUNT STATUS

User: JohnDoe

Last-Called On: 96/04/01

Current-Class: SYSOP

Days-Left: Unlimited

Credits-Left: Unlimited

You can limit access to account information over the web by setting up a key (defined in **STSKEY in TCPWEB2.MSG, evel 4 configuration**. If left blank, anyone with an account on the BBS can check out his or her account information through the web. On the other hand, if you want to allow only paying clients to see their information in this fashion, you can set it to the "PAYING" class for instance. On the other hand, if you allow anyone to check out their own info on the BBS via the WWW but want to restrict a few users, you can give their account the value of the **STSNKEY** key.

Moving over to the new web server, some tips

If you were running the old TCPWWW module before, you might want to follow these steps to make the transition from the old WWW server module to the new TCPWEB2 module easier. In an effort to prevent your system from having any web server "downtime", it's possible to run BOTH web server modules while you perform any web page changes off-hours or using a station on a local Lan to make your web pages work with the new web server module.

Lets assume you just installed the TCPWEB2 module using the default settings. Lets use an example to illustrate:

TCPWWW module:	Location of HTML pages: C:\HTML. There's a subdirectory called USERS (**C:\HTML\USERS**) Expected default page: **TOP.HTM**
TCPWEB2 module:	Location of HTML pages (future): C:\WGSERV\TCPWEB2\WEBPAGES Expected default page: **INDEX.HTM**

If you try to run both web servers without changing anything, you will get an error message in the audit trail saying **WEB2 Server Failed: 10048/1**, and neither web server will function. The reason why is because both web servers are listening to port #80, which is the standard web server port used on the world-wide-web.

Change the port number for the new web server module

After installing **TCPWEB2**, go to **level 4 configuration** in the CNF and look for **WEB2PORT**. **Set it to 8000**. This means that the new web server will be **listening to port 8000** instead of port 80, which eliminates the conflict mentioned in the previous paragraph. To access web pages in the C:\WGSERV\TCPWEB2\WEBPAGES directory, you would then do an **http://yourdomain.com:8000/.** To access the old web pages on port 80 running under the old web server module, you can do an http://yourdomain.com/. Note that you don't need to specify the port number in a URL if you're trying to access port 80.

What this means is that people can still get the intact web pages through the old web server while you start copying and modifying pages to the new web server directory.

Copy the pages from the old web server directory and modify your pages to work with the new web server

You can now copy the webpages running under the old web server in the **C:\HTML** directory to the new **C:\WGSERV\TCPWEB2\WEBPAGES** directory. Simply use the xcopy DOS command.

example: xcopy c:\html c:\wgserv\tcpweb2\webpages /e/s

The **/e/s** flags tell xcopy to copy everything in the c:\html including any subdirectory.

Once copied to the new directory, please note that most pages will not need to be altered. All you really need to change is the name of default web page **TOP.HTM to INDEX.HTM** and change any reference or links in the other pages that refer to the **TOP.HTM** to refer to the **INDEX.HTM** instead.

You can use **http://yourdomain.com:8000/** to test the new web server with the webpages in the C:\WGSERV\TCPWEB2\WEBPAGES directory.

Once you are assured that the web pages work with the new web server, deactivate the old web server and set the port back to 8000.

Okay, you've tested and tweaked the pages under the new web server module and they work fine. Use the **WGSMOD (Worldgroup)** or **BBSDMOD (MajorBBS v6.25)** program under the CNF option #7: Basic utilities to **deactivate the TCP/IP WWW Server module** Afterwards, go to **level 4 configuration** in the CNF and look for **WEB2PORT**. **Set it back to 80**.

To access your webpages under the new TCPWEB2 Web Server module, you can now use the original **http://yourdomain.com/** URL.

STEP #10:

Configure the SMTP module

Last revised, January 20th 1997.

- Added options **MAXLRCPT and MAXRRCPT**, controlling the number of local and remote recipients on routed e-mails.
- Added configuration option **AUTHMSG** that records when enabled the userid of the sender in the headers of SMTP messages routed by TCPSMTP if identifiable.
- **ENABROUT** now defaults to **YES**.
- Added Option **TCPGLALS** in TCPLIBM.MSG, level 4 configuration. This option is used to allow use of the GALALIAS alias management that comes with WG2.0 or better, instead of MajorTCP/IPs own alias system. This affects the ***"Determine which Aliasing scheme you will be using"*** section of this chapter.

Module Overview

SMTP Basics.

SMTP is a set of protocols that is used by computers on the internet as a standard mean to interchange private Electronic Mail. SMTP stands for (S)imple (M)ail (T)ransport (P)rotocol.

The way by which mail is sent and received is a little bit like opening a Telnet connection. A connection is made between the sending and receiving machines. Once the handshaking process is over, mail addressed to the receiving site is transmitted. Each piece of mail received is aknowledged, signaling the sender to transmit the next piece of E-mail. If the sender no longer has mail spooled for the site in question, the connection is closed.

In the past, MajorTCP/IP's SMTP needed a "middleman", or in net-jargon, a Sendmail Smarthost. All outgoing mail would be transmitted to the Smarthost site. This site would send the E-mail on it's way in the steed of the original sender. In a sense, a Sendmail Smarthost acts alot like a true post-office. It accumulates and sorts mail, and sends it to the right destination upon reception. All incoming mail addressed to the BBS is stored if for some reason, the BBS becomes temporarely inoperative.

Since that time (as of version 1.77-X of MajorTCP/IP actually), our implementation of SMTP comes with it's own built-in Sendmail Smarthost. This means that people who are getting their service from providers who don't offer Sendmail Smarthost services can rejoice. Sysops who can get a better deal from a provider that offer a very no-frills connection (ie: no Sendmail Smarthost) are also favored by this capability.

***IMPORTANT NOTE* SMTP should be installed and properly configured if you plan on using NNTP and/or POP3 as well as SMTP. These two modules depend on SMTP for some of their functionality.**

Installation procedure for the TCPSMTP module

Step by Step installation procedure for the TCPSMTP module

STEP	Description	Done
#1	Determine the messaging engine to used. MHS or the Worldgroup Engine	
#2	Make sure that your HOSTNAME and DOMNAME are properly set	
#3	Determine which Aliasing scheme you will be using	
#4	Verify with your provider if they've configured their name servers correctly	
#5	Determine E-mail delivery system you'll use: Direct or via Sendmail Smarthost	

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

#6	Set your system to the proper TimeZone	
#7	Configure the TCPSMTP.MSG file for proper E-mail Delivery	

Determine the messaging engine used, the Worldgroup or MHS Engine.

On Worldgroup

The Worldgroup Messaging Engine was created by the folks at Galacticomm to replaces MHS. Designed to be very simple, only a few settings have to be taken care of to make MajorTCP/IP's SMTP talk to the messaging system proper. When you first install MajorTCP/IP on a Worldgroup system, all of the MHS-Specific options are simply de-activated. They are still visible as configuration options, but changing them won't affect the behavior of MajorTCP/IP.
You should ignore the MHS-Specific options and simply go thru the TCPSMTP.MSG file at the end of this series of steps, paying attention only to generic or Worldgroup-specific settings.

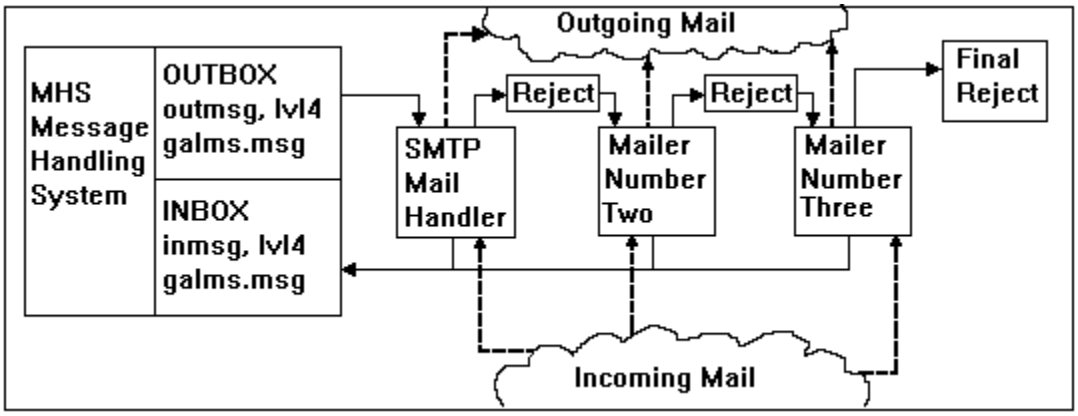
On MajorBBS v6.25

If you are running MajorBBS v6.25, you have no option but to run SMTP with MHS. To do this, you must first understand how the MHS chain operates. MHS is a mail exchange interface created by Novell to build a common messaging architecture. MajorBBS supports this interface. MHS basically uses a set of directory as in and out boxes, passing down mail in a sort of daisy-chain setup from Mail Handler to Mail Handler.

Incoming mail is fairly easy to handle for every Mail Handler. Each of them simply puts the message it received from the outside world directly into the MHS In-Box, which happens to be the directory defined in INMSG (level 4 configuration, GALMS.MSG). All directories should be on the same drive as SMTP's work directory, defined later in the SMTPPATH option.

Things get a little bit more complicated when we're talking about exporting mail FROM MHS to the outside world.

MHS Flowchart



To Illustrate the process, you can see that incoming mail all go to the same location, the **INMSG** directory **defined in level 4 configuration, GALMS.MSG.**

On the other hand, **outgoing mail is processed in series**. The first Mailer (which in our case, should always be SMTP) picks up mail to be delivered in the OUTMSG (level 4 config, GALMS.MSG).

If the Mail is destined for the internet, SMTP simply sends the mail on it's way and that's that.
On the other hand, **if SMTP isn't the mailer this message is addressed to, it puts it into it's reject directory.**

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

The second mailer in the chain looks in SMTP's Reject directory and finds this message waiting there. If it sees that the message is addressed to it, it will send it by whatever means it does it's tranmission. If not, it puts the message in it's reject directory. And so on and so forth.
So, to configure SMTP correctly, all we need to know then is what directories should be assigned to which parameter. First though, we must emphasize this. **SMTP should always be the FIRST mailer in the MHS chain.**

These are the key directories and their settings:

- **SMTPPATH:** This is simply SMTP's working directory and doesn't appear in the MHS chain. It is necessary however for the proper working of SMTP as mail is spooled there for processing and transmission.

- **MHSINPT:** This is where SMTP puts messages it received so that MHS can pick them up and put them in the MajorBBS messaging system. **MHSINPT should thus point at the same location as INMSG, in level 4 configuration, GALMS.MSG.**

- **MHSOUTPT:** This is where SMTP picks up messages that are outbound on the MHS chain. If the message starts with the INT: prefix or is of standard internet E-mail format (username@domain.com), it will process it and transmit it over the internet (storing it temporarely in it's working directory defined in SMTPPATH). If the E-mail is not for it, it is sent into it's Reject directory, to be picked up by the next Mail handler in the chain. **MHSOUTPT should point at the same directory as the one indicated in OUTMSG (level 4 configuration, GALMS.MSG)**

- **REJPATH:** This is the directory where messages that shouldn't be processed by SMTP are stored so that they can be picked up by the next Mail Handler in line. You should point the next mailer in line to the directory specified by this parameter. If you don't have any other Mail Handlers other then SMTP, the Reject directory will in fact become a sort of Reject Pile where all E-mails that weren't processed for some reason by SMTP will wind up. **Once specified, the directory will automatically be created.**

Make sure that your HOSTNAME and DOMNAME are properly set.

Before getting SMTP online, you have to make sure that your **HOSTNAME and DOMNAME settings in TCPLIBM.MSG (level 1 hardware configuration, page 32 of this manual)** are properly set.

In the case of a system that calls itself "bbs.widgets.com"
HOSTNAME should be **bbs**, **DOMNAME** should be **widgets.com**

In the case of a system that calls itself "lotsawidgets.com"
HOSTNAME should be **lotsawdigets**, **DOMNAME** should be **com**.

There's a parameter in **TCPSMTP.MSG, level 4 configuration called SMTPFROM** which lets you override the Hostname and Domnames. Unless you want to create an "alias" of your system's name. Normally, you should leave this parameter blank. If on the other hand, you want to have a mailing address that's different from your primary address, but you want the mail to be received by the BBS nonethless, you can do the following things (**we'll use bbs.widgets.com for our example**):

Most of your users have complained that the **bbs.widgets.com mailing address** (which also corresponds to your system's internet name) is too long to type when sending E-mail. So you decide you'd like a smaller name for E-mail only. You settle on **widgets.com.**

- Ask your provider to create an alias of **bbs.widgets.com** called **widgets.com**. Such aliasing means that widgets.com points at the same IP address as bbs.widgets.com.

- Afterwards, you should tell your provider to **forward all E-mail to widgets.com instead of the bbs.widgets.com address**. This means they have to change their Mail-Exchange records. (not necessary if you are using MajorTCP/IP's built-in Sendmail Smarthost).

- The next step is to make sure that outgoing mail will have the username@widgets.com instead of username@bbs.widgets.com in the From: field. That way, replies will be sent to username@widgets.com. To accomplish this, you can't change HOSTNAME and DOMNAME. **You can, however, override them for SMTP E-mail only by changing SMTPFROM in level 4 configuration, TCPSMTP.MSG to widgets.com.**

- You're done. Now, any incoming and outgoing mail will go to the widgets.com name instead of bbs.widgets.com. In fact, we've only create a disguise for bbs.widgets.com. People can still telnet bbs.widgets.com or do any other non-SMTP activity.

Determine which Aliasing scheme you will be using.

Because SMTP E-mail needs internet compatible usernames, there are three ways by which MajorBBS/Worlgroup usernames can be converted to internet E-mail compatible usernames:

- **No aliases:** Simply put, MajorTCP/IP simply converts usernames to an internet E-mail compatible format. This means changing spaces to periods, and truncating the names down to 16 characters. **No aliases means that USEALIAS in TCPSMTP.MSG, level 4 configuration (described in the TCPSMTP.MSG configuration section) has to be set to NO. This is the favored method of operation.**

- **Rlogin Alias file:** Rlogin comes with a built-in alias handling system. You can create a pair of Rlogin module pages. One with the command string of "ALIAS" which lets your users create internet/SMTP e-mail compatible usernames. The other with the "SYSOP" command string would let you edit the TCPUIDS.DAT file which contains all the user aliases. **Check out page 73 of the manual for further details. Note: if the user hasn't selected an alias, the system will use the No aliases method until selection is made.**

***NOTE* The Rlogin Alias file is no longer the favored method. Standard User ID's are now automatically "mangled" to fit the internet standards used for user names. Setting up an Rlogin Alias file is generally considered redundant now.**

- **MG/I Alias file:** Same as the Rlogin Alias file, except that it requires a pair of special settings. This only applies if you were running MG/I before installing MajorTCP/IP and wish to continue to use it's alias file. **Check out pages 72 to 75 to create the Rlogin pages and the special settings required for MG/I compatibility. Note: if the user hasn't selected an alias, the system will use the No aliases method until selection is made.**

- **GALALIAS alias file:** You can now use the GALALIAS modules and files for aliasing in MajorTCP/IP. To do so, set **TCPGLALS to YES** in **TCPLIBM.MSG, level 4 configuration** to tell the MajorTCP/IP modules to use the Galacticomm GALALIAS module for aliases. You can use this option only if you're running WG2.0 or above. All of MajorTCP/IP's alias

features are disabled and replaced by the ones in GALALIAS. RLogin USEMGI and MGIWRT and SMTP's USEALIAS settings will now be ignored. You should not use the RLogin "alias" sysop menu anymore described in the Rlogin section of the manual.

Notes about MG/I

If you were using MG/I for mail, you probably know that you need to prefix E-mail going out with IN: or INTERNET: in the address field. MajorTCP/IP will accept E-mail going out that have the IN: or INT: prefixes or that don't have any prefixes. SMTP looks at the outgoing address and by doing some pattern matching will decide if it is a valid internet address. If you are running WORLDGROUP we suggest that you set the prefix to INT (not IN), as there seems to be some problems with two-characters long prefixes in the WorldGroup Client E-mail module.

Verify with your provider if they've configured their name servers correctly.

You need to find out if your provider properly defined your system's hostname/domain name in his name server tables (DNS). If you are not in his tables, your hostname/domain name won't be locatable thru DNS resolution. Hence, E-mail won't be able to travel from you to the outside world and vice-versa.

Determine what E-mail delivery system you'll use: Direct or via Sendmail Smarthost

As of version 1.76-8, MajorTCP/IP now comes with a built-in Smarthost. This means you no longer need to use an external system as your sendmail smarthost. SMTP is fully capable of delivering mail by itself. There are still advantages of having an external Smarthost: a) It can keep mail for your BBS if for some reason, your system goes down temporarely. b) It removes a burden off of your system. Most providers offer Smarthost services for free. You might as well take advantage of that. But if you have to pay for your Smarthost or your provider doesn't offer Smarthost services, you're better off using the built-in Smarthost. **Check out parameter SMTPMXU in TCPSTMP.MSG, level 4 configuration.**

Set your system to the proper TimeZone.

When you're sending E-mail to computers all over the world, it start to be quite important that everyone agrees on a common way of indicating time and dates. In order to do that, SMTP must be told in which time zone your BBS is, and will convert this information so that it can be attached to E-mails that you send.

Indicating the timezone is done through the use of the TZ environment variable (this is a standard for DOS, so it might already be set on your computer). **The format of TZ is: TZ = zzz[+/-]d[d][lll].**
Where zzz is a three-character string representing the name of the current time zone your BBS is located into. All three characters are required: Example: PST, EST, CST, ...

[+/-]d[d] is a required field containing an optionally signed number with 1 or more digits. This number is the local time zone's difference from GMT in hours. Positive numbers adjust westward from GMT. Negative numbers adjust eastward from GMT. For example, EST would be 5 (or +5), PST would be 8 (or +8) and continental Europe would be -1.

lll is an optional three-character field that represents the local time zone daylight saving time. For example, the string PDT could be used to represent Pacific Daylight Saving Time. If this field is present, the computer will assume that this daylight saving time period is active.
To set this variable, you'd add something like this to your autoexec.bat file: SET TZ=EST5

Notes about MIME Encoding/Decoding

MajorTCP/IP now supports full MIME encoding and decoding of file attachments. To activate this feature, you must set **SMTPMIME to YES in TCPSMTP.MSG, level 4 configuration options**. Should you leave SMTPMIME off, incoming MIME-encoded file attachments will still be automatically decoded, however outgoing messages will be UUencoded instead.

Configure the TCPSMTP.MSG file for proper E-mail Delivery.

Level 3 - Security and Accounting configuration

- From the main configuration menu (CNF), select **F3 - Accounting and Security**
- Press on **F8 - Search**, type **TCPSMTP.MSG**
- The first item you should find is the **RMLKEY** parameter.
- Edit each item as described below, moving from item to item using the arrow keys.
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu.

RMLKEY **Key required to receive internet mail.**
NORMAL Users will need this key for SMTP to allow incoming SMTP E-mail for them. If they don't have this key, they won't be able to receive new internet mail via SMTP.

SMLKEY **Key required to send internet mail.**
NORMAL Users will need this key for SMTP to process their outgoing internet mail. If they don't have the proper key, SMTP will just move the message to the reject directory.

SAMLKEY **Key required to send attachments.**
NORMAL Users will require this key if they want to be able to send file attachments using SMTP E-mail. If they don't have this key, the file attachment won't be sent and a notice of that will be sent to the person receiving the message.

SMTPCHG **SMTP per-message surcharge.**
0 You may want to charge users extra for sending SMTP messages. The charge you enter here will be added to regular E-mail message charges when users write SMTP messages. You can also give users credits for using SMTP by specifying a negative amount. Leaving SMTPCHG at 0 means that SMTP messages are at the standard E-mail rates.

SMTPATCH **SMTP attachment surcharge.**
0 You may want to charge users extra for attaching files to SMTP messages. The charge you enter here will be added to regular E-mail attachment charges when users write SMTP messages.

SMTPPKCH **SMTP attachment per-kbyte surcharge.**
0 You may want to charge users attaching files to SMTP messages on a per-kilobyte basis. This way, users will be charged more for attaching larger files. The charge you enter here will be added to regular E-mail attachment charges when users write SMTP messages.

Level 4 - System options configuration

- From the main configuration menu (CNF), select **F4 - Configuration options**
- Press on **F8 - Search**, type **TCPSMTP.MSG**
- The first item you should find is the **SMTPENAB** parameter.
- Edit each item as described below, moving from item to item using the arrow keys.
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu.

SMTPENAB **Enable SMTP Server.**
YES This option activates MajorTCP/IP's SMTP Server. If SMTPENAB is set to to no, many of the following options associated with SMTP will remain invisible.

SMTPENA2 **Display message to SMTP request.** (Visible only if SMTPENAB is set to NO)
NO This is a switch that enables a warning message to other SMTP Mail handlers on the internet telling them that SMTP is unavailable at the moment on this system. If an SMTP mail handler attempts a connection and this option is set to YES, it will receive the warning message. If not, the connection will simply be refused.

SMTPMAX **Maximum concurrent SMTP Server users**.
3 SMTPMAX sets the maximum number of incoming SMTP connections MajorTCP/IP will accept for your BBS. Setting it to 0 will limit the number to 20. Each incoming connection uses up one TCP Handle. **(Check out NBTCP on page 32 of this Manual). This option is not visible if SMTPENAB is set to NO.**

SMTPMAXO **Maximum SMTP Outgoing sessions**
1 SMTPMAXO specifies how many concurent SMTP sessions can be in progress at the same time. The higher the number, the more SMTP will have an impact on the overall system performance. Note, also, that SMTP will need up to two file handles for each outgoing sessions, plus 1 TCP handle. Setting SMTPMAXO to ZERO will disable the outgoing server. **(beck out NBTCP on page 32 of this Manual). This option is not visible if SMTPENAB is set to NO.**

SMTPMXU **Send E-mail directly**,
YES This option tells MajorTCP/IP to enable the built-in SMTP Mail Exchanger. This feature is available as of 1.77 of MajorTCP/IP. This option alleviates the need for an external SMTP Smarthost. If you set SMTPMXU to NO, you MUST have a smarthost entered in the next option, SMTPSMRT for outgoing E-mail to work. When set to YES, SMTPMXU will make our SMTP server try to send E-mail to the proper host directly, and on the last attempt will send the E-mail to your smarthost instead, if one is defined. If you don't have a smarthost, then SMTPMXU MUST be set to YES. If your BBS is within a firewall, then SMTPMXU MUST be set to NO, and a smarthost must be defined. **This option is not visible if SMTPENAB is set to NO.**

SMTPSMRT **IP [NUMERIC] address of smarthost**.
0.0.0.0 The SMTP Server needs the IP address of a MAIL/SMTP smart host that will be used to route outgoing E-mail for us. Usualy, a host running sendmail or smail, at your IP provider's site will be sufficient. **This option is not visible if SMTPENAB is set to NO.**

SMTPMSS **Maximum Segment size of SMTP Server Connections**.
256 You can set the maximum length of packets sent and received by your SMTP Server. The smaller the paquet size, the less impact SMTP transfers will have on your other telnet/rlogin/... services. However, SMTP Server throughput will be reduced. Leave to 0, to use the default, system-wide MSS. MajorTCP/IP will automatically adjust this value so that it doesn't exceed the system-wide MSS. **This option is not visible if SMTPENAB is set to NO. Check out the system-wide MSS on page 31 of this manual.**

SMTPHEAD **Level of SMTP headers to record**.
0 SMTP routing headers can add quite a lot of data to internet E-mail that is received. You may want to have SMTP strip part of these headers, if you set SMTPHEAD to 0, SMTP will not record any header information. The higher the level you'll put there, the more information will be recorded. (Maximum 9).
This option is not visible if SMTPENAB is set to NO.

SMTPFROM **SMTP mail from.**
<empty> SMTP allows you to override the HOSTNAME and DOMNAME fields that are in TCPLIBM.MSG, level 1 hardware configuration, that are used in the FROM: field of any SMTP E-mail being sent out. The string you enter here will be added to the userID of the sender to form the full address. DO NOT ENTER the "@" sign. Example: bbs.widgets.com Clear to disable. **This option is not visible if SMTPENAB is set to NO.**

SMTPLOG **Record SMTP connections in log.**
YES Set this option to YES to record incoming SMTP connections into the MajorTCP/IP log. The MajorTCP/IP log is defined in TCPLIBM.MSG. **This option is not visible if SMTPENAB is set to NO.**

SMTPPATH **Work directory for SMTP.**
.\SMTP.DIR SMTP will be using a directory for workfiles. Enter here the path and directory name you want SMTP to use for that directory. Do not put a trailing '\'. It is preferable to specify a full path explicitely however.

Note: These options are valid for WORLDGROUP ONLY

SMTPPFX **Address prefix for SMTP exporter**.
INT In order to identify an address as being sent to a particular exporter, each exporter is identified by a unique prefix. This prefix may be two or three characters long and consist of letters or numbers only.

Enter here the prefix you wish the SMTP exporter to be identified by. NOTE: There seems to be a bug in the WG client module that prevents prefixes of two characters long to be working. We then suggest that leave the default INT in here. **WORLDGROUP Only**.

SMTPNAM **Name of SMTP exporter**.
Internet[SMTP] Each exporter is identified in lists and help messages by a name and/or description. Enter here the name you wish to use to identify the SMTP exporter. **WORLDGROUP Only**.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

SMTPDSC **SMTP exporter desc.**
SMTP Internet E-mail handler Each exporter is identified in lists and help messages by a name and description. Enter here the description you wish to use to identify the SMTP exporter. **WORLDGROUP Only.**

SMTPXMP **Example SMTP address.**
INT:TStryker @Engr.com In some help messages, users may be shown an example address for an exporter. This example should include the prefix specified in SMTPPFX and show a typical address with proper format for SMTP. **WORLDGROUP Only**.

SMTPHLP **SMTP help message.**
Below Users may request detailed help on specific exporters. This message will usually explain how to address a message to someone using SMTP, who your users can expect to each, and possibly what charges apply to use of SMTP, but you are free to provide whatever message you think would be most helpful. **WORLDGROUP Only**.

SMTP is the Internet standard protocol for real-time delivery of electronic mail. To send someone a message using SMTP, you need their address. Once you have their address, you tell the server that this is an Internet address by entering "%s:" followed by their address.

Note: These options are valid for MAJORBBS using MHS only.

MHSINPT **MHS-IN directory.**
.\MI This is the directory used by MHS to scan for new incoming messages. SMTP will write incoming messages in there. It should be the same as Level4 configuration option INMSG (in GALMS.MSG). **NOT NEEDED for WORLDGROUP**

MHSOUTPT **MHS-OUT directory.**
.\ML\REJECT This is the directory where SMTP will scan for outgoing messages. If you are using MailLink, you should usually set this to .\ML\REJECT. If you are not using any mail software, then it should be set to the same value as Level 4 configuration option OUTMSG (in GALMS.MSG), the MHS output directory. **MUST BE ON THE SAME DRIVE AS SMTPPATH. NOT NEEDED for WORLDGROUP**

REJPATH **Reject Directory**.
.\SMTP.DIR \REJECT When a message is found in MHSOUTPT that isn't for SMTP, we can move it in a new reject directory. REJPATH specifies where you want that message to be moved. Leave blank if you don't want the message to be moved. **REJPATH MUST BE ON THE SAME DRIVE AS SMTPPATH AND MHSOUTPT**.

These options apply generally to both MajorBBS and Worldgroup.

INTMOUT **Single step timeout for Incoming (minutes).**
1 This is the timeout for incoming SMTP server connections. This timeout will be triggered after n minutes without activity on the link.

OUTTMOUT **Single step timeout for Outgoing (minutes).**
1 This is the timeout for Outgoing SMTP server connections. This timeout will be triggered after n minutes without activity on the link.

OUTCYC **Number of seconds between out cycles.**
30 Every OUTCYC seconds, the SMTP server will do its outgoing cycling processing. A lower number means that mail will be going out quicker, but that the overall system response time might be reduced.

SMTPMXOC **Number of messages to log per OUTCYC.**
1 This is the number of messages SMTP will LOG per OUTCYC. A larger number will make each OUTCYC last longer, but will make E-mail go out faster. This has an impact only on 6.25 MajorBBS Systems (using MHS).

SMLOW1 **Minimum disk space available for SMTP (MB).**
5 When the amount of free diskspace reaches the defined number for SMLOW1, no new SMTP requests will be allowed to start. (this number is in MEGABYTES). Set to 0 to disable. This number should be a multiple of SMLOW2.

SMLOW2 **Minimum disk space available for SMTP (MB).**
1 When the amount of free diskspace reaches the defined number for SMLOW2, all current SMTP sessions will be terminated abruptly. Set to 0 to disable. This number is in MEGABYTES. This number should be smaller than SMLOW1.

DBUGLVL **Debugging Level (for LOG file).**
7 This selects the level of debugging information that will be recorded in the log file. 0 Disables the log, 9 turns on full debugging. Full debugging might slow down the BBS, somewhat.

POSTMAST **Destination of postmaster E-mail.**
Sysop POSTMASTER is an account that _must_ be able to receive mail, as per internet standard. You can, optionally, specify here to wich account should POSTMASTER E-mail be automatically forwarded.

ROOTMAIL **Destination for root E-mail.**
Sysop You can also specify an account to which you'd like E-mail for root to be automatically forwarded. Leave blank to disable.

USEALIAS **Do you want to use an alias file.**
NO If you leave this to NO, MajorTCP/IP will use the user ID of the user as it's internet address, converting all spaces to DOTs. ('.'). If you set to yes, MajorTCP/IP will use the RLogin alias file.

ATTENAB **File attachments allowed for outgoing E-mail?**
YES If you enable this option, SMTP will allow file attachements to be sent over the internet. These file attachements will be automatically UUENCODED and splitted in a number of messages not exceeding CHUNKSIZ (next option). You can disable the processing of file attachment completly here.

SMTPMIME **Enable MIME encoding/decoding of attachments?**
YES You can tell SMTP to automatically encode outgoing file attachments using the MIME encoding scheme, and to automatically decode MIME attachments into normal file attachments. To do so, set SMTPMIME to YES. **CHUNKSIZ is disabled when SMTPMIME is enabled. If SMTPMIME is set to NO, incoming MIME attachments will still be decoded automatically. However, outgoing file attachments will be UUENCODED instead of MIME encoded. This option is visible only if ATTENAB is set to YES.**

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

CHUNKSIZ **Maximum size of message chunk (in K).**
50 This allow you to specify the maximum message size of that SMTP will create, when splitting a file attachment in multiple parts. Not that this is in addition to any text the user may have put in the message body itself. 50 is a good number, you can disable the splitting of file attachment message by setting this to 0, but some SMTP servers may not like that. **Not used if SMTPMIME is set to YES. Not Visible if ATTENAB is set to NO.**

SMTPGPR **GME Import Priority.**
2 This controls the GME message importing priority. Default is 2. A Higher number will slow down importing. **WORLDGROUP Only**.

SMTPOFST **Kick start OutCyc with GME.**
NO Normally, SMTP waits until an "outcyc" comes by before actually processing E-mail that has been sent for the Internet with Worldgroup. You can set this option to YES to kick start an "outcyc" when a new message for the Internet is written. **WORLDGROUP Only**.

MAXTRY **Number of retries sending E-mail out**.
10 This is the number of attempts we'll make at sending an E-mail before flagging the message as undeliverable.

TRYWAIT **Base amount of time between retries (minutes).**
10 This is the number of minutes between each attempt at sending an E-mail to the target SMTP site.

MAXISIZE **Maximum size (in Kilobytes) of incoming E-mail.**
0 This is the maximum size an incoming SMTP E-mail message can have. Any messages bigger than that will be rejected. This size is in K-bytes. 0 disables the limit checking. This option was created to fix the problem of mail-bombs, where an irate person on the internet would send huge E-mail attachments (in the multiple-megabytes range) just to bog down the system.

SMTPDSG **Default signature for mail delivered by SMTP.**
<Empty> This parameter allows sysops to set a system-wide default signature for E-mail. These signature lines will be added automatically at the end of all messages sent via SMTP. **Leave empty to disable**. **This option is visible only if SMTPENAB is set to YES.**

ENABROUT **Enable SMTP Routing**
YES If you enable SMTP routing, SMTP will accept E-mail from other systems that are not intended for the BBS and will attempt to route them out. If you set this to YES, **then you MUST enter the various aliases for your bbs domain name in SMAL01 to SMAL20**. **You must set this to yes if your SLIP users will use your BBS as a SMTP/POP3 server**. **This option is visible only if SMTPENAB is set to YES.**

SMALnn **System alias number nn (where nn can be from 01 to 20**)
<Empty> Enter here the hostname/domainname alias SMTP will accept email for and consider it for the BBS. SMTP already accepts email for the HOSTNAME/DOMNAME as defined in tcplibm.msg, level 1 and for the SMTPFROM defined above. Please, make sure you make no typos, as if you make one, SMTP will attempt to send email back out to the internet. **This option is visible only if ENABROUT is set to YES.**

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

MAXLRCPT **Max. Number of Local Recipients (ROUTING).**
100 This limit the number of **LOCAL** recipients that someone using your SMTP server for routing purposes can send to in one operation. Setting this number too high may make your system more vulnerable to mail bombing.

MAXRRCPT **Max. Number of Remote Recipients (ROUTING).**
10 This limit the number of **REMOTE** recipients that someone using your SMTP server for routing purposes can send to in one operation. Setting this number too high may make your system more vulnerable to mail bombing.

AUTHMSG **Put authentication information in routed messages.**
YES When **AUTHMSG is set to YES**, the SMTP server will automatically put accurate identification of the user account that generated the message, if the user can be identified. Users can be identified when they connect through the SLIP/CSLIP/PPP server or through the RADIUS server. The identity will be put in a custom header field called "X-TCP-IDENTITY: <username>".

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

STEP #11:

Configure the SLIP/CSLIP/PPP server

Last updated January 20th, 1997.

- Added **PPPSNSGC** option that lets you disable auto-sensing on incoming telnet/rlogin channels.
- Added security option **SLI2NRKY** which defines a key that will limit traffic to the local LAN (class C for instance, according to your netmask) as opposed to SLIPNRKY which limits traffic solely to the BBS.
- Changed **SLIPDURT** option in level 4 configuration. Now will affect credit based accounts and time-based accounts as well.
- Added **CRDMON** option in level 3 accounting and security for the TCPSLIP.MSG file. This is used to monitor the "Credit Rate" field of the user in ghost mode. If a third party accounting package modifies the field, we will ajust our credit rate accordingly.
- People who purchased ICO/AIO and are moving to MajorTCP/IP can use the **/SLIP or /PPP** suffix instead of the slip: or ppp: prefixes used by MajorTCP/IP owners. That way, they don't need to change and distribute any login scripts used by their clients.
- Added **PPPFORC** option to force people into PPP mode upon connection.

Module Overview

What is it used for?

MajorTCP/IP's SLIP/CSLIP/PPP server allows you to provide IP connectivity over serial/modem lines. SLIP stands for Serial Line Internet Protocol. It's a simple protocol that allows the exchange of IP packets over slow communication links like serial and modem lines. CSLIP is simply a different flavor of SLIP that includes compression. Finally, PPP stands for Point-To-Point Protocol which is an entirely different beast from SLIP and CSLIP. **In fact, the industry trend right now is to move away from SLIP and CSLIP and to go to PPP.**

When connected to the Internet using SLIP, CSLIP or PPP, computers really become "nodes" on the Internet and have complete access to all connectivity services of the Internet. As any other computer on the Internet, computers connected using the SLIP/CSLIP/PPP server must be assigned IP addresses.

The SLIP/CSLIP/PPP server is used mostly to let users go onto the World-Wide-Web. This is by no means the only thing your users can do thru their connection however. Your clients need a TCP/IP stack (like Trumpet Winsock) and a graphical web browser (like Mosaic or Netscape) to get on the World-Wide-Web. They can also use a plethora of other client programs for Trumpet Winsock that can take advantage of your SLIP link, all of these being Windows-Based.

Check out this URL: http://cwsapps.texas.net

This is Consumate Winsock Applications page. This is a comprehensive list of all the popular Winsock applications that exist on the internet. Each entry includes a full review, hardware requirements, pricing (if commercial) and so on and so forth. Winsock clients that perform the same function are scored against one another (A five star products is way better than a product with two and a half stars) and include links to the FTP sites where these can be downloaded from directly at the click of a mouse.

What's CSLIP? (Van Jacobson Header Compression)

TCP/IP (the protocol used for WWW, Telnet, FTP) has a normal overhead of 40 bytes per packet, 20 bytes for the IP header and 20 bytes for the TCP header. This can take a lot of time

to transmit over a modem line, especially if you're just sending one character of valid data (say the user pressed a key). That means that just for one keystroke, the computer would be sending 41 bytes to the BBS. Then the BBS would echo that back to the user, another 41 bytes.

This huge overhead doesn't really matter on high speed links, but on modems it does. To help reduce the overhead, we have added CSLIP support to MajorTCP/IP's SLIP/CSLIP/PPP server. This protocol compresses the TCP/IP headers down to 5-6 bytes, instead of 40, for an important performance gain.

CSLIP support is fully automatic (if you really want, you can disable it by setting the **CSLIPENA parameter to NO**, in **Option 4, Configuration options**). You don't need to specify who's using CSLIP and who isn't. A user that wants to use CSLIP instead of SLIP has to enable it in his TCP/IP stack. This may be called CSLIP, Compressed SLIP or Van Jacobson Header Compression.

What's PPP?

PPP or Point-to-Point protocol is the new kid on the block in terms of protocol suites. PPP is the new standard mode of connection used these days to provide TCP/IP connectivity via modem. Contrary to SLIP and CSLIP, PPP offers a time-saving feature called PPP Authentication Protocol. This means that, if connecting to a system that offers PAP connections in PPP, you no longer need to supply cumbersome scripts to your users for them to establish the connection properly. The TCP/IP stack they use (Trumpet Winsock or Win95's built-in stack) only need to be told to use PAP, and to enter their user Ids and password to connect to your system. These will be automatically detected and this, without any sort of automated script. **To enable PPP, you simply need to set PPPENAB to YES in TCPSLIP.MSG, level 4 Configuration Options. Furthermore, you can restrict PPP access by using the PPPKEY parameter in TCPSLIPM.MSG, level 3 Accounting and security**. Here are the details of our implementation of PPP:

PPP provides performance optimization. Like CSLIP, PPP supports Van Jacobson Header Compression. In addition, PPP supports address and protocol compression, which makes it marginally faster than CSLIP. In reality, the performance gain is nothing to write home about. The big plus of PPP is the simpler connection requirements.

PPP smart-sensing: Our PPP server automatically recognizes, in the auto-sensing phase, that the caller is using a PPP stack. The channel is immediately switched to PPP mode without being prompted by some sort of script (although scripts can still be used, if you really insist). This eliminates complex and customized login scripts, greatly simplifying the end user's setup. **Translation**: No more login scripts which means less technical support phone calls from your users. Furthermore, Mac users who seem to be unable to find a good stack that does SLIP or CSLIP can now rejoice because PPP is the only thing most Macs will do these days. **The elements of Smart-Sensing include the PPP authentication protocol, IP address negotiation and Primary DNS Address negotiation. You can turn on Smart-Sensing by setting PPPSNS to YES in TCPSLIP.MSG, level 4 configuration.**

PPP authentication protocol (PAP): Most PPP stacks your clients might be using support PAP. Used with the PPP smart-sensing, this makes the end-user setup an amazingly simple task, reducing significantly your technical support requirements. The PPP server logs the user in ghosting mode. This allows your client to "telnet" back to your BBS, either in Client/Server mode or terminal mode, while concurrently using any other TCP/IP clients, such as a Web Browser or a graphical IRC client.

IP Address Negotiation: With this option, the caller doesn't need to know anything about IP addresses, and where to enter them. No matter what gets entered in the IP address field of the caller's stack, it will be overridden by this automatic negotiation. This option works without any kind of scripting on.

Primary DNS Address Negotiation: Microsoft published a new standard in December `95 to support the automatic negotiation of the primary name server IP address. Much like the above IP address negotiation, this automatic negotiation takes the user one step farther from the technical aspect of connecting to the Internet. Since the standard is so recent, few stacks are supporting this feature. It has been tested with Windows 95's dialup networking and Windows NT. On the other hand, Trumpet Winsock doesn't have this feature, so it'll be necessary for your users who use Trumpet Winsock as their TCP/IP stacks to put in the DNS address in the corresponding field. This is address is the same as the one you have in PRIDNS, level 1 Hardware configuration in TCPLIBM.MSG.

The SLIP/CSLIP/PPP server and IP Addresses

Addresses that you will be allocating to your users must be routed to your Local Area Network by your provider and your router. (If you are using SLIP, CSLIP or PPP yourself to connect your BBS to the Internet, we don't recommend that you resell SLIP/CSLIP/PPP access. It will just be too slow. In any case, if you still want to do it, you'll have to tell your provider to route additional IP addresses to your BBS).

Usually, BBSes that have a direct connection to the Internet are allocated Class C network addresses, allowing them to have up to 254 IP addresses on their site. For instance: let's say one IP address is allocated to your Router and one for your BBS, you'd have 252 addresses remaining that you can allocate to your users.

This pool of IP addresses can be divided in two finite group of addresses. **STATIC IP addresses** are allocated permanently to a specific user. **Dynamic IP addresses** are allocated on the fly, when a SLIP server call is established, and released when the person logs-off.

You can see that STATIC IP addresses should be allocated with very much care, as they are a precious commodity. As the Internet grows, and grows, a shortage of IP addresses is starting to occur. We recommend not allocating STATIC IP addresses to anyone, unless there is a very specific need for that. You should probably charge more for these type of users.

Static IP addresses

As mentioned above, STATIC IP ADDRESSES are allocated permanently to a user. You do that by using the TCPSLIP Sysop menu (a Module page link pointing to TCPSLIP, accessible to Sysops ONLY) by picking option #2 of that menu to associate a STATIC IP address to a user.

This address must be in the pool of STATIC IP ADDRESSES that you'll define in the TCPSLIP.MSG message file configuration. No two users can have the same STATIC IP ADDRESS allocated to them.

Dynamic IP addresses

These addresses (also part of a pool of addresses you allocate in the TCPSLIP.MSG message file) are allocated on the fly every time a user starts a SLIP connection. They are re-used when the user finishes his session. There is no way to predict if a user will get the same IP address twice.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Since your caller will most likely be using a Windows-based TCP/IP Stack (like Trumpet Winsock), DYNAMIC IP ADDRESSES might look like a pain to use, since you have to enter the IP address that you are using every time your start your SLIP/CSLIP/PPP software on your Winsock setup. But, fortunately, stacks like Trumpet Winsock have mechanisms to automate that completely. **In your main BBS directory, you'll find a file called LOGIN.CMD**, which is a sample Trumpet Winsock login script that allows your users to automate completely your user's SLIP connections. You may have to customise this file for your BBS, the login prompts might be slightly different on your BBS. You can learn about the script language used in the Trumpet Winsock documentation.
With the advent of PPP, this is made even more painless because you can do away with scripts alltogether. This is a godsend to SYSOPs who'se days are often filled with technical support calls asking how to setup SLIP/CSLIP scripts.

IP ADDRESSES AND NAME SERVERS

The IP addresses that you reserve for SLIP, CSLIP and PPP (static and dynamic) should be in your name server if you want your users to be able to use all FTP Servers using an FTP client. Some FTP servers will verify that an IP address is associated with a host name by doing an "inverse pointer lookup". If you didn't have your Name Server Provider (the person who is managing the name server for your domain) set-up inverse pointers in the name server database, then your users doing FTP will be denied access by the FTP Servers.

Let's assume you have a range of dynamic IP address,from 199.84.216.200 to 199.84.216.205, the entries in your provider's Name Server should look something like this:

slip200.domain	**199.84.216.200**
199.84.216.200	**slip200.domain**
slip201.domain	**199.84.216.201**
199.84.216.201	**slip201.domain**
slip202.domain	**199.84.216.202**
199.84.216.202	**slip202.domain**

and so on and so forth ...

Where "domain" is your domain name. This is not the actual format that the records will have in the Name Server database, but this is the kind of associations your provider will need to make.

Routing Issues

The key point of routing packets with MajorTCP/IP's SLIP/CSLIP/PPP server is to make sure that your router (and your provider's router) send IP packets addressed to the IP addresses in your STATIC and DYNAMIC ranges to your local area network. Once that is done, the SLIP/CSLIP/PPP server takes over thanks to the Proxy-ARP technology we have built into it. When a router or another TCP/IP host on your LAN queries the LAN for the Ethernet Address of an IP address that is allocated to a user, the BBS will respond and will inform the host making the query to send all packets for that IP address to the BBS directly. That way, you don't need to maintain any complex routing table.

SLIP/CSLIP "Forgiving" Mode

Users often don't read instructions, and they are bound to get into the SLIP module with the improper IP address set for the end of the connection. This is especially true if you are converting from some sort of "proxy" SLIP alternative like TIA and SLIRP, where all users are using the same IP address. To help make it a bit easier on the users (and on you, the Sysop), we've enhanced the SLIP module with the "Forgiving" mode. This mode will automatically correct the IP address of packets that are sent and received by the users in a way to make them acceptable even if they don't have the right IP address. This will work for most application (including WWW page browsing in Netscape) with the notable exception of FTP transfers. **Forgive mode isn't really usefull for people who use a login script or PPP users as these automatically grab the IP address that was allocated for their use.**

To make it even easier on you and the users, we optionally display a message in the audit trail when we're doing the IP address translation and can optionally E-mail the user about the problem in the hope that he will correct for his next call. Both the topic and the body of the E-mail that is sent to the user are configurable. Check out Option 4 - Configuration options from the main configuration menu that are related to this new feature which are not listed below: SLIPFORG, SLIPFORN, SLIPFORE, SLIPFOTO, SLIPFOBO. Please see the **"Configuring the TCPSLIP.MSG file"** for more information.

LOGGING-IN AS A SLIP/CSLIP USER

Your users can use three methods to connect:

Direct manual login

This is simple. Instead of logging in user your normal User-ID, the user types "slip:User-ID" at the login prompt. Example, if your User-ID is JohnDoe, you would enter slip:JohnDoe. Afterwards, you type in your password normally. If you have the proper access level to use SLIP (you own the SLIPKEY), you'll see the message that says that SLIP has started and which IP address was allocated to you. All you need to do from this point is to go into your TCP/IP stack configuration **(for Trumpet Winsock, click on FILE, then SETUP)** and type in the IP adress given in the IP adress field.

Login from the Menu

Your users can go into SLIP/CSLIP mode directly from the menu. A user who has the SLIPMKEY key can now enter SLIP mode by just picking a menu item that points to the SLIP server. Since he doesn't have the SLIPSKEY, he won't be presented the sysop menu, instead, he will drop directly into SLIP. Note that all SLIP-specific accounting is disabled in this mode,
Instead, SLIP via menu is fully compatible with the Galacticom accounting system and will work with third party accounting software. **For this to work, you must call the SLIP module from the menu tree using a module page (explained later).** As in the direct manual login, the user will see that an IP adressed was assigned to him. All he needs to do is to enter this IP address in his TCP/IP stack. **(for Trumpet Winsock, click on FILE, then SETUP, and type in the IP adress given in the IP adress field).**

Automated login for Trumpet Winsock

This automated login is performed via a login script we wrote called LOGIN.CMD (in your BBS directory when you install MajorTCP/IP) that you copy into your client's trumpet winsock directory. The login script may require some customization if you are not using standard prompts while a user connects to your BBS. Some pointers are given later in this section on how to accomplish this. If you need assistance, we are happy to do the customization for you if you can't manage it yourself. Basically, the login script enters the username and password for the user automatically, captures the IP address and uses it, all of this automatically, without any intervention from your client's part. **Check out "Configuring Trumpet Winsock" in this section**.

We could support other TCP/IP stacks, but there are so many of them, we decided to emphasize the one that is used by the largest number of people, namely Trumpet Winsock. For other TCP/IP stacks, call us on our tech support line or consult the various forums that talk about MajorTCP/IP.

LOGGING-IN AS A PPP USER

PPP users have it much easier. Because of the Smart-Sensing, they don't need to do any of the irksome steps illustrated in "Loggin-in as a SLIP/CSLIP user". Assuming you've turned on Smart-Sensing and people are using your average TCP/IP stack, all they need to do is this:

- **Enable PAP.** This is the case for Trumpet Winsock. Win95 and Mac's have it by default.
- **Enter** their **user-ID and password** in their TCP/IP stack's configuration.
- **Enter the DNS address** in the stack's configuration. **(not necessary with Win95).**
- Tell the TCP/IP stack they use to **connect to your system.**

As you can see, there's no reason why you shouldn't move over to PPP. You can still use PPP in the same manner as SLIP or CSLIP, but you really don't have any reasons to do so.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Something about account ghosting

This feature permits you to be able to telnet back into the BBS from your Windows computer once you have the SLIP/CSLIP/PPP link activated. MajorTCP/IP turns your SLIP account into a “ghost” looking like: (SLIP: IP Address). In essence, account ghosting lets your users login twice into the system. Once in SLIP, CSLIP or PPP, a second time by Telnetting back into your machine either thru Worldgroup Manager in Telnet mode, or by using a Telnet Client.

Ghosting features. Several new parameters were added to make this dual logon capability safer. In the past, user ghosting could, in some instances lead to people from the outside logging in under a ghosted user’s connection while the other user was online. The system operator can now restrict who is able to Telnet back into the system, and restrict such Telnets to coming only from the address assigned by the pass-through server, preventing multiple people from using the same account concurrently. Credit consumption rates for the second telnet can also be customized for your system’s needs.

In level 3 accounting and security, you have two new parameters:

SLIPDUKY: a key used to allow/dissalow people from logging-in back into the system from a SLIP/CSLIP/PPP connection via telnet.

SLIPDURT: lets you set a surcharge ratio for people who telnet back into the system, from 0% to 100%, both on credit-based accounts and time-based accounts.

In level 4 configuration options, you have one new parameter:

SPDUCKIP: This items restricts dual connections to come from an incoming Telnet/RLogin channel and that this Telnet/RLogin originates from the IP address allocated by the SLIP/CSLIP/PPP server to the user.

Users in SLIP/CSLIP/PPP mode and accounting

Since your SLIP account is now a ghost, accounting for SLIP/CSLIP/PPP isn’t handled by the BBS but by the SLIP/CSLIP/PPP server. **Thus the per minute credit charge that you define in level 3 configuration of TCPSLIP.MSG defines the actual charge that will be applied to your account**. If you telnet back into the BBS, you take an additional telnet channel for this connection and accounting for this connection is handled directly by the BBS, as if you were a normal caller.

The user can be also charged **per kilocharacter exchanged**, and **credit-exempt classes can be also charged**. **Charges are applied every 5 minutes**.

Classes per-call and daily time limits are enforced by the SLIP/CSLIP/PPP server. **If the user is connected twice (once over the SLIP server, another time over a Telnet line), you can use the SLIPDURT to set a ratio that determines how much the person will pay extra for that dual logon. Don’t forget that someone doing this uses two licenses from your six-packs, so you might want to recoup your investment by charging for this mode.**

[Vircom Inc’s MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Simultaneous Netscape and Worldgroup usage

Yes, this is possible. Thanks to the user ghosting feature of our SLIP/CSLIP/PPP server, and the fact that the WorldGroup Client software has Telnet built-in, you can use Netscape (or any other TCP/IP application) at the same time you are using any application of the WorldGroup Client software. You tell the WorldGroup client program to telnet to your BBS instead of using a phone line. This is done in the "preferences" option of the WorldGroup Client Software on the user's Windows system. **Note that a person logged-in this way is telnetting back into BBS, thus he is using time twice as fast, occupying two Hardware channels that count on your user six packs.**

- User connects using **Trumpet Winsock** with the **LOGIN.CMD** script file.
- Once connection is established, user can run **Worldgroup in telnet mode**.
- User can **run winsock clients like Netscape** simultaneously.

X.25 Options with the SLIP/CSLIP/PPP Server

New options were added to the SLIP/CSLIP/PPP server to handle X.25 links with remote PAD echo. These options are very experimental. They will not affect anyone else.

SLIP/CSLIP/PPP sessions and their effects on TCP Handles

SLIP/CSLIP/PPP sessions do **not** use up any TCP Handles. A SLIP/CSLIP/PPP session will use up a TCP Handle only if the user Telnets back into the BBS, or uses local services like the Web Server via the SLIP/CSLIP/PPP connection. You should consult each service's NBTCP effect for details. For more details about TCP Handles, check out NBTCP (**page 32 of this manual**). Each SLIP/CSLIP session uses up one Galacticomm license off of your six-packs per user. (In fact, it's the modem connection, not the SLIP/CSLIP connection per say).

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Installation procedure for the TCPSLIP module

MajorTCP/IP's SLIP server is relatively complex. It's important to follow these instructions exactly. We also explain how to create a **SLIP Menu option**, how to **configure Trumpet Winsock** and how to modify the **login.cmd** script for automated Winsock login.

Step by Step installation procedure for the TCPSLIP module

STEP	Description	Done
#1	Configure the TCPSLIP.MSG file for SLIP/CSLIP/PPP connections	
#2	Put the TCPSLIP module in the menu tree for SYSOP or direct SLIP/CSLIP/PPP access	

Configure the TCPSLIP.MSG file for SLIP/CSLIP PPP connections.

Level 3 - Security and Accounting configuration

- From the main configuration menu (CNF), select **F3 - Accounting and Security**
- Press on **F8 - Search**, type **TCPSLIP.MSG**
- The first item you should find is the **SLIPKEY** parameter.
- Edit each item as described below, moving from item to item using the arrow keys.
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu.

SLIPKEY **Key required to use SLIP, CSLIP and PPP.**
<empty> This key is required for users to be able to enter SLIP/CSLIP and PPP mode. This key is checked every 5 minutes while the SLIP/CSLIP/PPP connection is active for this user. If the user looses this key, the connection will be killed. All users except those with the MASTER key need this key to be able to use the SLIP/CSLIP/PPP server in any mode.

SLIPMKEY **Key Required to enter SLIP, CSLIP and PPP from the menu tree.**
SLIPMENU This key is required for users to be able to enter SLIP mode from the menu tree. You need to setup the TCPSLIP module in the menu tree where they will be able to select the SLIP module. Note that all SLIP-special accounting is disabled in this mode. Instead, the normal BBS accounting takes place. **Users can't telnet back into their accounts if they enter SLIP from a menu**.

SLIPNKEY **Key to prevent SLIP, CSLIP and PPP usage.**
NOSLIP This key will prevent a user from using SLIP/CSLIP or PPP **even if he owns the above SLIPKEY**. This key is checked every 5 minutes while the connection is active for a user. If he gains this key while logged-on and doesn't have the **SLIPSKEY**, his connection will be killed.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

SLIPSKEY **Key required for module sysop menu access.**
SYSOP This key is required in order to be able to use the SYSOP functions of the module, to edit profiles, amongst other things. Someone who access the TCPSLIP module from the menu tree without this key **and owns the SLIPMKEY will simply drop into SLIP/CSLIP or PPP**. If he owns neither keys, the module will prevent the user from accessing the module alltogether.

SLIPNRKY **Key that will stop routing.**
NOROUTE If a user owns this key (**and does not have the master key**), the module will only accept packets that are to be exchanged to the BBS, thus blocking all access to resources outside of your net. **Useful for Demo users**. Note that **option SLIPDNSR defines if DNS packets are controlled by this key too.**

SLIPDNSR **Allow restricted routing of DNS packets.**
YES If a user has the SLIPNRKY (above), then no TCP packets will be routed to the external world. If you set SLIPDNSR to NO, then no DNS packets will be routed either. However, your user won't have access to name servers. Setting SLIPDNSR to YES will let the user use any DNS Name Server. This key is verified every five minutes.

SLI2NRKY **Key that will stop routing (LAN).**
NOROUTE2 If a user owns this key (and does not have the master key), then the SLIP/CSLIP/PPP server will only route packets if the destination is on the local lan. That means that packets that are intended for anything outside of your lan will not be routed.

SLIPRATE **Credits per minute charge for SLIP, CSLIP and PPP users.**
60 You can specify a charge per minute for all non credit exempt users. This charge is NOT a surcharge and thus replaces any charges that you have built-in as standard charges for your BBS. **Note that this is not used if the user enters the module from a menu.**

SLIPKCHG **Charge for each KiloCharacter sent or received.**
0 You may want to charge user for each KiloCharacters being exchanged through the SLIP/CSLIP/PPP server. This allows you to do that. This includes incoming and outgoing traffic. **Note that this is not used if the user enters the module from a menu**.

SLIPEXCK **Key that override credit charge exemptions.**
EXCHARGE Users that have this key (**and not the MASTER key**) will be charged for SLIP/CSLIP/PPP access. You use this key if you have users that are charged a flat rate for local services, but you want to charge them an hourly rate for Internet Services, or even just SLIP/CSLIP/PPP services.

SLIPNZKY **Key that prevents SLIP/CSLIP/PPP idle zap.**
SLIPNOZAP Owners of this key will never be zapped for inactivity while connected to the SLIP/CSLIP/PPP server. Good for Sysops or Bulletin Boards that your provide a connection for.

SLIPNOCH **Key that will exempt user from credit charges.**
EXEMPT If this key is not blank, and a user owns it, he will be exempted from all credit charges due to their SLIP, CSLIP or PPP connection. Leaving this key blank will disable this feature.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

SLIPFORC **Key that forces SLIP/CSLIP/PPP mode.**
GOSLIP If this key is not blank, and a user owns that key, he will be forced into SLIP/CSLIP or PPP mode even if he logs in without prefixing his user-id with slip: or ppp:. The user must still have any other keys required for slip access like the **SLIPKEY**.

PPPFORC **Key that forces PPP mode**
PPPFORC If this key is not blank, and a user owns that key, he will be forced into PPP mode even if he logs in without prefixing his user-id with ppp:. The user must still have any other keys required for PPP access.

SLIPDUKY **Key required for dual login.**
<empty> This key is required to be able to telnet back into the BBS, when connected over SLIP/CSLIP/PPP. Leaving SLIPDUKY to blank, lets everyone do it. NO PSEUDO KEYS FOR SLIPDUKY.

SLIPDURT **Ratio of connect charges for dual login.**
100 This percentage will be applied against the connect time charges defined above (SLIPRATE) when the user is logged back in. This is because the user will be charged the normal BBS charges on the Telnet session, so you may not want to fully surcharge SLIP/CSLIP/PPP usage. If you set SLIPDURT to 50 (for example), then the SLIPRATE will be halved while the user is telneted in. If you set it to 0, then no connect time charges will apply to the SLIP/CSLIP/PPP session, only while the user is telneted in.

MajorTCP/IP will now do time-based charging as well in the case of the SLIPDURT option. What this means is that a person logged in say, with a two hours a day limit will see his or her time used diminish proportionately to the SLIPDURT value if logged in twice. Example: if SLIPDURT is set to 50, the person's time online will be consumed at one and a half times the normal rate (instead of twice the normal rate before the SLIPDURT option came about)

PPPKEY **Key required for PPP.**
<empty> This key is required for PPP, in addition to all the other keys you may require above. Including the SLIPKEY. Once the PPP session has started, this key is no longer checked. This key is used by some Sysops to charge a "setup fee" for people who already have SLIP/CSLIP access. Once the user has paid the fee, the user is given the PPP key so they can use PPP.

CRDMON **Enable CRDRAT monitoring *Experimental***
NO If you set this to **YES**, then the SLIP/CSLIP/PPP server will be monitoring the "Credit Rate" field for ghost accounts. If some external accounting package modifies this field, we'll apply the credit rate difference to the current user. This option only works with for ghosted accounts (not for connections that start from a menu) and only if the current user is being already charged for credits. This is experimental. We suggest you leave this option disabled until testing is complete.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Level 4 - System options configuration

- From the main configuration menu (CNF), select **F4 - Configuration options**
- Press on **F8 - Search**, type **TCPSLIP.MSG**
- The first item you should find is the **SLIPENAB** parameter.
- Edit each item as described below, moving from item to item using the arrow keys.
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu.

SLIPENAB **Enable the SLIP server on the BBS.**
YES This tells TCPSLIP.MSG to function on this BBS. Note that SLIPENAB must be set to YES if you want to use the SLIP/CSLIP/PPP dialer. If this option is set to no, most of the following parameters will not be visible.

SLIPNET **Network used by SLIP/CSLIP/PPP users. Not visible if SLIPENAB set to**
0.0.0.0 **NO.** This is the network address that will be used by your users. Usually, the last digit of network addresses is zero. Example: If your BBS is 199.84.216.2 and your netmask is 255.255.255.0, then your SLIPNET value would be 199.84.216.0. **For the SLIP server to function properly, the BBS IP address (MYIPADDR in level 1 hardware config, TCPLIBM.MSG) and the IP addresses assigned for SLIP/CSLIP/PPP must all be in the same class C**. In other words, the first three digits of the IP adress must be the same. If a BBS is on 199.84.216.2 but the IP addresses allocated to you range from 199.84.254.20 to .30, this will not work. All must begin by 199.84.216.X in this example.

SLIPDLOW **Lowest and Highest adress in the dynamic range.**
SLIPDHIGH The **SLIPDLOW** and **SLIPDHIGH** fields let you define which address range will both to 0 be used by the module to allocate DYNAMIC IP addresses. Possible values are from 1 to 254, and can only include IP addresses that can be routed by your network. These values will be used as the last digit (added to) of your network address. Enter the lowest address in the dynamic range at the **SLIPDLOW** parameter. Enter the highest adress in the dynamic range at the **SLIPDHIGH** parameter. Set both to 0 to disable. **Make sure that this range of IP addresses does not overlap with any existing hardware. Nor must they overlap with the SLIPSLOW and SLIPSHIGH parameters.** Dynamic IP addresses are allocated when the users needs them. Once they disconnect, these are de-allocated and made usable by the next caller in line. **Not visible if SLIPENAB is set to NO.**

SLIPSLOW **Lowest and Highest adress in the static range.**
SLIPSHIGH The **SLIPSLOW** and **SLIPSHIGH** fields let you define which address range will both to 0 be used by SLIP to allocate STATIC IP addresses. Possible values are from 1 to 254, and can only include IP addresses that can be routed by your network. These values will be used as the last digit (added to) of your network address. Enter the lowest address in the static range at the **SLIPSLOW** parameter.
Enter the highest adress in the static range at the **SLIPSHIGH** parameter.
Set both to 0 to disable. **Make sure that this range of IP addresses does not overlap with any existing hardware. Nor must they overlap with the SLIPDLOW and SLIPDHIGH parameters.** Static IP addresses must be reserved in advance by individual users. The Sysop allocates these through the TCPSLIP menu page. **Not visible if SLIPENAB is set to NO.**

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

SLIPPRIO **SLIP/CSLIP/PPP priority setting.**
10 Normally, the SLIP/CSLIP/PPP server will process one user packet per cycle. If you find this too slow, you can increase SLIPPRIO. If you set it to 0, it will process all awaiting packets every time. With the exception of 0, a higher priority value means more priority is put on SLIP/CSLIP/PPP users. **Not visible if SLIPENAB is set to NO.**

SLIPIZAP **SLIP/CSLIP/PPP Inactivity delay before hangup.**
10 If a user is inactive (no packets received from the user's side) for SLIPIZAP minutes, the SLIP/CSLIP/PPP server will automatically hangup the user's connection. Set to 0 to disable. **Note that if the user has the key SLIPNZKY, he won't be zapped because of inactivity. MASTER key owners are never zapped. Not visible if SLIPENAB is set to NO.**

SLIPFORG **Forgive wrong IP addresses.**
YES Users sometime forget to read the documentation, and thus will end up connected in SLIP or CSLIP mode without telling their TCP/IP stack what dynamic IP address they are using. MajorTCP/IP's module can be set to operate in "forgive" mode where it will automatically substitute the right IP address on incoming packets and do the reverse on outgoing packets. It should work for most things, with the notable exception of FTP clients because most FTP sites do a reverse DNS lookup, which will fail with this IP substitution. **SLIPFORG is basically useless for PPP users as these obtain the right IP address automatically if they are using PAP. Not visible if SLIPENAB is set to NO.**

SLIPFORN **Show who was forgiven in the audit trail.**
YES When we notice that someone is using the wrong IP address, do you want the SLIP/CSLIP/PPP server to output a message saying so (once per session) in the audit trail? **Not visible if SLIPFORG is set to NO.**

SLIPFORE **Send E-mail to user if we're forgiving him.**
YES In addition to the notice in the audit trail, the module can automatically send an E-mail to the user, telling him that we were nice despite the fact that he didn't use the right IP address and telling him about potential problems. **If SLIPFORE is set to YES, then we'll send that E-mail**. The actual text and topic of the E-mail are below in options **SLIPFOTO** and **SLIPFOBO**. **Not visible if SLIPFORG is set to NO.**

SLIPFOTO **Topic of the E-mail sent to the forgiven SLIP user.**
* See text * This is the topic of the E-mail sent to the user about forgiving him for the misuse of an IP address. **Not visible if SLIPFORG is set to NO. The default value of SLIPFOTO is " * SLIP NOTICE * ".**

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

SLIPFOBO **Body of the the E-mail sent to the forgiven SLIP user.**
* See text * This is the body of the E-mail sent to the user about forgiving him for the misuse of an IP address. **Not visible if SLIPFORG is set to NO.**

```
Dear %s,

This is to let you know that at the time this E-mail was sent to you,
you were using the SLIP server with an incorrect IP address of %s instead
of the %s IP address that was issued to you when the SLIP server started.

The SLIP server did try to prevent this problem from disrupting your SLIP
connectivity but note that while it's doing that, you can still run into
Internet roadblocks. A prime example of that is that no FTP transfers
will work while you don't have the proper IP address entered.

You can make sure that you are using the right IP address in different ways,
probably the easiest is just to look at the display you get after logging
in and note down the IP address and enter it in your TCP/IP (or winsock)
program. If you are using Trumpet Winsock (and possibly others), your
Sysop probably has a LOGIN.CMD login script that will do that automatically.

We certainly hope that you will be able to resolve this problem, but in
the mean time...Keep'on SLIP-ing!

<This was an automated notice>
```

CSLIPENA **Enable CSLIP Van Jacobson Header compression.**
YES CSLIP (common name for Van Jacobson Header Compression) over SLIP is a protocol that has less overhead and thus can yield much higher performance, especially on small packets (like keystrokes of an interactive session).
MajorTCP/IP will automatically detect if a user is using CSLIP instead of SLIP and will switch CSLIP on on that session. But if you set CSLIPENA to NO, MajorTCP/IP will never enable CSLIP for anyone. The only reason that I can see that one would have to turn this off is if some bugs are detected in CSLIP and one would want to prevent crashing the BBS. **Not visible if SLIPENAB is set to NO.**

PPPENAB **Enable PPP?**
YES PPP or Point-to-Point Protocol allows for much easier connections to the Internet This option allows you to enable the PPP protocol. **This option is visible only if SLIPENAB is set to YES.**

PPPSNS **Enable PPP Smart-Sensing?**
YES PPP Smart-Sensing allows your users to connect to your BBS using PPP without requiring a script. If enabled, the auto-sensing sequence will check for PPP users and switch the line to PPP mode and use PAP (PPP authorization protocol) to validate the UserID and Password. **This option is visible only if PPPENAB is set to YES.**

PPPSNSGC **Enable PPP Smart-Sensing on telnet/rlogin Channels?**
YES Some sites may want to disable PPP auto-sensing for calls coming in on TELNET, RLOGIN or TELALT channels. Setting **PPPSNSGC** to **NO** will let you do just that.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

PPPSNSDL **Smart-Sensing Delay in seconds.**
8 This is the amount of time (seconds) PPP will wait at the Auto-Sensing prompt for a PPP packet. The delay can range between 3 and 20 seconds. This means that a user who is NOT connecting in PPP will see the connection prompt for that time before logging on the system, which can be annoying if the delay is set too long. You may want to experiment with shorter delays gradually to see which one works best while minimalizing the wait for other users who aren't trying to connect in PPP. **This option is visible only if PPPSNS is set to YES.**

PPPSNSST **Auto sensing prompt.**
* See box * This is the message that will be displayed at the start of the PPP auto-sensing. The %d will be replaced by the number of seconds the delay will last. **This option is visible only if PPPSNS is set to YES**

Auto-sensing PPP...(%d seconds)

PPPSNSAB **Seconds before allowing PPP sensing abort.**
3 You may want to allow the PPP auto-sensing to be aborted, but you don't want the users to start aborting it while the ANSI auto-sensor is still active. PPP will wait for PPPSNSAB seconds before displaying the abort message. If set to 0, the abort mode will be disabled. You can enter a value ranging from 0 to 15 seconds. **This option is visible only if PPPSNS is set to YES**

PPPSNSAS **Abort Message.**
* See box * This is the auto-sensing abort message. It will be displayed after PPPSNSAB seconds. **This option is visible only if PPPSNS is set to YES**

Hit CTRL-X to abort

SLIPTRL **Show SLIP/CSLIP/PPP Logins/Logouts in the Audit Trail.**
YES This option allows you to have SLIP, CSLIP and PPP logins and logouts recorded in the audit trail. **Not visible if SLIPENAB is set to NO.**

SPDUCKIP **Restrict dual logins to user's IP address.**
NO By default, dual logons (telneting to the BBS and logging on the same account that is used for SLIP) are allowed only on GCDI channels (usually used for telnet only, but also with equinox drivers). However, if you set SPDUCKIP to YES, then the call will have to be coming from not only a telnet/rlogin channel, but also will be accepted only if coming from the IP address that has been assigned to the user. **This option is not visible if SLIPENAB is set to NO.**

SPCX25 **Enable special X.25 handling.**
NO Some X.25 systems require special programming before and after a SLIP/CSLIP/PPP call is handled. This enables such programming. Do not change unless you have an X.25 connection into your BBS, and really, really know what you're doing. **This option is not visible if SLIPENAB is set to NO.**

SPCX25ST **SLIP/CSLIP/PPP x.3 prefix**
2:0 This X.3 string will be sent to the PAD just before a SLIP/CSLIP/PPP connection is started. **This option is not visible if SPCX25 is set to NO.**

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

SPCX25EN **SLIP/CSLIP/PPP x.3 suffix**
2:1 This X.3 string will be sent to the PAD just after a SLIP/CSLIP/PPP connection is ended. **This option is not visible if SPCX25 is set to NO.**

Put the TCPSLIP module in the menu tree for SYSOP or direct SLIP access.

This page will be usable by both the SLIP users and the SYSOPs. If you want to create a copy of the page at a different location to keep these separate, the setup is exactly the same. If someone (like a Normal user) owns ONLY the SLIPMKEY, the person will not get the SLIP SYSOP Menu. Only people with SYSOP or MASTER access get the SYSOP menu.

- From the main configuration menu (CNF), select **F2 - Design Menu Tree**
- Make sure that the menu item cursor is located on **your Internet Services page**
- Select **F2 Edit** to change the Internet Services menu
- Go to the menu options area and **add a new option**, say **[S] Enter the SLIP module**.
- In the **EDIT OPTION** window ...
    - Short Description .....could be “Enter the SLIP module”
    - Key required for this option..... the **SLIPMKEY**
    - Destination page..... could be called **SLIP**
    - **Save the menu**. A new page in the menu tree should’ve been created.
- Move the cursor to the new page called **SLIP**
- Press **F2 Edit** to configure this module page.
    - Allow go to this page ..... should be set to **YES**
    - Key required ..... should be the **SLIPMKEY**
    - Select module window, you should chose the **TCPSLIP** Module
    - Display header ..... should be set to **YES**
    - The command string should be left empty.
    - Save the resulting page.
- Done.

What a normal user with the SLIPMKEY should see:

The only thing a normal SLIP user should see if starting SLIP from the menu is the line **“Starting SLIP server mode: Your address is: xxx.xxx.xxx.xxx”.** From here, the user needs to get out of his or her terminal program and start up Trumpet Winsock. The user should go into the Winsock setup and type in the IP address he was allocated in the IP address field. Here’s a step-by-step breakdown of the process.

- User with SLIPMKEY select the SLIP module from a menu option.
- Slip module returns**: “Starting SLIP server mode: Your address is: xxx.xxx.xxx.xxx”.**
- User exits terminal program / worldgroup manager **without** hanging up.
- User starts their TCP/IP stack (in most cases, this means **Trumpet Winsock**).
- User clicks on **FILE** from the Trumpet window.
- User clicks on **SETUP**
- User changes the **IP address field to match the number given by the BBS.**
- User clicks on **Ok, minimize Trumpet Winsock and start his/her winsock clients**.

[Vircom Inc’s MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

What a SYSOP/MASTER user should see

People with the SYSOP and/or MASTER keys get a special menu when selecting the SLIP server from a menu option. This is what it looks like:

```
MajorTCP/IP SLIP Server Maintenance page.
=================================
        1 - Display Stats of current SLIP users
        2 - Edit/Review/Delete user's SLIP records
        3 - Enter SLIP mode (menu-slip-mode)
        4 - Enable PPP debugging
        5 - Display detailed PPP information of a channel
        X - Exit back to menu.
```

Option #1 brings you to a menu tree function where you can find out stats for each user in SLIP. You receive the number of packets sent, the largest packet sent, outgoing junked packets, packets received, largest packet received and incomming junked packets.

Option #2 lets you assign STATIC IP addresses to a specific user ID. The option brings you to a question asking you which user ID to edit. Then, you get to assign the IP address to this user. Once assigned, you can select QUIT or SAVE. Once done, you go back to the SLIP maintenance page.

Option #3 is the same as if the SYSOP/MASTER user was getting into the module with the SLIPMKEY only. You get the "Starting SLIP server mode ..." string. The SYSOP/MASTER user can then startup his TCP/IP stack .

Option #4 enables PPP debugging. All PPP connections (either from users connecting in PPP or the BBS connecting to the provider using PPP) will be logged in the TCPPPP.LOG file in the BBS directory (WGSERV or BBSV6).

Option #5 lets you see the details of a channel being used for a PPP connection.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Configure Trumpet Winsock and Windows 95 for PPP use.

PPP and Trumpet Winsock

Making Trumpet winsock work with a PPP connection is a snap. This particular setup assumes that you will enable the PPP auto-sensing. Your users just need to follow these steps:

Step #1 - Configure Trumpet Winsock SETUP options

- Startup Trumpet winsock.
- Click on the **FILE** menu, afterwards click on the **SETUP** option.
- The User should put in the **IP address of your Primary Domain Name Server** in the DNS Field of the SETUP screen. This is the same address you use in the **PRIDNS** parameter in **TCPLIBM.MSG under level 1 - Hardware Configuration.**
- Internal PPP should be selected.
- Port is the COM port the client will use.
- Hardware Handshaking should be used.
- Van Jacobson SLIP compression should be enabled.
- DCD/RLSD check should be enabled.
- User should then click on OK.

Step #2 - Configure Trumpet Winsock PPP options

- Click on the **FILE** menu, afterwards click on the **PPP options** selection.
- The user should click on the “use Password Authentication Protocol (PAP)” box.
- Next, the user types in his BBS user ID in the Username field.
- Afterwards, the user types in his BBS password in the Password field.
- Finally, the user should click on OK.

Okay -- we’re done. The user will never need to configure Winsock again, except if he or she changes password or account on your system. To connect to your system, they can easily do it manually.

Dialing with Trumpet Winsock

- Click on **Dialer**, select the **Manual Login option**.
- Type atdt<phone number> and hit enter. (Phone number is your BBS phone number)
- As soon as the user sees the word “CONNECT”, he hits escape.
- A few seconds later, winsock should see a message telling it that the connection was accepted and that the user’s IP address is some number. (One of your IP addresses from your pool)
- User minimizes winsock and starts using whatever winsock client he wants.

You can automate this little login process by writing essentially a **5 line login script** and have it downloaded by your client. All the **login.cmd** file needs are these lines:

```
output "atz"\13
input 10 OK
output "atdt 123-4567"\13
input 60 CONNECT
wait 30 dcd
```

Of course, substitute 123-4567 with your own phone number, but that’s about the gist of it. As soon as connection is established, the auto-sensing will kick in and establish the connection.

PPP and Windows 95

If you thought making Trumpet with PPP was easy, here's how it looks like with Windows 95.
We assume here that the user is using PPP dialup over the modem, and doesn't have a network card in his machine.

The only step, configuring windows95

- Double-click on **"My Computer"**
- Double-click on **"Control Panel"**
- Double-click on **"Add/Remove Programs"**
- Click on **"Windows Setup"** tag
- Click on **"Communications"**
- Click on **"Details"** button
- Click on **"Dial-up Networking"** (should have a checkmark)
- Click on **"Ok"** button
- Click on **"Ok"** button
- **Insert requested disk in proper drive**
- Close **Control Panel**
- Double-Click on **"Dial-up Networking"**
- Double-Click on **"Make new Connection"**
- Enter **name of BBS**
- Click on **"Next"** button
- **Enter phone number**
- Click on **"Next"** button
- Click on **"Finish"** button

This creates a BBS Icon configured to dial your particular system.

Calling your BBS in PPP mode

- Double-Click on the new BBS icon
- Enter BBS user-id
- Enter BBS password
- Click on "Connect" button

You're on-line in PPP mode! You can now start Netscape. You can also test by opening a DOS Prompt window and typing "ftp ftp.microsoft.com". You login anonymously and can now download files directly from Microsoft's FTP site.

Setup win95 to automatically start the dialer as soon as you launch an internet application

Left click on your Internet icon on your desktop and click on Properties. Then click on AutoDial if you are not already on that tab then click on "Use Auto-Dial". Then choose the Dial-Up Connection you want to use and you are all set.

Each time you invoke a program that requires an Internet Connection, it will start the Dial-Up Networking automatically.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Configure Trumpet Winsock for SLIP and CSLIP (and distribute the ini file)

To configure Trumpet Winsock correctly, follow these steps:

- Startup Trumpet winsock.
- Click on the **FILE** menu, afterwards click on the **SETUP** option.
- The IP address should be **0.0.0.0**
- The Netmask should be the same as the NETMASK parameter in the TCPLIBM.MSG file, level 1 - Hardware Configuration. Most of the time, it's **255.255.255.0**
- The **Gateway address should be left empty** unless the person connects via a LAN or other local connection. In the latter case, you can put in the IP address of your router.
- The DNS address should be the **IP address of your Primary Domain Name Server**. This is specified in the **PRIDNS** parameter in **TCPLIBM.MSG under level 1 - Hardware Configuration.**
- The Domain Suffix is simply your BBS internet name. For instance, bbs.widgets.com.
- VECTOR ... should be set to 0
- MTU ..... should be set to 1500
- RWIN ..... should be set to 4096
- MSS ..... should be set to 1460
- RTOMAX....should be set to 60
- Internal SLIP should be selected.
- Port is the COM port the client will use.
- Hardware Handshaking should be used.
- Van Jacobson SLIP compression should be enabled, except if CSLIPENA is set to NO in TCPSLIP.MSG. Level 4 - Configuration Option.
- DCD/RLSD check should be enabled.

This SETUP generates a file called TRUMPWSK.INI. You could distribute this file or make it available for download to make the life of your clients easier (not to mention yours). All they need to do then is to put in the right IP address when connecting, and specify the right COM port to use for Trumpet.

Configure the LOGIN.CMD script to work with your screens.

If you use a text editor like DOS Edit, you should be able to read and modify this file. Anything in bold is commentary that was added here and is not present in the original file. Please read them as such. The LOGIN.CMD script can be found in your BBS and should be distributed to all of your clients who will be using Trumpet Winsock to get into SLIP/CSLIP. Once you know the login.cmd file works, you should distribute it to your clients.

The standard login script does the following things:

- If the user is a first time user of SLIP, it asks for the username, password and phone number to call. It writes this information at the end of the TRUMPWSK.INI file. If you find yourself in a situation where one of your users make a mistake while typing this information in, simply ask them to Edit the TRUMPWSK.INI file and delete the last lines with $number, $username and $password on them.

- It does some basic modem stuff like resetting the modem and dialing up the provider till there's a valid connection.

- It **waits for the language prompt**. If it sees "1 to 2", it selects 1 and carries on.

- It **waits for the username prompt**. If it sees the word "new", it sends the user's name with the SLIP prefix in front, **like slip:JohnDoe**. Note that we wait for the word "new" because on a standard setup of MajorBBS or Worldgroup, the whole user name prompt looks like this:

> **If you already have a User-ID on this system, type it in and press Enter. Otherwise type "new":**

  As you can see, the line that asks for the user name proper is **Otherwise type "new":** so we simply look for the last word on that line, the word **'new'**.

- It **waits for the password prompt**. If it sees the word "password", it sends the user's password normally.

- It waits for the IP address. If it sees the **"Starting SLIP server"** prompt, **it captures the IP address displayed and plunks it into the IP address field of the Trumpet Winsock setup screen.**

- User can now minimize Winsock and start the various Trumpet Winsock clients that exist out there.

As you can see, there are several things that the Script looks for that might not be the same on your system. Namely the Language prompt, the username prompt and the password prompt. Sometimes, the "Starting SLIP server" prompt also gets modified (usually simple colorization). **You should not colorize the latter**.

To make sure that this script will work with your system, you should use a terminal program to logon your own system with the screen capture on. Then, you should compare the result with the information given just a couple of paragraphs back. Here is a sample login sequence that simulates the kind of problem you may face:

```
Auto-Sensing

Connected to Sticky Widgets BBS.
Running Galacticomm's Worldgroup
<insert a very big ansi art picture>
(N)on-Stop, (C)ontinue, (Q)uit: C
<insert the rest of the picture>

If you are a new user, type in "new"
else, just type in your username: slip:JohnDoe

Now, what's your password?: xxxxxxx

***
Starting SLIP server mode: Your address is: 199.84.216.128
```

What differs from a standard straight logon sequence here?

- There's no language question.
- The line where the user is prompted for his username does not contain the word "new"
- There's a (C)ontinue question because of a very big ANSI logo.

How do we solve the problem?

- We delete the lines of the Script that deal with the language question.
- Instead of looking for the word "new" for the username prompt, we can look for "username"
- We should add a few lines in the script for the (C)ontinue question.

The classic Login Script with detailed commentary

```
#-------------------------------------------------------------------------------------------------------------
# Here we ask the first time Trumpet user to enter the phone number
#
if ![load $number]
 if [query $number "Enter your dial up phone number"]
   save $number
 end
end
```

```
#-------------------------------------------------------------------------------------------------------------
# Then the username
#
if ![load $username]
  if [username "Enter your login username" (Enter slip:yourUserID)]
    save $username
  end
end
#-------------------------------------------------------------------------------------------------------------
# Then the password
#
if ![load $password]
  if [password "Enter your login password"]
    save $password
  end
end
#-------------------------------------------------------------------------------------------------------------
# Here we define our prompts.  *IMPORTANT* This is where we need to change
# things at least partly to make the script work with any type of screen setup.
#
$modemsetup = "&c1&k3"
$userprompt = "new"              <- Username prompt variable, alter to fit with your screens
$passprompt = "password:"        <- Password prompt variable, alter to fit with your screens
$addrtarg = "Your address is:"
#-------------------------------------------------------------------------------------------------------------
#  This is where we do the dialing stuff, ignore.
#
%attempts = 10
output "atz"\13
if ! [input 10 OK\n]
  display "Modem is not responding"\n
  abort
end
output "at"$modemsetup\13
input 10 OK\n
%n = 0
repeat
  if %n = %attempts
    display "Too many dial attempts"\n
    abort
  end
  output "atdt"$number\13
  %ok = [input 60 CONNECT]
  %n = %n + 1
until %ok
input 10 \n
wait 30 dcd
```

```
#-------------------------------------------------------------------------------------------------------------
# This is where we wait for the language prompt.  If you do not use a language
# prompt on your screens, remove these lines between the #----- seperators.
#
display "Waiting for Language prompt..."\n
input 30 "1 to"
output 1\13
#-------------------------------------------------------------------------------------------------------------
#  Here we wait for the username prompt.  You may need to change the $userprompt
#  variable in the prompt definition section.  Simply modify what's in the the quotes.
#
display "Waiting for User-ID prompt..."\n
input 30 $userprompt
output $username\13
#-------------------------------------------------------------------------------------------------------------
#  Here we wait for the password prompt.  You may need to change the $passprompt
#  variable in the prompt definition section.  Simply modify what's in the the quotes.
#
display "Waiting for Password prompt..."\n
input 30 $passprompt
output $password\13
#-------------------------------------------------------------------------------------------------------------
#  Here we wait for the SLIP mode prompt.  It should *NEVER* be changed.
#
input 20 ***
input 5 $addrtarg
address 5
display \n
display Connected.  Your IP address is \i.\n
#-------------------------------------------------------------------------------------------------------------
# SLIP/CSLIP connection established.
```

Here are the lines we will modify to make it work with the example:

We delete the following lines because we don't have a language prompt

```
# This is where we wait for the language prompt.  If you do not use a language
# prompt on your screens, remove these lines between the #----- seperators.
#
display "Waiting for Language prompt..."\n
input 30 "1 to"
output 1\13
```

We modify this line to check for the word "username" instead of "new"

$userprompt = "new"** becomes **$userprompt = "username"

And finally, we need to add a few lines at the right location in the command sequence. It so happens that the location where the language prompt WAS is perfect to check for the continue prompt at the beginning of the login procedure. Here are the lines we insert:

```
display "Waiting for the (C)ontinue prompt..."\n
input 30 "(C)ontinue"
output C\13
```

So the new script will look like this:

```
#-------------------------------------------------------------------------------------------------------------
# Here we ask the first time Trumpet user to enter the phone number
#
if ![load $number]
 if [query $number "Enter your dial up phone number"]
   save $number
 end
end
#-------------------------------------------------------------------------------------------------------------
# Then the username
#
if ![load $username]
  if [username "Enter your login username" (Enter slip:yourUserID)]
    save $username
  end
end
#-------------------------------------------------------------------------------------------------------------
# Then the password
#
if ![load $password]
  if [password "Enter your login password"]
    save $password
  end
end
#-------------------------------------------------------------------------------------------------------------
# Here we define our prompts.  *IMPORTANT* This is where we need to change
# things at least partly to make the script work with any type of screen setup.
#
$modemsetup = "&c1&k3"
$userprompt = "username"        <- Username prompt variable, alter to fit with your screens
$passprompt = "password:"       <- Password prompt variable, alter to fit with your screens
$addrtarg = "Your address is:"
#-------------------------------------------------------------------------------------------------------------
#  This is where we do the dialing stuff, ignore.
#
%attempts = 10
output "atz"\13
if ! [input 10 OK\n]
  display "Modem is not responding"\n
  abort
end
output "at"$modemsetup\13
input 10 OK\n
```

```
%n = 0
repeat
  if %n = %attempts
    display "Too many dial attempts"\n
    abort
  end
  output "atdt"$number\13
  %ok = [input 60 CONNECT]
  %n = %n + 1
until %ok
input 10 \n
wait 30 dcd
#-------------------------------------------------------------------------------------------------------------
# Waiting for the continue prompt
#
display "Waiting for (C)ontinue prompt..."\n
input 30 "(C)ontinue"
output C\13
#-------------------------------------------------------------------------------------------------------------
#  Here we wait for the username prompt.  You may need to change the $userprompt
#  variable in the prompt definition section.  Simply modify what's in the the quotes.
#
display "Waiting for User-ID prompt..."\n
input 30 $userprompt
output $username\13
#-------------------------------------------------------------------------------------------------------------
#  Here we wait for the password prompt.  You may need to change the $passprompt
#  variable in the prompt definition section.  Simply modify what's in the the quotes.
#
display "Waiting for Password prompt..."\n
input 30 $passprompt
output $password\13
#-------------------------------------------------------------------------------------------------------------
#  Here we wait for the SLIP mode prompt.  It should *NEVER* be changed.
#
input 20 ***
input 5 $addrtarg
address 5
display \n
display Connected.  Your IP address is \i.\n
#-------------------------------------------------------------------------------------------------------------
# SLIP/CSLIP connection established.
```

STEP #12:

Configure the NNTPD News Server Module

Overview

The internet has an equivalent to MajorBBS/Worldgroup forums called Usenet. Usenet is comprised of close to twelve thousands different Newsgroups (forums), each interested in just about every subject imaginable, from the sublime to the totally ridiculous. Contrary to services like Genie, Compuserve or AOL, there is no central computer system where Newsgroups are stored. All over the internet, thousands of systems keep copies of the entire mass of messages that have been posted to various Newsgroups. They accomplish this using the NNTP protocol or Network News Transfer Protocol.

NNTP is the means by which news is ferried back and forth between computer systems on the Internet. In the case of your computer system, this means that you'll need to find a source to obtain your news from and send your posts to. In most cases, one obtains a newsfeed from the same people who provide you with your internet connectivity, meaning your provider. The big questions is, how much news do you want to carry? Realistically, the amount of news your system can carry depends on two factors: **bandwidth, storage and system speed**.

Bandwidth: The speed of your connection to your provider is the first limiting factor. How much of your bandwidth are you willing to sacrifice solely for Newsgroups? Also, some newsgroups have more traffic than others. The **alt.binaries** Newsgroups carry so much traffic that for each one of those Newsgroups you could carry several dozen Newsgroups with only moderate traffic. That's something to think about when you decide what you want to carry.

Storage: How long do you want to keep messages before you delete them? 3 days? 10 days? If you plan to carry several hundred newsgroups, you may find yourself in a dilemma. Do you tie up more bandwidth and disk space for your newsgroups? How much is enough?

System speed: It takes time to import all these messages into the system. While the system is transferring a message from an incoming batch to the Forums, this increases the load on the disk and slows down other disk accesses. It also gobbles up CPU cycles, which also slows down the system.

Just to give you a baseline to start from, someone who wants to carry a full newsfeed (12,000 newsgroups) requires at least a T1 connection (1.2 megabit per second). A full feed also requires 1 gigabyte of storage per day before deletion. And these numbers will only grow over time.

***IMPORTANT NOTE* For NNTP to work properly, SMTP and Rlogin must be installed and running on your system.**

MajorTCP/IP's NNTPD's implementation specifics

MajorTCP/IP's implementation of NNTP will import Usenet Newsgroups directly into the MajorBBS/Worldgroup Forum architecture. Any public posts or replies in those Forums defined as Usenet Newsgroups will be exported back to your provider so that these messages will be disseminated through-out Usenet. The really interesting thing about MajorTCP/IP's solution to Usenet News importing/exporting is that your users don't need to relearn how to use another messaging engine. They can use the Newsgroups like they would use any other Forum on your system.

The Newsgroup Hierarchy

Newsgroups follow a naming hierarchy that is fairly easy to understand. Most Newsgroups you will carry will belong to one of these hierarchies. Other hierarchies exist, but these mostly deal with national issues. For instance, Canadian-specific newsgroups start with **can.***

alt.* Alternate Newsgroups. This is where most Newsgroups that don't fit anywhere else wind up. Not all providers carry the full list of alt groups. You may want to check with your provider. Alt groups are not carried by every service provider because it's much easier for people to start an alt group than to start a group in the other hierarchies. This often leads to frivolous topics like **alt.wesley.crusher.die.die.die** which providers don't want to waste disk space carrying.

biz.* Business Newsgroups. Most of these groups allow advertising although you must still stick to the newsgroup's topic. These groups are mostly for the business community and entrepreneurs.

comp.* Computing Newsgroups. This is where discussions about computers occur. Topics range from hardware issues to computer languages and programming issues to issues about specific products. **comp.bbs.majorbbs** is the newsgroup that talks about the MajorBBS and Worldgroup line of products and third party software.

misc.* Miscellaneous Newsgroups. This is pretty much like the alt.* hierarchy but has attained greater legitimacy. The entire hierarchy is carried by most providers with large newsfeeds.

news.* The Usenet Admin Newsgroups. This is where policy about Usenet and questions concerning internet services including Usenet can be posted to. The **news.newusers.questions** is highly recommended. Your users will be able to ask Internet questions and get answers from highly knowledgeable people.

rec.* The Recreation Newsgroups. These involve mostly discussions about recreational topics from basket weaving, to sports, to model car racing and hundreds of other activities. Discussions about books, television and movies are part of the rec hierarchy.

sci.* The Science Newsgroups. This is where most of academia discuss scientific topics ranging from the abstract like theoretical physics and cosmology to the more practical like engineering and biology.

soc.* The Social issues Newsgroups. This is where you'll find topics ranging from feminism to cultural discussion groups based on nationality and religion.

talk.* The controversy Newsgroups. Talk newsgroups often involved highly controversial topics from discussions about origins (evolution versus creationism) to abortion, passing through atheism. Eternal flame-wars abound here so make sure you are wearing an asbestos suit.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

There is one element of Usenet that has to be emphasized: basic **netiquette or net-etiquette**. Just like on BBSes, there are certain social rules that have to be respected when people post messages to Newsgroups. These social conventions evolved as Usenet took shape years ago. It would be very good for you to advise your users on basic netiquette. People who abuse Usenet will invariably cause you problems in the form of nastygrams, complaints, and sometimes even mail-bombing campaigns, which can literally overwhelm your hard-disk and totally clog your bandwidth.

Basic Net-Etiquette

Here is the comprehensive list of rules that your users are expected to follow when posting messages to Newsgroups. It may be a good idea for you to write a document explaining this to your users. Comments in brackets [] are additions from the author of this manual. *From "THE NET USER GUIDELINES AND NETIQUETTE", By Arlene H. Rinaldi, Academic/Institutional Support Services Florida Atlantic University July, 1994*

- Keep paragraphs and messages short and to the point.

- Focus on one subject per message and always include a pertinent subject title for the message, that way the user can locate the message quickly. **[Note: as opposed to many posts on BBSes where a user will reply to 10 different people in a single message]**

- Don't use the academic networks for commercial or proprietary work. **[Note: Usenet was originally run by the North-American universities. Any kind of commercial message, especially advertising is seen as being in very bad taste.]**

- Include your signature at the bottom of E-mail messages. Your signature footer should include your name, position, affiliation and Internet and/or BITNET addresses and should not exceed more than 4 lines. Optional information could include your address and phone number.

- Capitalize words only to highlight an important point or to distinguish a title or heading. *Asterisks* surrounding a word also can be used to make a stronger point. Capitalizing whole words that are not titles is generally termed as SHOUTING!

- Limit line length and avoid control characters. **[Note: most Unix newsreaders chop lines at the 72nd characters. Lines that are too long might appear awkwardly on these systems.]**

- Follow chain of command procedures for corresponding with superiors. For example, don't send a complaint via E-mail directly to the "top" just because you can.

- Be professional and careful what you say about others. E-mail is easily forwarded.

- Cite all quotes, references and sources and respect copyright and license agreements.

- It is considered extremely rude to forward personal E-mail to mailing lists or Usenet without the original author's permission.

- Be careful when using sarcasm and humor. Without face to face communications your joke may be viewed as criticism. **[Note: badly written humor or sarcastic remarks have been the source of many flame-wars on usenet.]**

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

- Acronyms can be used to abbreviate when possible, however messages that are filled with acronyms can be confusing and annoying to the reader.

Other issues noted by the author of this manual include:

- Your user should spend some time getting acquainted with the particular Newsgroups they are following before posting messages. Each group has a charter and a FAQ (Frequently Asked Questions) that gets posted once or twice a month. Users should read the FAQ of a newsgroup before posting to it.

- Users should stick to the Newsgroup's topic. Talking about beer-making in the sci.astro.amateur newsgroup is very bad Netiquette.

- Usenet is International. References to obscure television shows or publications unique to your nation might not be understood by people from other countries. It's good to add a little bit of explanation to such references. For instance, people in Japan or Russia may not know who Rush Limbaugh is.

In addition, there are other rules that if violated, may bring great harm to your system:

- Make it very clear to your users that commercial posts in inappropriate newsgroups may very well get your system in trouble. People who advertise products in inappropriate newsgroups will often result in the mass mail-bombing of your system. Mail bombing is simple: hundreds of people will **each** send hundreds of copies of the same E-mail to the offending user and/or the postmaster (ie: sysop), filling up your hard-disk and tying up your connection to the net.

- Chain Letters, pyramid schemes and other fraudulent money-making schemes WILL get the offending user in trouble and will result in the mail-bombing of your system. Some people on the internet will go as far as calling the F.B.I. warning them of your user's improprieties.

- Posting the same message to multiple newsgroups, often in newsgroups where the message doesn't belong is regarded as SPAMMING, and will result in the cancellation of the messages, and some nasty-mail to you complaining about the offending user.

NNTP importing/exporting and it's effect on TCP Handles

Each concurrent NNTP importing session uses up one TCP Handle. Usually, you will only allow one importing session at a time (via NNTPMAX). In addition, export of posts done on your BBS to Usenet will also use up one TCP Handle. For more details about TCP Handles, check out NBTCP (**page 32 of this manual**).

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Installation procedure for the NNTP Module

Setting up NNTP is a fairly straight-forward process. Simply follow the sequence of instructions on this page and you'll be fine. Make sure you have the **"what you need to know"** section of this manual on hand and filled out to configure NNTP properly.

Step by Step installation procedure for the NNTP module

STEP	Description	Done
#1	Put the TCPNNTPD Daemon (Module) in the menu tree	
#2	Configure the TCPNNTPD.MSG message file	
#3	Define the forums that will carry Usenet traffic	
#4	Generate the forum mapping	
#5	Give your provider the list of newsgroups you wish to carry	

Put the TCPNNTPD Daemon (module) in the menu tree

You need the NNTP Daemon (module) in the menu tree because it's through this module that you will generate your newsgroup-to-forum mapping. The forum mapping is simply a database that lists the newsgroups you carry and their corresponding forums. From this database, information is kept about the messages received by message-ID. The NNTP server at the provider remembers which messages were sent, but it still queries your NNTP server to see if it wants to receive a message with a specific ID. Your NNTP server agrees or denies the request. The BBS has no way to actively tell the provider's machine which newsgroups to feed. (That's why the last step is to give your provider the list of newsgroups you want to carry).

Use the following procedure to create the NNTP maintenance page

- From the main configuration menu (CNF), select **F2 - Design Menu Tree**
- Make sure that the menu item cursor is located on **your Sysop menu page**
- Select **F2 Edit** to change the Sysop Menu page
- Go to the menu options area and **add a new option**, say [N] for NNTP maintenance.
- In the **EDIT OPTION** window ...
    - Short Description .....could be "NNTP Maintenance"
    - Key required for this option..... **SYSOP or MASTER key.**
    - Destination page..... could be called **NNTP**
    - **Save the menu**. A new page in the menu tree should've been created.
- Move the cursor to the new page called **NNTP.**
- Press **F2 Edit** to configure this module page.
    - Allow go to this page ..... should be set to **YES.**
    - Key required ..... **The SYSOP or MASTER key.**
    - Select module window, you should chose the **NNTPD Deamon.**
    - Display header ..... should be set to **YES.**
    - Command String ..... Leave it blank.
    - Save the resulting page.
- That's it!

Configure the TCPNNTPD.MSG message file

Level 3 - Security and Accounting configuration

- From the main configuration menu (CNF), select **F3 - Accounting and Security**
- Press on **F8 - Search**, type **TCPNNTPD.MSG**
- The first item you should find is the **SNNKEY** parameter.
- Edit each item as described below, moving from item to item using the arrow keys.
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu.

SNNKEY **Key required to send Usenet Messages.**
NORMAL Users will need this key for NNTP to process their outgoing Usenet messages. If they don't have the proper key, NNTP will not accept their messages. This key applies only to outgoing messages transported by the NNTP exporter. Replies by E-mail to Usenet messages do not count inasmuch as the SNNKEY is concerned. **This key is only used by Worldgroup**. Because MajorBBS v6.25 must uses the **MHS messaging engine**, we have to use SMTP's **SMLKEY** to provide the same surcharging. **Check out page 131 of this manual** in the SMTP section. **SMLKEY is found in level 4 configuration, under TCPSMTP.MSG**

SANNKEY **Key required to send attachments.**
NORMAL Users will require this key if they want to be able to send file attachments using NNTP. If they don't have this key, the file attachment won't be sent and a notice of that will added to the body of the Usenet post. **This key is only used by Worldgroup**. Because MajorBBS v6.25 must uses the **MHS messaging engine**, we have to use the SMTP's **SAMLKEY** to provide the same surcharging. **Check out page 131 of this manual** in the SMTP section. **SAMLKEY is found in level 4 configuration, under TCPSMTP.MSG**

NNTPCHG **NNTP per-message surcharge.**
0 You may want to charge users extra for sending NNTP messages. The charge you enter here will be added to regular forum message charges when users write NNTP messages. If you wish to charge users extra for writing NNTP messages, enter a surcharge here. If you want to give users credits for using NNTP, enter a negative number here, or enter zero for free NNTP use. This Key is only used for messages transported by the exporter. Replies by E-mail to Usenet posts aren't surcharged by this key. **This key works only with Worldgroup. There is no MajorBBS 6.25 equivalent.**

NNTPATCH **NNTP attachment surcharge.**
0 You may want to charge users extra for attaching files to NNTP messages. The charge you enter here will be added to regular forum attachment charges when users write NNTP messages. If you wish to charge users extra for attaching files to NNTP messages, enter a surcharge here. **This key works only with Worldgroup. There is no MajorBBS 6.25 equivalent.**

NNTPPKCH **NNTP attachment per-kbyte surcharge.**

0 You may want to charge users attaching files to NNTP messages on a per-kilobyte basis. This way, users will be charged more for attaching larger files. The charge you enter here will be added to regular forum attachment charges when users write NNTP messages. If you wish to charge users per-kilobyte for attaching files to NNTP messages, enter a surcharge here. **This key works only with Worldgroup. There is no MajorBBS 6.25 equivalent.**

Level 4 - System options configuration

- From the main configuration menu (CNF), select **F4 - Configuration options**
- Press on **F8 - Search**, type **TCPNNTPD.MSG**
- The first item you should find is the **NNTPENAB** parameter.
- Edit each item as described below, moving from item to item using the arrow keys.
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu.

NNTPENAB **Enable NNTP Server.**

NO Use this parameter to enable or disable your NNTP server. If set to **NO**, most of the following parameters will be invisible.

NNTPENA2 **Display message to NNTP request?**

NO While you're saying that you want the NNTP Server to be disabled, do you want the NNTP server to tell the users that it is disabled (**message NNTPISB**) or do you want it just to refuse all NNTP Server connections. Leaving this parameter to **NO** will simply force the disabled NNTP server to refuse connection. **This parameter is visible only when NNTPENAB is set to NO.**

NNTPMAX **Maximum concurrent NNTP Server Feeds.**

1 NNTPMAX sets the maximum number of incoming NNTPD feeds to your BBS NNTPD will accept. This should normally be set to 1, unless you have multiple feeds. Multiple feeds from different news providers should be under the proviso that newsgroups imported from one provider shouldn't be imported from another. **This parameter is visible only when NNTPENAB is set to YES.**

NNTPFEED **Numeric IP address of your provider's NNTP server.**

0.0.0.0 Enter here the IP address of the NNTP Server that can feed you news. If you leave this blank, anyone can send you news. It's not a good idea to leave this blank. **Enter the numeric IP address you noted down on page 25 of this manual, in the "what you need to know" section. This parameter is visible only when NNTPENAB is set to YES.**

NNTPEFED **Numeric IP address of your News of exporter.**

0.0.0.0 Enter here the IP address of the NNTP Server that will accept a newsfeed from you. We'll be calling this server to export new messages that were posted in the USENET forums that we carry. If you leave NNTPEFED to 0.0.0.0, the exporter will be disabled. In most cases, NNTPFEED and NNTPEFED will be the same, as you'll probably get your feed and export posted messages to him. **Enter the numeric IP address you noted down on page 25 of this manual, in the "what you need to know" section. This parameter is visible only when NNTPENAB is set to YES.**

NNTPDORG **Organization.**
<Empty> Enter here the "organization" your BBS is a member of. This will be showed in an organization header line on **outgoing posts** transmitted by the NNTP exporter. To use our well-used example, the Widgets BBS could represent the **Widgets Manufacturing company**, so this is what they would enter as an organization. **This parameter is visible only when NNTPENAB is set to YES.**

NNTPEDLY **Delay between exporter runs (Minutes).**
30 If you have the **NNTP exporter enabled**, (**NNTPEFED is set to a value other than 0.0.0.0**), this field control how often the exporter will try to send new messages in USENET forums to the remote NNTP server. The delay is in minutes. **This parameter is visible only when NNTPENAB is set to YES.**

NNTPMSS **Maximum Segment size of NNTP Server Connections.**
1024 You can set the maximum length of packets sent and received by your NNTP Server. The smaller the packet size, the less impact NNTP transfers will have on your other telnet/rlogin/... services. However, NNTP Server throughput will be reduced. **Leave to 0 to use the default system-wide MSS**. MajorTCP/IP will automatically adjust this value so that it doesn't exceed the system-wide MSS. For more information concerning MSS, **check out page 31 of this manual describing the system's MSS. This parameter is visible only when NNTPENAB is set to YES.**

NNTPLOG **Record NNTP connections in log.**
YES Set this option to **YES to record incoming NNTP connections** into the TCP/IP Log. (defined in TCPLIBM.MSG). **This parameter is visible only when NNTPENAB is set to YES.**

DBUGLVL **Debugging Level (for LOG file).**
1 This selects the level of debugging information that will be recorded in the log file. 0 Disables the log, 9 turns on full debugging. Full debugging might slow down the BBS, somewhat. **If you just installed the system, it is suggested that you run on full debugging for the first few days. This parameter is visible only when NNTPLOG is set to YES.**

NNTPPATH **Work directory for NNTP.**
.\NNTPD.DIR NNTP will be using a directory for workfiles. Enter here the path and directory name you want NNTP to use for that directory. Do not put a trailing '\'. This directory is where all mail batches are stored. **This parameter is visible only when NNTPENAB is set to YES.**

NNTPDPFX **NNTP & NNTPD Prefix.**
US This is the prefix that is used by NNTP and NNTPD to indicate USENET posting. We recommend that you leave this at the default **US**. **This only applies to the NNTP exporter. This feature is similar to SMTP where all message destinations are prefixed with INT. US will serve as the prefix for Usenet News.**

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

NNTPNAM **Name of NNTP exporter.**
Usenet News Each exporter is identified in lists and help messages by a name and/or description. Enter the name you wish to use to identify the **NNTP exporter**. **This option has to be set with WORLDGROUP Only.**

NNTPDSC **NNTP exporter desc.**
NNTP Usenet news handler Each exporter is identified in lists and help messages by a name and description. Enter here the description you wish to use to identify the NNTP exporter. **This option has to be set with WORLDGROUP Only.**

NNTPXMP **Example NNTP address.**
US:misc.test In some help messages, users may be shown an example address for an exporter. This example should include the prefix specified in NNTPDPFX and show a typical address with proper format for NNTP. **This option has to be set with WORLDGROUP Only.**.

NNTPHLP **NNTP help message.**
<box below> Users may request detailed help on specific exporters. This message will usually explain how to address a message to someone using NNTP, who your users can expect to reach, and possibly what charges apply when using NNTP. You are free to provide whatever message you think would be most helpful. **This option has to be set with WORLDGROUP Only.** Exporter only.

NNTP is the Internet standard protocol for real-time exchange of Usenet News. To send a message to a newsgroup using NNTP, you need the newsgroup address. Once you have the address, you tell the server that this is a Usenet address by entering "%s:" followed by the address.

NNTPEPFX **SMTP E-mail prefix.**
INT This is the prefix you have defined in option **SMTPPFX (level 4, TCPSMTP.MSG)** if you are using SMTP to deliver Internet E-mail. If you are using any other E-mail program for internet E-mail, enter the prefix that you have assigned to that internet E-mail program. This will allow proper delivery of E-mail replies to posters of messages in the USENET forums. **This parameter is visible only when NNTPENAB is set to YES. Removed as of v1.78-E.**

MHSINPT **MHS-IN directory.**
.\MI This is the directory used by MHS to scan for new incoming messages. NNTP will write incoming messages in there. **It should be the same as Level 4 configuration option INMSG (in GALMS.MSG). This is not used if you are running WorldGroup.**

INTMOUT **Single step timeout for Incoming (minutes).**
5 This is the timeout for incoming NNTP server connections. This timeout will be triggered after n minutes without activity on the link. **This parameter is visible only when NNTPENAB is set to YES.**

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

SMLOW1 **Minimum disk space available for NNTP (MB).**
5 When the amount of free diskspace reaches the defined number for SMLOW1, no new NNTP requests will be allowed to start. (this number is in MEGABYTES). Set to 0 to disable. This number should be a multiple of SMLOW2. **This parameter is visible only when NNTPENAB is set to YES.**

SMLOW2 **Minimum disk space available for NNTP (MB).**
1 When the amount of free diskspace reaches the defined number for SMLOW2, all current NNTP sessions will be terminated abruptly. Set to 0 to disable. This number is in MEGABYTES. This number should be smaller than SMLOW1. **This parameter is visible only when NNTPENAB is set to YES.**

IMPCYC **Import Task Wake Up Delay.**
30 This control how often (in seconds) that the Usenet importer task will wake up to see if any new batches of Usenet messages are waiting to be imported.

IMPSLOW **Import Task slow down factor.**
0 The import task will normally only use "spare" processing cycles. However, you may want the import task to skip some cycles, if it still slows your BBS down too much. The number entered here is the number of spare cycles that will be skipped.

IMPATT **Convert long messages to attachments.**
YES The normal "MajorBBS" way of dealing with large text messages is to split them in multiple forum messages. If you set IMPATT to yes, then the long messages will instead be converted into file attachments. **NOTE: On 6.25, the attachments will not be automatically approved.**

DFTEXPY **Default Expiration of history file (DAYS).**
1 **On MajorBBS 6.25**, NNTPD can't keep track of the messages posted in the forums. So you must define a default expiration timer for the NNTP history file. This file is only to prevent you from receiving duplicate messages. This timer is a number of DAYS. **Only used with MajorBBS 6.25**.

DOCANCEL **Process CANCEL control messages.**
NO MajorTCP/IP can process CANCEL messages requesting that one message from the forums (Usenet only) must be deleted. However, note that anyone can forge a CANCEL message and thus delete other messages. DOCANCEL decides if you want MajorTCP/IP to delete the message or only record the CANCEL request in the appropriate forums. **This option is ALWAYS NO on MajorBBS 6.25.**

NNTPDSG **Default signature for messages delivered by NNTP.**
<Empty> This parameter allows sysops to set a system-wide default signature for Messages posted to Newsgroups. These signature lines will be added automatically at the end of all messages sent via NNTP. **Leave empty to disable. This option is visible only if NNTPENAB is set to YES.**

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Define forums to carry Usenet traffic

Now that you configured the NNTP message file correctly, you need to define which newsgroups you will carry in your forums. To do this, you need to create new forums with proper access privileges. **Refer to the list of newsgroups you've requested from your provider. (mentioned on page 25 of the "what you need to know" section)**. For our examples, we will be using the **comp.bbs.majorbbs Newsgroup**, which carries information about MajorBBS and Worldgroup including third party software. The forum creation procedure for MajorBBS v6.25 is slightly different from the Worldgroup procedure. Each is explained separately. Repeat the same procedure for each Newsgroup you wish to define.

Defining Newsgroups under Worldgroup

- Start up your BBS using the **F5-GO!** command.
- Once the system is up and running, **press on F7-Login to log-on locally**.
- From Worldgroup's Main Menu, **select option (F)** to go into the Forums menu.
- From the Forum menu, **select option (O)** to go into the Operations menu.
- From the Operations menu, **select option (C)** to create a new Forum.
    - Forum name ..... Type in **CompMBBS**.
    - Description ..... Type in **Usenet comp.bbs.majorbbs newsgroup**
    - (Define the various access privileges parameters as you wish)
    - Exit (Save/Quit ...).. Select **SAVE.**
- After saving the forum, **select the option (E)** to Edit Echoes.
- At the "Echo address to add:" prompt, type in **US:comp.bbs.majorbbs.**
- After pressing enter, the entry is recorded. You should see the same menu. **Press Enter**.
- **Finally, press Enter to create the Forum**.
- **You're done.**

Defining Newsgroups under The MajorBBS version 6.25

- Start up your BBS using the **F5-GO!** command.
- Once the system is up and running, **press on F7-Login to log-on locally**.
- From The MajorBBS's Main Menu, **select option (F)** to go into the Forums menu.
- From the Forum menu, **select option (O)** to go into the Operations menu.
- From the Operations menu, **select option (C)** to create a new Forum.
    - When asked for the Forum name, type in **/CompMBBS**.
    - (Define the various access privileges parameters as you wish)
    - MajorBBS will then make you create the first message of this forum.
        - At the Topic box, type in **Usenet comp.bbs.majorbbs newsgroup**
        - Type in the body of the message at the top the line that tells MHS how to deliver messages to and from this forum....
          Type in MHS ADDR: US:comp.bbs.majorbbs.
        - **Press on CTRL-G to save the message.**
    - The Forum should be created at this point.
- **You're done.**

Generate the forum mapping

Once you've defined the Newsgroups your forums will carry, you have to generate the forum mapping that MajorTCP/IP will use to associate the Forums with the corresponding Internet Newsgroups. The mapping function generates a file that contains the names of the Forums, the corresponding Newsgroups they carry, and the number of the last message received from each newsgroup. **Each time you create or delete a Forum with it's associated Newsgroup, you must rebuild the forum mapping.**

To generate the forum mapping, we need to go the NNTPD module that you've put in the menu tree earlier in the pages of this section.

- Log-on to your system under an account with **SYSOP or MASTER** access.
- From the Main Menu, **chose the menu option that corresponds to your net services**.
- From your Internet Menu, **chose the option that calls up the NNTPD module**.
- This is the menu you should see:

```
MajorTCP/IP -- NNTPD Sysop menu
===========================
1 - Rebuild Usenet to Forum Mappings.
2 - Log a batch file for importing.
X - Exit

Enter your choice >
```

- Select **option number 1** from this menu.
- The reconstruction of the mapping file takes a few seconds.
- **You're done!**

Give your provider the list of newsgroups you wish to carry

You're almost ready. Once the forum mapping is done, all that's left for you to do is to hand over the list of newsgroups you will carry. You must tell your provider to start the feed to your system. Make him aware that MajorTCP/IP uses the IHAVE (aye-have) protocol and that he should adjust his News Server accordingly.

If you run into problems, you should contact our Tech Support service mentioned at the beginning of this manual. It's important for you to provide us with the TCPLOGF.LOG file in your BBS directory which will tell us the behavior of NNTP. **Make sure that your DBUGLVL is set to 9 (Full Debugging). See TPCNNTPD.MSG, level 4 configuration in this section of the manual.**

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

STEP #13:

Configure the IRC Client module

Last revised July 29th, 1996

The new capabilities illustrated here have been added to the **IRC Beta 2 version**. New features include: a list of default IRC servers that will be cycled through if the BBS cannot connect to a server, default nickname and description for each user and standard accounting and security features that let you set various access keys and credit charge rates for IRC usage. Note that should any problems arise, you should report them to our technical support staff.

- Added "trick" paragraph and section new facilities in the IRC Server list (SERVnn option).
- Added /QUOTEKEY key (level 3 CNF) that restricts access to the /QUOTE command. /QUOTE is a porwerfull command letting you send "RAW" commands to an IRC Server.
- Added CARABT, ULBASE and MOTDDSP options in level 4 CNF, TCPIRC.MSG.
- Added the UPLOAD, DCCSEND, DCCCANCEL and /QUOTE command to the IRC commands available online.

Overview

IRC stands for Internet Relay Chat. It was developed in 1988, as a way for people on the Internet to chat with each other. It's like the MajorBBS/Worldgroup teleconference, except on a much wider scale. Some parts of the IRC have over 5000 people chatting at once. There are usually thousands of channels or topics to choose from.

Like the rest of the internet, the IRC is a system based on the principal of redundancy. There's no central system that people hook-up to. Instead, we have several dozen servers linked together that act as entry points to the IRC network. Each server knows who is on the network and what channels these people are on. When a person types something on his machine, the message is broadcast thruout the network. If it happens to be a private line of text, only the server with the user whom the message is addressed to will display it. IRC servers are connected to a number of other servers. The whole forms the IRC network. Should one server go down, the traffic would simply employ an alternate path. This maintains the network's stability.

The Nitty Gritty

Each user that wishes to connect to the IRC networks does so using a program called an IRC client. The IRC client takes care of transmitting and receiving information between itself and the server the user connects to. In the case of MajorTCP/IP, each user uses an "instance" of the IRC client. To make it simpler, consider that each user on the MajorTCP/IP IRC client is a client on the IRC network. So if you have 10 people using IRC on your machine, they are 10 clients using the network.

The server you connect to does two things: it transmits data from client to server, and from server to server. The network of servers form the IRC network you are using. The number of servers out there is relatively unimportant. The more servers there are, the more people can go on IRC. On the other hand, the slower the response time as packets that go from your keyboard to a friend's screen at the other side of the network has more hops to make.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Another problem is that the more servers you have on the network, the more connections you have that links one server to a number of others. It takes time for a server to decide how it'll route a packet towards the destination. Ergo: the more connections you have for a particular server, the longer it takes this server to decide where to send the packet next.

Finally, there is more than one IRC network. The most important ones are the **Efnet** and the **Undernet**. People who are using a server on one network cannot talk to people connected to a server on the other network.

Problems with the IRC network

IRC is not the most stable environment to operate on. The biggest problems one sees on the various IRC networks are:

- **Net-Splits** Occurs when one server on the network goes down.
- **Net-Lag** Occurs when traffic on the network exceeds the total bandwidth.
- **IRC-Wars** Occurs when troublemakers go on a rampage to annoy normal users.

Net-Splits

A net-split occurs when one or more server goes down, or the connection from one server to other servers goes down. Usually, what a user on a channel sees is that several people seem to log-off simultaneously from the current channel. What's really happening is that the server those people are on has lost contact with the server our hypothetical user is on. Sometimes, entire segments of an IRC network can go down, generating some of the more spectacular net-split episodes. The funny thing about a net-split is that those users on the affected server see the same thing! They see the people on the other servers disconnecting en-masse.

There are many reasons WHY a net-split can occur. Sometimes, it's the physical machine that acts as a server that goes down. Sometimes, operators on the machine want to re-route traffic to other servers to increase performance. The disconnection and re-routing may take a few minutes. In the meantime, a net-split occurs between this server and other machines down the line as the operators close the connection to do their re-routing.

Can you do anything about net-splits? No. Net-Splits are totally outside of your or your provider's control. The way to avoid net-splits is to chose an IRC network that has less servers meaning, less chances of a breakdown (and less traffic). See the **Efnet** and **Undernet** sections.

Net-Lag

Network lag is a more generalized problem than net-splits. Network lag can be caused by a much larger number of factors. The principal symptom of network lag is simple: anything you type takes forever to reach everybody on the current channel. People notice lag when they type something and get a response to their text from 30 seconds to two minutes later. One way to see how much lag the IRC network is suffering from is by **pinging (see the IRC instructions section)** a user on the channel. **Pinging** tell us how much time it takes for a signal to go to a given user and back. Normally, lag is low when the delay is under 10 seconds. If it takes much more than 10 seconds, the connection from the user to another user on another server is **lagged.** Lag isn't uniform. Sometimes, lag only occurs between one server and another server. In fact, lag can even occur between a server and the client a given person is using.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

You can have multiple sources of lag:

- **Local Lag:** Your connection to your provider is slow because you're already stretching the capability of your bandwidth. If you have alot of people doing stuff like FTP or Web Surfing, or even receiving files via DCC and this exceeds the capacity of your bandwidth, lag will occur locally. Any ping to the outside world will exhibit lag. **Solution:** Increase your bandwidth, reduce the number of FTP/SLIP/DCC sessions allowed, reduce the MSS of your system to favor the interactive sessions like Telnet, Rlogin and IRC.

- **Provider Lag:** Your provider's connection to the internet is itself stressed by the heavy load of all those system your ISP is offering services to. Pinging someone else on the IRC network (on another server) would yield the same result as local lag. **Solution:** Provider must increase his bandwidth to the net, or you can switch providers. The second option should be used only if the lack of bandwidth on your provider's side is harming your system in other ways.

- **IRC Server Lag:** The server you are connecting to is already at it's peak loading capacity, or it's bandwidth on the net is already saturated. If you can ping somebody else using the same server, the delay shown will be only of a few seconds. But pinging someone on any other server will yield lag. **Solution:** Switch IRC servers.

- **IRC Network Lag:** The entire network itself is operating at full capacity. This often occurs at peak hours where IRC usage is at it's highest. Pinging anyone anywhere is practically impossible. **Solution:** Use IRC outside of peak load hours. Use an IRC network that has less volume.

IRC-Wars

One thing that can't be stressed enough about the IRC is that nobody owns it. Nobody controls the IRC. Even if you are the sysop of a machine on the net, this means nothing to the global internet. What you do have are "zones" of control.

- **Local Zone:** This is the only point where you really have control. Namely, you have control over who can and can't use your IRC client. This zone of control has more to do with the behavior of your users which can have repercussions on your connection. If you have users who are abusing their IRC priviledges by making trouble on channels, you can quickly find your system banned from some channels, and if severe enough, even some servers! Should you find yourself in such a situation, you'll have to negotiate with whomever operates a channel or server to get your system unbanned.

- **Channel Zone:** Any users that opens up a new channel becomes ChanOp or Channel operator. Some channels have **bots** that keep channels open and give Ops powers to particular users who were given permission by the bot's owner. Channels are created automatically when someone tries to join a new channel. Some popular channels are kept open and access to ops powers are restricted by the use of **bots. A bot is a program that runs on a Unix machine that acts like a user. Most bots are capable of multiple functions including the maintenance of a list of users who have the ability to gain ChanOps powers on the channel the bot is on.** Someone with ChanOps powers can do many things:

- They can change the channel's topic.
- They can ban and unban people from the channel.
- They can ban entire sites (like your BBS) from the channel.
- They can limit the number of users that can access the channel.
- They can make the channel secret, hidden, or invite-only.
- They can kick a person off the channel (without banning them).
- They can De-Op someone with Ops powers.

- **Server Zone:** Those people who operate the IRC servers have the power to ban sites from their server if the people calling from that site are causing trouble. They can also ban people from using offensive bots connected thru their servers.

Where all of this comes in:
IRC wars occur when smart kids have way too much time on their hands. Often, the goal of their game is to take control of channels, kick off the people who are using them, and make themselves general nuisances on IRC. You also have the various psychopaths that can also cause trouble simply by being their psychopatic selves.

People will "Flood" channels using file dumps on a given channel. Some will do private floods, doing the same thing but only on the screen of a target user. The more sophisticated IRC warriors will run "war-bots" on unix machines where the sole goal of the bot is to create as much mayhem as possible, by trying to Deop "channel-bots", ChanOperators, or even kick normal users off the channel by obtaining Ops powers. The methods used to counter these nuisances are many:

Channel Flooders: Channel flooders have to be kicked and banned from a channel to stop them from flooding it. **That's usually the job of the various Chanops on the channel**.

Private Flooders: Private flooders are actually easier to control. All the user needs to do is to use the **Forget <nick>** command. The command is described in **the IRC instructions section.** Forgetting a user simply stops all text output from such a user to reach you.

Op-warriors: Op-warriors are kids who are trying to gain Ops powers on a channel by trying to defeat the ChanOps or the Channel Bot. In some cases, one technique they use is "**riding the net-splits**". If a net-split occurs that makes them alone on the channel, they will have ops powers, being the only people there. Once that occurs, as soon as the other people come back to the channel as the system comes back to normal, they find themselves De-opped, banned and kicked off the channel. There's no real-defense against a net-split attack except by having a ChanOp on Every server of the IRC network. **The only recourse is to have the kids banned from the server they are using, giving the ChanOps time enough to regain control**.

War-Bots: War-Bots are like Op-warriors, except 10 times worse. They can lie in wait for the right net-split to come around and gain control of a channel. Like the previous paragraph, the only recourse is banning from an entire server. **You or other people on the channel that are victim of such an attack have to talk to the server operators on which the offending bot is connected from.**

Psychopaths: All the user needs to do is to do is use the **Forget <nick>** command to ignore these losers. The command is described in **the IRC instructions section.** Forgetting a user simply stops all text output from such a user to reach you.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Should one of your users cause troubles in the manners described above, it'll be your job to appeal to the appropriate people who have site-banned your system. Sometimes, site-banning is refered to as being **K-Lined**. The ultimate punishement is to be totally banned from an entire network.

IRC Networks: the EF-net and the Undernet

The EF-net was the first IRC network. It quickly became the most popular of the networks. Because of the extraordinary growth of the Internet, the EF-net has become plagued with all the problems mentionned above. Net-Splits, Net-Lag and IRC-Wars are rife on the EF-net. Yet despite all this, it remains popular with the IRC fans. On average, you can have over 10,000 people using the EF-net during peak hours, with over 5000 channels. But the EF-net is falling apart at the seams.

The Undernet is the largest alternative to the EF-net. Opened only a few years ago by people wanting to create an alternative to the EF-net, America-Online joined in on the effort to create a cleaner, more responsive network. Most Server Operators and Channel Operators cooperate together to keep the Undernet relatively free from the hackers that plague the EF-net. However, this being said, the Undernet is still the smaller kid on the bloc. On average, from 2000 to 3000 people use the undernet during peak hours, with around 1000 channels. The big advantage of the Undernet is stability, less lag, and less truancy. All and all, the Undernet is "cleaner".

A list of EF-net and Undernet servers can be found in the Annex.

The IRC client's effect on TCP Handles

Each user on IRC uses up one TCP Handle. If the user initiates a DCC connection while on IRC, he will use up another TCP Handle. For more details about TCP Handles, check out NBTCP (**page 32 of this manual**).

Installation procedure for the IRC Client module

Step by Step installation procedure for the IRC module

STEP	Description	Done
#1	Put the TCPIRC module in the menu tree	
#2	Configure the TCPIRC.MSG message file	

Put the TCPIRC module in the menu tree

To make it possible for your users to access the IRC client, you need to put the IRC module in the menu tree, preferably in the **Internet Services Menu** most sysops create for the various internet connectivity tools they use.

Use the following procedure to create the IRC client page

- From the main configuration menu (CNF), select **F2 - Design Menu Tree**
- Make sure that the menu item cursor is located on **your Internet menu page**
- Select **F2 Edit** to change the Internet Menu page
- Go to the menu options area and **add a new option**, say [I] for Access Internet Relay Chat.
- In the **EDIT OPTION** window ...
    - Short Description ..... could be “Access Internet Relay Chat (IRC)”
    - Key required for this option..... **The key required for internet access.**
    - Destination page..... could be called **IRC**
    - **Save the menu**. A new page in the menu tree should’ve been created.
- Move the cursor to the new page called **IRC.**
- Press **F2 Edit** to configure this module page.
    - Allow go to this page ..... should be set to **YES.**
    - Key required ..... **The key required for internet access.**
    - Select module window, you should chose the **IRC Client Module.**
    - Display header ..... should be set to **YES.**
    - Command String ..... Leave it blank.
    - Save the resulting page.
- That’s it!

Configure the TCPIRC.MSG message file

Level 3 - Security and Accounting configuration

- From the main configuration menu (CNF), select **F3 - Accounting and Security**
- Press on **F8 - Search**, type **TCPIRC.MSG**
- The first item you should find is the **DCCKEY** parameter.
- Edit each item as described below, moving from item to item using the arrow keys.
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu.

IRCNKEY **Key to prevent IRC usage.**
NOIRC If a user has this key, they will NOT be allowed to enter IRC.

DCCKEY **Key needed to accept DCC file transfer.**
PAYING Direct Client-to-Client file transfer is the means by which one of your users can receive files over the IRC network. A problem with DCC transfers is that they can tie up bandwidth very rapidly in the same fashion FTP transfers do. You may want to limit access to DCC file transfers if your bandwidth is limited, hence the **DCCKEY**.

CHTKEY **Key needed to accept DCC chat request.**
PAYING Direct Client-to-Client chat lets your users converse with other people on IRC using a secure line of communication, bypassing the servers that are prone to net-splits and lag. Contrary to DCC file transfers, DCC chatting uses about the same bandwidth as normal IRC conversations. If you provide some sort of DEMO access where people have limited access to Internet features, you may want to use the **CHTKEY** to restrict the DCC features, in addition to the DCCKEY.

[Vircom Inc’s MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

ADTKEY **Key needed to see 'adult' channels**
18OLD This key lets you filter channels that have adult topics in them. What we mean by “filtering” is that, if you try to obtain a list of channels, those with adult topics will not be displayed unless the person has the ADTKEY. **This key doesn’t prevent someone to join an adult channel. It only restricts the display of adult channels in the channel list.** The words MajorTCP/IP looks for that make a topic “adult” are defined in the next configuration section. **The parameters from ADTWD1 to ADTWD20 contain those words.**

JOINKY **Key needed to join channels.**
PAYING Users that have this key will be able to join other channels. Users that do NOT have this key will be forced to stay in the default channel.

IRCRATE **Credits/minute when using IRC.**
0 Here you enter the number of credits that will be used per minute as a surcharge when a user is in IRC.

SURKEY **Key to be surcharged even when exempt.**
<Empty> If a monthly, credit-exempt, user owns the following key, IRC will apply the appropriate surcharge for the connection manually. Leave blank to disable this feature. Note that IRC will never surcharge anyone with the master key.

NSURKEY **Key that will exempt from any surcharges.**
<Empty> You can also define a key that will exempt the user from any surcharges due to usage of IRC.

QUOTEKEY **Key required to use /QUOTE.**
<Empty> The /QUOTE command allows users to send command strings directly to the remote IRC server. This is usefull when an IRC server uses non-standard commands (for LIST, for example). You may not want to let all users use /QUOTE so that they don't flood the server with quoted commands.

Level 4 - System options configuration

- From the main configuration menu (CNF), select **F4 - Configuration options**
- Press on **F8 - Search**, type **TCPIRC.MSG**
- The first item you should find is the **IRCDEB** parameter.
- Edit each item as described below, moving from item to item using the arrow keys.
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu.

IRCDEB **Enable debugging options?**
NO This option enables full debugging. All IRC processes get listed in the audit trail for analysis by our Technical Support staff. **To turn on debugging, change this option to YES**. Note that IRC with full debugging on will slow down your system slightly if the IRC client is used frequently.

IRCDB2 **Enable debugging of server messages?**
NO This option enables server debugging mode. This lets you see messages sent by the server you are connected to. This option exists to assist the Technical Support staff at Vircom in the analysis of any IRC problem that might surface.

DEFCHN **Default IRC Channel.**

#worldgroup This is the default IRC channel to use. Most IRC clients on the market usually dump you basically nowhere, waiting for the user to type in a command to join a channel. MajorTCP/IP's IRC client lets you select a default channel for your users. This is specially appreciated by IRC neophytes, as these aren't just staring at a prompt wondering where they are. From the start, they find themselves in a channel with other people (hopefully) which could lend your user a hand. By default, the channel we suggest is #worldgroup. You could set this channel to other popular new-user channels like #irchelp (Efnet) or #wasteland (Undernet). Chances are though that users on these channels will not be familiar with this particular IRC client.

IRCINPL **Number of characters allowed in input.**

255 This option lets you choose the maximum number of characters allowed on a line of input. It is recommended to leave it at the default of 255.

CARABT **Use caret to abort input line.**

NO The Galacticomm teleconference uses the caret ("^") to abort a line of input. IRC allows the caret as part of a nickname. As a result, if you enable this option, users may not be able to get certain information about users with a caret as the last character of their nickname. If you want the IRC to work more like the teleconference, you could set this to **YES.**.

DEFMIN **Default minimum # of users to list.**

5 When users type LIST or QLIST to get a list of channels, only channels with at least a certain number of users will be listed. DEFMIN contains the default setting for this. The reason we need to force a limitation on the list is simple: there are thousands of channels, most of which have one or two people in them. Often, these people turn out to be bots that were put there to keep the channel open. Out of a list of say, 1000 channels, perhaps less than 20% of them have more than 3 people, never mind 5. Another reason we want to restrict the number of channels is thus: some servers will disconnect a user that tries to get a full channel list because this ties up too much bandwidth. Better to keep this setting as is. The bare minimum we suggest though is 3. Anything lower than that is a waste of time and bandwidth.

LSTMIN **Minimum # of users in channel to save desc.**

5 Many IRC servers have thousands of channels. This IRC Client will save as much of this list as it can for the default server. In order to save as many channels names as possible, it will not save the descriptions of small channels. Here you get to choose the minimum number of users that must be in a channel in order to save the description of the channel. 5 is usually a good number if you have many channels. If there are 500 or less channels, you can lower it to 2 or 3.

TOTLST **Maximum number of channels to save.**

2000 The TOTLST option lets you choose the maximum number of channels that the IRC will store in memory for the default server. NOTE: If you set this option to a number LOWER than the actual number of channels on the default server, some channels will not appear in the list. A good ballpark figure to shoot for is this: on the Efnet, you can have as many as 5000 channels. On the undernet, 1000. Of these, depending on your settings for **DEFMIN.** You'll need to keep only 25% to

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

33% of the total number of channels of a given IRC network. 2000 is a good default value to put in: Overkill for the Undernet, and just about right for the Efnet. Feel free to change this value, although a smaller value may result in some channels not being listed.

DSCMAX **Max. number of channels w/description.**
300 The DSCMAX option lets you choose the maximum number of channel descriptions that the IRC client will store in memory. Up to DSCMAX channels will appear in lists complete with a description. The rest will appear, but will have no description listed. Many IRC channels do not have a description anyways.

LSFREQ **Seconds between list updates.**
1200 This IRC Client will automatically log on to the default server at a pre-set interval and get a new list of all available channels. This will include channels that were added since the list was last updated. This option lets you choose how often (in seconds) to get a new list. **600 to 1800 seconds is recommended**.

ONEDEF **Have only default list server?**
NO The IRC Client will connect to IRC Servers occasionally to get a list of channels. It can either connect only to the first server listed, or it can alternately connect with all of the servers listed as Group #1. Setting this to "NO" may help prevent your main server from banning you, from connecting to it too often.

DNSCLR **Seconds between clearing DNS.**
600 The IRC Client automatically remembers the IP addresses of the various servers. This can save a bit of time when a user connects to a server. However, some server domain names can point to various servers, depending on their load. If you set this to 0, it will only check with the DNS resolver once a day. Any higher value will force the client to check the with the DNS resolver if that many seconds have elapsed since it last checked.

FCHUNK **Number of channels to refresh each pass.**
10 This IRC Client will automatically refresh the list of channels. If there are any users on the default IRC server, the IRC Client will check to see if channels have changed (a new topic, or new number of users). This option lets you determine how many channels to update each time. If the number is too high, users may experience unnecessary delays. If the number is too low, it will be longer before channel information is updated. It is recommended to set this option to 10.

DCCFRE **How many megabytes must be free for DCC file transfers?**
2 This option lets you determine the minimum amount of disk space that must be available in order for DCC file transfers to continue. If the free disk space falls less than this amount, the transfer will be aborted.

DCCMAX **Maximum length in Kilobytes a DCC file can be.**
1000 This option lets you determine the maximum length that a DCC file can be.

ULBASE **Port to start DCC Connections at.**
6000 DCC SEND requires a separate port be used for eachsimultaneous connection. This means that a block of 256 ports needs to be set aside for IRC. You should enter the starting port here. It is recommended that you keep this at 6000.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

MOTDDSP **Display MOTD upon connecting to server.**
YES IRC servers usually have a small information text called the "message of the day" (MOTD) that can be displayed upon connecting to the server and by using the MOTD command once logged in. Do you want the MOTD to be displayed when you (and your users) connect to the server?

SERVnn **Name of Server.**
<see CNF> This option and the ones following it let you choose up to 20 different servers that can be used. They can be grouped together, if you like; for example, you can have EFNet servers in one group and UnderNet servers as a separate group. Group 1 is the default. Options go from SERV01 to SERV20. You would normally enter here the domain name of the particular server. For instance, irc.colorado.edu would be a valid server name (although it's not certain at this point if this particular server exists).

You can, alternatively, put in a string of this format: **#ShortName/IP:port**

Example: **#QuarterDeck/122.122.122.1:6663**

This new format lets you assign a "nickname" for a given IRC server. The IP address for a given server can be derived using the /DNS command by feeding it the domain name, you should obtain the corresponding IP address to put here. Finally, the port number was added to allow connections to other ports aside from the "default" port of 6667 that most (but not all) IRC servers use.

GRPNnn **Group Number for Server.**
<see CNF> This option lets you choose a Group Number for this server. Users can select a Group by number, so that you can have options for several different Nets. You should make sure that all servers with the same Group number are all on the same Net. Group 1 is the default (the Net users will go to if they hit Enter), and is the "Best" as it will buffer the list of channels.

ADTWDn **'Adult' word #n. (n=1 to 20)**
<Empty> The next 20 options let you choose words that are considered 'adult'. If these words are found in a channel name or topic, it will only list them to users with the key listed in **ADTKEY**. **Note that these words will only act as a filter for the list of channels. Someone can still access an adult channel even though it isn't displayed in the list.**

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

IRC Instructions

MajorTCP/IP's implementation of IRC is different from the other IRC clients you may have experience with. Contrary to most other IRC clients, MajorTCP/IP IRC was designed to mimic to a certain extent the Teleconference system of MajorBBS/Worldgroup instead of using the Unix command set available under IRCII (the main client available under unix). The reason we designed it this way is simple: ease of learning. It's easier for MajorBBS/Worldgroup Teleconference users to migrate to our implementation of IRC than it would be if we supported the IRCII command set.

The first-time IRC session:

When the user goes to the IRC module for the first time, he or she can set certain initial parameters to taste. These parameters are: the **user's nickname**, **default channel**, **user information and the IRC server or group to use by default**. Hitting X at any of these options will let the user leave the IRC module.

Default Nickname

```
IRC Information Editor
------------------------------

(Hit ENTER to keep any setting the same)

Enter your nickname, or Enter for '': ?

A nickname is used in IRC to identify yourself.  It can be up to 9
letters long, with no spaces.

Enter your nickname, or Enter for '': JohnDoe
```

The user JohnDoe pressed the '?' key first to find out what's expected of him. He must supply his nickname, which must be no longer than 9 characters. Once he's typed this information, it will be remembered for any subsequent IRC session. He can change this information later on if he so desires.

Default Channel

```
Enter channel to start at, or ENTER for '#Worldgroup': ?

When the IRC client connects stats, it will automatically place you in
a channel.  You can choose what channel to start in by changing this
option.  You may want to set this to #Worldgroup.

Enter channel to start at, or ENTER for '#Worldgroup': #FunTalk
```

The Default Channel is the channel the user wants to wind up in automatically when he enters the IRC client module. The channel name must start with a pound '#' sign. The person might want to use the one supplied by default (#worldgroup) by simply hitting enter. This way, later on, he can do a channel list and find out which channels would suit him better. This information can be changed later on.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Default user information

```
Enter your User Info, or ENTER for  'No Information supplied by user '
: ?

IRC users can use a command called USERINFO to get more information on a
user.  By changing this option, you can change what other IRC users will
see.

Enter your User Info, or ENTER for  'No Information supplied by user '
: Will program for Food
```

The Default user info is used to tell other users on IRC a little bit about you. When a person on IRC uses the USERINFO command (or with the IRC Client, you do a CTCP ON, then use the USERINFO <nick> command), this is the information people will see. In the case of JohnDoe, the userinfo line will show that he "Will program for food". This information is conserved for any subsequent IRC session, but can be modified later on.

Default IRC Server or group of servers

```
Enter starting group number, server or ENTER for 1: ?

When you enter IRC, if you hit ENTER you will automatically get
connected to an IRC server.  If you don't know of a specific Net
or server you want to connect to, enter "1" here (no quotes).

Or, you can enter to connect to Undernet IRC servers, or 3 to
connect to DALnet.

Or, you can enter the name of a specific server you want to
connect to every time.

Enter starting group number, server, or Enter for 1: 2
```

Here, the client selects which group he'll use. You should provide the user (ie: either modifying this text block or on some sort of instruction sheet) the servers you put in each group. It's suggested also that you put all Efnet servers into group 1, all undernet servers under group 2 and all DALnet servers in group 3. That way, a person can select via the group number which net to connect to. The person can also type in his or her
favorite server as default instead of the BBS defaults. All this information can be changed at any time by the user.

Once the user has entered all his login info for the first time, he will get the standard IRC screen on subsequent sessions ...

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Standard Sessions

Worldgroup IRC Client
(c) Copyright 1995 Computerized Horizons

When connected:
Type LIST to see all channels available.
Type JOIN <channel> to join a channel.
Anything you type from then on is seen by everybody in that channel.
Type ? or HELP to get more information.

Enter “E” to edit your info, ENTER for quick logon, or server name/group: ?

Hitting ENTER will automatically log you onto IRC.
Entering a number will connect you to a specific group or IRC servers.
Entering a server name will connect you to that server.
Or type “E” to edit your IRC information.

The programmed group of servers are:

ServerName	Group#
irc.cerf.net	1
irc.frontiernet.net	1
irc.bridge.net	1
irc.voicenet.com	1
irc.neosoft.com	1
irc.epix.net	1
irc.ecn.uoknor.edu	1
irc.mo.net	1
irc.law.emory.edu	1
irc.stealth.edu	1
chicago.il.us.undernet.org	2
joplin.mo.us.undernet.org	2
manhattan.ks.us.undernet.org	2
montreal.qu.ca.undernet.org	2
vancouver.bc.ca.undernet.org	2
igc.fl.us.dal.net	3
services.dal.net	3
groucho.ca.us.dal.net	3
dragon.ut.us.dal.net	3
uncc.nc.us.dal.net	3

If the user presses “E”, he will see the same questions as the first-time IRC session. That is, he or she will be asked for a nickname, a default channel, default user info and the default server or server grouping.

The user can press <RETURN> to use the default settings he put in his first IRC session. IRC will try to connect the user automatically to the first server in the selected server group. If it fails, it tries the second one, the third one ... so on and so forth. You can have up to 20 default servers.

Finally, if the user insists, he or she can type in a server name. We have an up to date list of IRC servers in the annex of this manual. Feel free to extract it and distribute it to your users.

Attempting to connect to IRC Server .....

Connected to IRC!

Signing on.....

You are in the #Worldgroup IRC channel
Channel Topic: MajorBBS and Worldgroup are Hip!
*** #Worldgroup Someguy 123456789
Steve, Todd, Jeff, **Lila,** are here with you.

If the server you are trying to connect to is not suffering from excess loading, John Doe shouldn't have to wait too long for the connection to be established. Should the connection time-out or be refused (the server is full), MajorTCP/IP will try the second server in the server grouping, then the third, the fourth, the fifth ... so on and so forth..

What each line means:
You are in the #Worldgroup IRC channel.....The name of the channel the user is in.
Channel Topic: MajorBBS and Worldgroup are Hip!..The current topic in this channel
*** #Worldgroup Someguy 123456789.....The person who last changed the topic
Steve, Todd, Jeff, **Lila,** are here with you. .....Who are in the channel. **Lila** is ChanOp.

Note that with a color screen, Lila would be deep red, the rest of the channel denizens would have their names written in white.

What can the user do from here?
Anything the person types that isn't an IRC command will be transmitted to all those on the channel. The commands the person can use in the channel are listed in the following tables.
Basic commands are the minimal commands most users should know to enjoy IRC. Advanced and operator commands are useful but not fundamental to the enjoyment of IRC.

Basic Commands	Description
Anything typed normally	Is transmitted to everyone. This is what you're saying on the channel.
MAIN /M	This returns the user to the default IRC channel define in DEFCHN, level 4 configuration in the TCPIRC file.
JOIN <channel> JOIN #<channel> /J <channel>	The join command lets the user join any channel on the IRC. The user can use the command in those three forms. Example, say the user wants to join the #Worldgroup channel. He can use: JOIN #Worldgroup JOIN Worldgroup /J Worldgroup

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

More Basic Commands	Description
LISTNUM <number>	Tells MajorTCP/IP To list channels with the <number> of users or more currently on them. This lets you limit the size of the list you generate. This command is used before you use the LIST or QLIST commands..
LIST LIST <char>	Lists all the channels on the IRC Network with description. Can be used with LISTNUM to reduce the size of the list generated. LIST can be used on the default server and another server as well. If using the command **on the default server**, you can also list the channels that start with the letter defined in <char>. Ex: **LIST A** will list all the channels that start with the letter A.
QLIST QLIST <char>	List all the channels on the IRC Network in compressed form (five channels per line) This command can only be used on the default server. You can also use the QLIST <char> command to list only the channels that start with the letter specified by <char>. Ex: **QLIST C** will list all the channels starting with the letter C.
WHOIS <user> /W <user>	This gives you some information about a user. WHOIS Joe would give: **Nickname: Joe Realname: Joe-Bob** **E-mail Address: JoeBob@somewhere.com** **Joe is on: #Widgets** **Joe is using server washington.dc.us.undernet.org (Undernet Server for the Greater Washington area)** **Joe has been idle 27 seconds.**
WHOIS <Channel> /W <Channel>	Lists the users on a given channel. WHOIS #Widgets would give: **Joe, Jeff, Tim, Richard are here with you.**
WHISPER TO <usr> <text> /<user> <text> // <text>	Sends a private line of <text> to the user <usr> WHISPER To Joe Hiya Joe, howzit going /Joe Howzit going. // Did you hear me? <- Sent to the last whispered person.
ACTION <action> /A <action>	Lets the user perform an action. Lets assume Joe is the one acting ACTION is sleepy ..... Would appear as **Joe is sleepy.** /A is tired ..... Would appear as **Joe is tired.**
FORGET <user>	If a user is bothering you, you can ignore any of his text by type FORGET <user>. Example: FORGET Steven Anything Steven typed would not be visible for you.
REMEMBER <user>	If the person has become reasonable again, you can use the REMEMBER <user> command. Example: REMEMBER Steven. Anything Steven types now will be visible again.
NICK <nickname>	If you want to change your nickname while you're on a channel, simply type in NICK <newnickname>. Example: Joe wants to be known as JoeBob. **NICK JoeBob** is the command to use.
QUIT X	QUIT to leave IRC. X does the same thing, but should be used as the last resort.
HELP LIST	Gives you detailed instructions about LISTNUM, LIST and QLIST
HELP ADVANCED	Gives you a summary list of the advanced commands.
HELP OPERATOR	Gives you a summary list of the operator commands.

Advanced Commands	Description
AWAY <info>	This marks you as being away from your keyboard. You can say why in the info section. Example: AWAY I'm gone to get coffee. Someone who tries to whisper to you or does a whois on you will see the notice. Typing something at the keyboard when you come back automatically unmarks you.
DCC	If somebody tries to send you a file via DCC file transfers, You'll see a notice on your screen saying "Type DCC to receive <file> from <user> of length <bytes> long". If you type DCC, the transmission will begin. You can continue to use IRC normally, although you shouldn't try to receive a second DCC while one is initiated. Once the file is received, you can use one of the normal file transfer protocols to receive the file on your computer.
UPLOAD <filename>	Upload a file to send via DCC. Before doing a DCCSEND, you first need to upload the file from your home computer to the BBS. Once the file is uploaded, you can then do a DCCSEND <nickname of user> to send the file off to the desired person over IRC. Ex: **UPLOAD SOMEFILE.TXT**
DCCSEND <nick>	Send the file you uploaded to <nick>. This command lets you send the file that you uploaded to the BBS via the UPLOAD <filename> command. Ex: **DCCSEND Someguy**
DCCCANCEL	Cancel the DCC send. This command lets you cancel a DCCSEND in mid-transmition.
DCCCHAT	If somebody wants to go into DCC chat with you, you type in DCCCHAT to initiate the connection. From this point, type /DCC <message> will transmit the text after the /DCC command directly to the other person privately. This bypasses normal IRC Servers. In a sense, you are connected directly to the other person's Client.
/DCC <message>	Once a DCCCHAT is initiated, this is the command to use to send text over the DCC session. /DCC Hiya, how are ya. The person on the other end will see the "Hiya, How are ya".
MYINFO <info>	You can associate a line of information to your name if someone wants to find out about something about you. **MYINFO I'm a mean guitar player** will put the "I'm a mean guitar player" caption in your USERINFO description.
CTCP ON/OFF	CTCP (Client-To-Client Protocol) is turned on or off. **You need to do a CTCP ON to be able to use the next command**. These commands let you find out information about the Client program the target user is running, the time in his location and tons of other things.
FINGER <user> *Needs CTCP ON*.	Finger lets you find out some basic information about the person specified in <user>, including the time the user has been sitting idle Example: **FINGER Rick** would return ... **Finger info (Rick): Real Name: Rick Blatt Idle: 10 seconds**.
USERINFO <user> *Needs CTCP ON*.	Userinfo returns the text a person entered using the MYINFO command. For instance, if someone did USERINFO on the person in the previous MYINFO example, he would see: **User Info (JoeBob): I'm a mean guitar player.**
PING <user> *Needs CTCP ON.*	Ping lets you find out the time it takes for information to make a round trip between you and the person specified in <user>. For instance, say you **PING JoeBob**, it could return something like: **Ping Info (JoeBob): Delay: 27 seconds.**

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

More advanced commands	Description
TIME <user> *Needs CTCP ON.*	Time lets you find out what time it is in the person's time zone. Say, you do **TIME JoeBob**, the information returned looks like: **Time Info (JoeBob): 10:27:00 12/01/95**
VERSION <user>	Lets you find out what Software and it's version number the <user> is running to connect to the IRC. **VERSION JoeBob** could yield: **Version Info (JoeBob): MajorTCP/IP IRC Client:.98 MBBS/WG**
CLIENTINFO <user> *Needs CTCP ON.*	Lets you find out what CTCP commands the specified person's software can handle. **CLIENTINFO JoeBob** could yield: **Client Info (JoeBob): I know: ACTION FINGER VERSION SOURCE USERINFO CLIENTINFO PING TIME ERRMSG**
SOURCE <user> *Needs CTCP ON.*	Lets you find out where you can get the user's IRC Client. For instance: **SOURCE JoeBob** would yield in his case: **Souce Info (JoeBob): gm.gamemaster.qc.ca**
MOTD	Ask server to display MOTD file again. MOTD means (M)essage (O)f (T)he (D)ay. It's basically a logon banner all IRC servers have.
/QUOTE <command>	Send command to server, directly. Documenting all the possible commands with the /QUOTE command is outside the scope of this manual. Basically, if you type **/QUOTE HELP**, you'll see all the commands you'll be able to use on the IRC server you are connected to. Please be advised that this command is very dangerous as it gives you some measure of control over the IRC server you are connected to. Any abuse of the IRC server could get you K-Lined from that server.
Operator commands	Description
INVITE <user>	Someone who has ChanOps can invite a user to the channel. This is especially important if the channel was set invite-only using the MODE command. **INVITE JoeBob** would tell him that he's invited to your channel.
UNINVITE <user>	Just in case you change your mind on the invitation, you can uninvite someone before the person gets to your invite-only channel. **UNINVITE JoeBob** would tell him that he can longer access your channel.
TOPIC <Description>	If you have ChanOps, you can change the Topic of the channel. Typing **TOPIC We're here to stay** would change the channel topic to "We're here to stay".
MODE <parameters>	MODE is the lifeblood of the ChanOp. See the special section below.

MODE List, with detailed description

Banning a user or system from the channel.

MODE <channel> +b|-b <nick>!<user>@<hostname>

This commands lets you ban (+b) or unban (-b) someone from your channel. You can use the wildcard character (the asterisk *) to make it a more general ban. For instance. Say you are Channel operator on the #Widgets Channel.

MODE #Widgets +b JoeBob!Joe@somewhere.com
would ban the user JoeBob connecting from somewhere.com from your channel. To find out where a person is connected from, simply do a WHOIS on that person. The person's E-mail address is a good indicator of where the person is connecting from.

MODE #Widgets +b *!*@somewhere.com
Would prevent everybody that calls from somewhere.com to go into the #Widgets channel. This is what is called a site-ban.

MODE #Widgets -b *!GLeepard@nowhere.com
This command would be used to Unban a user that was previously banned from your channel. Since Gleepard uses many different nicks, we want to make sure that it's the Gleepard person that we Unban.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Restricting the channel to Invitation only mode

MODE <channel> +i|-i

MODE #Widgets +i
Set the channel to invite-only mode. When a channel is invite-only, you have to use the **INVITE <user>** command described earlier to give permission to the user to access the channel. If user wasn't invited, he won't be able to get it.

MODE #Widgets -i
Removes the invite-only restriction on the channel.

Restricting the number of users that can connect to your channel

MODE <channel> +l <num> OR MODE <channel> -l

MODE #Widgets +l 10
Restricts the users who can use your channel to 10 people or less.

MODE #Widgets -l
Removes all user restrictions.

Making the channel moderated.

MODE <channel> +m | -m

MODE #Widgets +m
This makes the channel moderated, only channel operators can talk.

MODE #Widgets -m
Removes the moderation letting everyone talk on the channel.

Restricting messages from the outside

MODE <channel> +n | -n

MODE #Widgets +n
Makes it impossible for someone outside of the channel to whisper to users currently on the channel. This command is often used to prevent interruption in a private discussion.

MODE #Widgets -n
Remove the whisper restriction.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Give a user ChanOps priviledges

MODE <nick> +o | -o

MODE JoeBob +o
This command gives JoeBob ChanOps powers.

MODE JoeBob -o
And now, we remove them.

Make a channel Private

MODE <channel> +p | -p

MODE #Widgets +p
Using this command, we can make the #widgets channel private. Only people that have been invited can make it in.

MODE #Widgets -p
Remove the privacy flag on the channel.

MAKE a CHANNEL secret and invisible.

MODE <channel> +s | -s

MODE #Widgets +s
This command makes the #Widgets channel secret. Such channels are invisible when one lists the channels using the LIST command.

MODE #Widgets -s
Makes the channel normal again.

Prevent ordinary users from changing the channel's topic.

MODE <channel> +t | -t

MODE #Widgets +t
This command prevents non-ChanOps from changing the channel topic.

MODE #Widgets -t
This command makes it possible for everyone to change the Channel topic.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Make yourself invisible from anybody that doesn't know the exact spelling of your nick.

MODE <nick> +i | -i

MODE JoeBob +I
Makes JoeBob invisible when someone does a WHOIS on him or on the channel.

MODE JoeBob -i
Makes JoeBob visible again.

Trick - Fooling a reticent IRC server

MajorTCP/IP's IRC client connects invisibly to the first IRC server you specify in the server list to maintain a list of channels internally. This has the benefit of saving bandwidth on the IRC server side. Why? Everytime a user does a /list command, this generates a large amount of disk I/O and consumes alot of bandwidth as well on the server side. The problem is compounded when you have more than one user doing this.

Because MajorTCP/IP maintains a list internally, the impact of multiple /list requests is thus minimized. However, this is accomplished by having the IRC client operate as a "bot". Many systems frown on bots and therefore, might K-line you from their server.

You can do two things in this case:

a) talk to the admininstrator of that particular server and explain to him what MajorTCP/IP's IRC client does, and how it saves him precious resources.

b) leave the first entry in your IRC server list blank. This way, MajorTCP/IP will not use its "bot" to maintain the internal list.

STEP #14:

Configure the POP3 Server module

Last version January 20th 1997.

- **Added experimental option POP3PHDR**. When enabled, POP3 will try to preserve the internet e-mail headers of an incoming message (if SMTPHEAD is set to 9 in TCPSMTP.MSG, level 4 configuration) so that users getting their e-mail with a POP3 client can have access to the full headers properly.
- Added new configuration option **POP3OBSZ** in CNF level 4, configuration options. Similar parameters were added to other modules and their effect are discussed in the **Performance Optimization chapter in the annex**.
- Added **CNF level** 4 option **POP3MXMG**

Overview

POP3 or Post Office Protocol (some prefer Portal of Power) lets your users check their MajorBBS/Worldgroup mailbox remotely over the internet, either by being connected to your system directly over SLIP/CSLIP/PPP or from a remote SLIP/CSLIP/PPP connection anywhere else over the net. You can restrict access to the POP3 module to people who are logged-in locally if you so wish.

One note: POP3 is only useful for people who want to use TCP/IP clients that act as mail-readers like Eudora, Pegasus Mail or the Netscape 2.0 facilities. Furthermore, POP3 works in conjunction with SMTP, so you need to configure a pair of parameters in MajorTCP/IP's SMTP server configuration options. POP3 is principally used to fetch old or new mail sitting in the user's mail box while SMTP is used to forward any outgoing mail traffic unto the internet.

MajorTCP/IP's implementation of POP3 includes MIME support. The current version of POP3 does not support APOP.

***IMPORTANT NOTE* For POP3 to function properly, both the Rlogin and SMTP modules must be installed and functionning. POP3 is dependant on Rlogin for proper aliasing, while SMTP is used for any outgoing mail traffic.**

The POP3 server's effect on TCP Handles

Each person that uses POP3 over SLIP/CSLIP/PPP uses up one TCP Handle. The maximum number of such connections at any given time is defined in the POP3MAX variable, mentioned later on in this section of the manual. For more details about TCP Handles, check out NBTCP in the Manual.

Installation procedure for the POP3 module

POP3 is very easy to configure. For one thing, this is one of the few modules that **doesn't** need to be in the menu tree. You need to configure it's parameters and two parameters in the SMTP module. **POP3 can only function in conjunction with SMTP, so you need to have SMTP Enabled and functioning.**

Step by Step installation procedure for the TCPPOP3 module

STEP	Description	Done
#1	Configure the TCPPOP3.MSG file	
#2	Configure the TCPSMTP.MSG file	

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Configure the TCPPOP3.MSG message file

Level 3 - Security and Accounting configuration

- From the main configuration menu (CNF), select **F3 - Accounting and Security**
- Press on **F8 - Search**, type **TCPPOP3.MSG**
- The first item you should find is the **POP3KEY** parameter.
- Edit each item as described below, moving from item to item using the arrow keys.
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu.

POP3KEY **Key required to use POP3**
NORMAL Your users will need to have this key in order to be allowed to connect to the POP3 server.

POP3TCHG **Per minute credit rate while in POP3**
0 This allow you to charge for POP3 connect time. You enter an amount that is a per-minute credit rate. This is charged at the end of the POP3 session only. A negative amount will give credits to the user.

POP3MCHG **Per message credit rate**
0 This allow you to set a charge for each message retrieved by POP3. This charge will be charged every time a message is retrieved. A negative amount will give credits to the user.

POP3KCHG **Per Kilo-Character credit charge**
0 This charge will be accrued for each 1024 characters sent to the user. Only characters sent that are part of the messages (not traffic generated by the POP3 protocol itself) will be counted. A negative amount will give credits to the user.

Level 4 - System options configuration

- From the main configuration menu (CNF), select **F4 - Configuration options**
- Press on **F8 - Search**, type **TCPPPOP3.MSG**
- The first item you should find is the **POP3ENAB** parameter.
- Edit each item as described below, moving from item to item using the arrow keys.
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu.

POP3ENAB **Enable POP3 on your BBS.**
YES Set this option to YES to activate the POP3 Server. Leaving POP3ENAB to NO will hide all of the following options.

POP3MAX **Number of POP3 users at one time.**
5 This is the maximum number of connections your POP3 server will accept at any given time. Each connection uses one TCP Handle. (Check out NBTCP in the manual) In addition, each POP3 user you define in POP3MAX will reserve 16.5K of extended memory. **This option is visible only if PO3ENAB is set to YES.**

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

POP3LAC **Restrict to Local Callers.**
NO Set POP3LAC to **YES** if you want to restrict mail box access to people calling directly over your local network -- in other words, people who are connected via SLIP/CSLIP/PPP directly to your BBS. For this to work however, you must make sure that the **NETMASK** (See Hardware Configuration Options, level 1 configuration) is set properly as your internet provider has specified. The NETMASK is used to determine how one differentiates a local caller .vs. someone who's elsewhere on the internet. **This option is visible only if POP3ENAB is set to YES**.

POP3NEWO **Restrict to NEW E-mails only.**
YES You can tell the POP3 server to only act upon new E-mail instead of all the person's mail by setting the option to YES. Setting it to NO means that ALL the E-mail in the user's mailbox will be accessible. **This option is visible only if PO3ENAB is set to YES.**

POP3DEL **Restrict message deletion.**
NO Usually, a user can use the POP3 DELETE command to delete messages from his or her mailbox. You may want to prevent POP3 from doing this for testing or security purposes. **Set it to YES to initiate restriction conditions**. **This option is visible only if PO3ENAB is set to YES.**

POP3OBSZ **POP3 Output buffer size.**
2048 This sets the size of the output buffer for POP3 sockets. The larger, the better the performance of the POP3 server. However, this also increase the amount of memory taken for each POP3 socket. **Check out the Performance Optimization section in the annex for further details.**

POP3TMOT **Time-out for POP3 connections (in minutes).**
10 Connected POP3 sessions consume some of your BBS resources. This option lets you define for how long a connection will be allowed to remain idle. The POP3 standard requires an inactivity time-out delay of at least 10 minutes. **This option is visible only if PO3ENAB is set to YES.**

POP3MXBU **Maximum time to spend building drop file (seconds**).
0 After a POP3 user is accepted (password is ok), the POP3 server builds a "mail drop file", that will be referenced by POP3 later on during the session. Building that file takes time, and some POP3 clients may timeout during that period of time. Setting POP3MXBU to a non-zero value will force POP3 to stop building that file after n seconds. Messages that were excluded because of that will be included in the next POP3 call. **This option is visible only if PO3ENAB is set to YES.**

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

POP3PATH **Work directory for POP3.**
.\tcppop3.dir This directory will be used for POP3's work file. Type in the path and directory name you want POP3 to use for that directory. **Do NOT put a trailing '\'**. **This option is visible only if PO3ENAB is set to YES.**

POP3DLOW **Free Disk space required for POP3 to function (MB).**
5 POP3 will not accept connections if there is less than DLOW Megabytes of disk space remaining on your default drive. Set to 0 to disable any free disk space checking. **This is not recommended**. **This option is visible only if PO3ENAB is set to YES.**

POP3SLOW **POP3 Tasker Slowdown.**
10 POP3 normally use only "spare" processing cycles to service users. You may want to tell POP3 to skip some cycles if it still slows your BBS down too much. The number entered here is the number of spare cycles that will be skipped. **This option is visible only if PO3ENAB is set to YES.**

POP3LOG **Record POP3 information's in log**
YES Set this option to YES to record debugging information about POP 3 in the standard MajorTCP/IP log. **The MajorTCP/IP log is defined in TCPLIBM.MSG**. By default, the file name is TCPLOGF.LOG. **This option is visible only if PO3ENAB is set to YES.**

DBUGLVL **Debugging Level (for LOG file)**
4 This selects the level of debugging information that will be recorded in the log file. 0 Disables the log, 9 turns on full debugging. Full debugging might slow down the BBS somewhat. Note that level 9 debugging will also record the passwords that have been tried in the TCPLOGF.LOG file, so be sure this file is kept secure. **This option is visible only if PO3ENAB is set to YES.**

POP3MXMG **Maximum messages per session.**
30 This is the maximum number of messages that will be retrieved per POP3 session. We reccomend that you leave this to the default value of 30. **This option is visible only if PO3ENAB is set to YES.**

POP3PHDR **Try to preserve Internet Email Headers.**
NO If POP3HDR is set to YES, then POP3 will try to preserve headers from incoming internet e-mail so that they are sent complete to the POP3 mail reader. **Note that for this function to work, SMTPHEAD must be set to 9 in TCPSMTP.MSG, level 4 configuration options. This option is visible only if PO3ENAB is set to YES.**

Configure the TCPSMTP.MSG message file

Because most newsreaders require an SMTP smarthost to be able to send messages back out on the internet, we've implemented a mail routing scheme that enables MajorTCP/IP's SMTP server to route mail not addressed directly to the system. That combined with the POP3LAC parameter will let you control who uses your SMTP server and who doesn't.

A few issues have to be dealt with though. For SMTP routing to work, you have to tell SMTP how to distinguish a message that is addressed to the BBS from a message that is destined for the outside world. Say we have our hypothetical BBS named bbs.widgets.com. Associated to this name is the address www.widgets.com. Both addressed in fact point at the same IP address. So E-mail coming in to people at either address should make it on your BBS.

Now here lies the problem. SMTP only knows one thing. The BBS is called bbs.widgets.com.
If it receives a message to a user called JohnDoe@www.widgets.com, SMTP will think that this message is actually destined to someone out on the internet (not to someone on the BBS which is in fact the case). So, SMTP rejects the message.

The bounced mail gets back to the Sendmail Smarthost system run by your provider. It sees that the message was in fact correctly addressed (to it, www.widgets.com points at the same place as bbs.widgets.com), so it bounces back the mail the BBS, which bounces it to the provider's smarthost, which bounces it back to the BBS .... so on and so forth.

As you can see, for SMTP mail routing to work, we have to tell the BBS which other hostnames are used by the BBS. That's what you specify in the SMALnn parameters.

Level 4 - Configuration Options

- From the main configuration menu (CNF), select **4 - Configuration Options**
- Press on **F8 - Search**, type **ENABROUT**
- Edit each item as described below, moving from item to item using the arrow keys.
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu.

ENABROUT **Enable SMTP Routing**

YES — If you enable SMTP routing, SMTP will accept E-mail from other systems that are not intended for the BBS and will attempt to route them out. If you set this to YES, **then you MUST enter the various aliases for your bbs domain name in SMAL01 to SMAL20**. **You must set this to yes if your SLIP/CSLIP/PPP users will use your BBS as a SMTP/POP3 server**. **This option is visible only if SMTPENAB is set to YES.**

SMALnn **System alias number nn (where nn can be from 01 to 20**)

<Empty> — Enter here the hostname/domainname alias SMTP will accept email for and consider it for the BBS. SMTP already accepts email for the HOSTNAME/DOMNAME as defined in tcplibm.msg, level 1 and for the SMTPFROM defined above. Please, make sure you make no typos, as if you make one, SMTP will attempt to send email back out to the internet. **This option is visible only if ENABROUT is set to YES.**

How to configure the POP3 mail readers.

Since there are many different POP3 mail readers out there, it would be hard to cover them all.
In this section, we will deal with two of the most-used POP3 readers: Eudora and Pegasus Mail.
In all cases, your user should know what his internet User-ID looks like. (ie: blanks are converted to dots, unless the person has a separate internet ID using the Rlogin alias page).

Eudora

- Startup Eudora
- Go into the Special pop-down menu
- Select the Settings option.
- Click on the Getting Started icon
- POP account should be the users internet e-mail address on your system ie: JohnDoe@yourbbs.com.
- Real Name should be the user's real name ie: John Doe
- Click on the Personnal info icon
- Return address should be the user's normal internet e-mail address, meaning JohnDoe@yourbbs.com
- Click on the Hosts icon
- SMTP should be your BBS internet address: yourbbs.com
- Finger should be your BBS internet address: yourbbs.com

Pegasus Mail

- Startup Pegasus Mail
- Go into the File menu
- Select the Network configuration option
- Fill in the following parameters ...
- Outgoing SMTP E-mail: Hostname/domain name of your BBS or it's IP address.
- From Field: user's internet E-mail address: JohnDoe@yourbbs.com
- Incoming POP3 Mail address: Hostname/domain name of your BBS or it's IP address.
- Port Number: should always be 110.
- Username: can be the person's internet or BBS user-ID
- Password: person's password on the BBS.

It's hoped that these examples will provide you with the proper basic information that any other kind of POP3 mail reader may require. As you can see, it's pretty simple.

***NOTE* Remember that you need to enable routing in the SMTP module to allow POP3 traffic. This means setting ENABROUT to YES in TCPSMTP.MSG, level 4 configuration options. See the previous page for details.**

STEP #15:

Configure the FTP Server module

Last version January 20th 1997.

- Added new configuration option **OBUFSIZ** in CNF level 4, configuration options. Similar parameters were added to other modules and their effect are discussed in the **Performance Optimization chapter in the annex**.
- Can now delete files from a DOS-Only library if you are lib-op.
- Will now accept an internet alias for secured logins. (in the same way our SLIP/CSLIP/PPP server does).

Overview

The FTP Server allows users on the internet to access your file libraries, in the same fashion you can now go to remote FTP sites using MajorTCP/IP's FTP client. Furthermore, people on the BBS itself can gain access to your FTP site if in SLIP/CSLIP or PPP, using any windows-based FTP client like the built-in FTP support in Netscape, WS_FTP or CuteFTP.

MajorTCP/IP's FTP Server allows several different type of access to your libraries. **Secured FTP access**, **Sysop FTP access** and **Anonymous FTP access**. Furthermore, MajorTCP/IP's FTP server supports **multi-homing**. This means that you could offer corporate clients, depending on the IP address assigned to them, a specific keyed library that only clients of theirs, or anonymous users coming through that particular IP address, will be able to access. This is a feature that makes our FTP server particularly interesting. ***(Consult the Advanced Issues: Multi-Homing section of the manual).***

Finally, MajorTCP/IP's FTP server also supports **special home-page management services**. To take advantage of this feature, you need packages that automatically maintain home-page directories Here is the list of packages that currently support this new feature:

> **High Velocity Software's Web Master, version 1.10C:** They can be reached by E-mail at sales@support.hvs.com or over the WWW at http://www.hvs.com. Their sales phone number is (800) 572-5582. You can also call up their support line at (602) 234-2207.
>
> **Dialsoft's Web Blaster, version 2.7:** They can be reached via E-mail at sysop@jungle.net, or on the WWW at http://www.dialsoft.com. Their sales department can be reached by phone at (800) 888-8026. Their support line is at (201) 586-1550. They also publish a product called Signature Editor that lets your users manage signature for SMTP, NNTP and a PLAN file (like the .plan file on Unix).
>
> **Dynamic's Home Page Manager, version 2.5:** They can be reached via E-mail at tfazio@unix.trilogy.net, or on the WWW at http://www.trilogy.net/mpg. The product can be purchased from Logicom at (800) 764-4226 or WilderLand Software at (414) 273-4580.
>
> **Micro Magic's Web Spinner, version 1.40:** They can be reached via E-mail at keford@magicbbs.com or over the WWW at http://www.magicbbs.com. Their phone number is (205) 971-9711.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

The FTP server's effect on TCP Handles and six-pack licenses

MajorTCP/IP's FTP server uses **one TCP Handle for the connection**, and **another TCP Handle for the actual transfer of data**. So for every FTP session, you can expect a usage of between one and two TCP Handles. This isn't much of a limitation since the base package of MajorTCP/IP allows upwards of 256 TCP connections. You could, if need be, upgrade that to 1024 with the unlimited version of MajorTCP/IP. In terms of **six-pack usage**, our FTP server will use up **one license of a six pack per open connection**. The FTP server is the only module aside from Telnet/RLogin that requires six-pack license for incoming connections. What this means is that, if you wish to allow say, a maximum of 10 simultaneous FTP connections, you can expect the FTP server to use between 10 and 20 TCP Handles and **10 six-pack licenses** (two and a half six-packs) at peak load time.

Please note that the channels used for FTP sessions are **telnet channels**. This means that telnet users and FTP users will share the same available channels you've allocated for incoming telnets. For instance, lets say for the sake of argument, you have 6 telnet channels defined.
You could thus have 3 telnetters and 3 FTP users online simultaneously, or any combination thereof.

The reason **why** we must use six-pack licenses is simple. FTP sessions, like telnet sessions are full login sessions. That is, people are actually logged onto the system. We are obligated, per Galacticomm to use up six-pack licenses under these circumstances. Other forms of incoming traffic like web hits, incoming SMTP or NNTP mail traffic do not constitute full sessions where an actual user is connected to your system. Therefore, it can be argued that the latter do not require use of six-pack licenses. The same cannot be said for FTP sessions.

Installation procedure for the FTP server module

The installation procedure for the FTP server is extremely simple. All you need to do is to configure the various CNF parameters associated to the server and that's it. The FTP server works in the background, listening to port #21. It doesn't need to be in the menu tree. **For the FTP Server's multi-homing capability, you should consult the "Advanced Issues: Multi-Homing" section at the end of this manual.**

Step by Step installation procedure for the FTP Server module

STEP	Description	Done
#1	Configure the TCPFTPD.MSG file	

Configure the TCPFTPD.MSG message file

Level 3 - Security and Accounting configuration

- From the main configuration menu (CNF), select **F3 - Accounting and Security**
- Press on F8 - Search, type TCPFTPD.MSG
- The first item you should find is the **FTPKEY** parameter.
- Edit each item as described below, moving from item to item using the arrow keys.
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu.

FTPKEY **Key req'd for FTP access to your system.**
<Empty> You assign this key to a user of your system to grant him or her access to your FTP site. If the person in question has an account on your system but doesn't own this key, he or she will be rejected. Having access to your FTP site isn't the same as having access to your libraries. The person could conceivably be able to connect to your FTP site but not be able to get any kind of access to your libraries.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

LIBKEY **Extra key req'd for FTP access to Libraries.**
<Empty> This key allows you to create extra restrictions for FTP callers to your file libraries. **Leaving the LIBKEY empty** means that the person will have the same access to your libraries as he/she has to your File Libraries via the MajorBBS/Worldgroup file-library management system.

You might want to assign a key to this option to completely shut off the File Library section of your Worldgroup to certain FTP callers. Or you could use this option if you wanted these users to access only a single special DOS drive under FTP, and none of your File Libraries.

FTPDCHG **Additional credits/minute for secured FTP callers.**
0 This options lets you specify how many extra credits per minute should users be **charged extra** for access to your secured (as opposed to anonymous) FTP services on your MajorBBS/Worldgroup system.

Make this number 0 if you want secured FTP access to be charged at the standard system rate, defined in option **MMUCRR in level 3 configuration, accounting and security in BBSMAJOR.MSG**. You can also assign it a negative value so that secured FTP callers will be charged **LESS** credits while they're on-line than the amount specified in the **MMUCRR** option.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

FTPKCHG **Charge per 1K bytes traffic via secure FTP.**
0 This option specifies the charge, in credits, for each 1K (1024) bytes transferred over FTP control and data connections, in either direction. This is a connection traffic charge and is over and above any File Library imposed charges. Aborted transfers are always included in this charge.

ANON **Allow "anonymous" FTP access.**
NO Many systems on the Internet allow access to public files to users who don't have a UserID and password on the system. Users type "anonymous" instead of a User-ID with their E-mail address in place of a password. **Set this parameter to YES if you would like to provide anonymous access to some of your files in your libraries**. Leaving this option to NO restricts access solely to people with UserID's on your system.

ANONCLS **Class for "anonymous" FTP callers.**
<Empty> This is where you specify the name of the CLASS that grants access to certain libraries to anonymous callers. Basically, you need to create a class that will only contain a keyring of keys that grant access to the various libraries you would like to grant public access to. **This option is visible only if ANON is set to YES**.

DOSVKEY **Key required to view DOS files via FTP.**
SYSOP This option is where you specify which key is required to gain access to some or all of your DOS drives in addition to the MajorBBS/Worldgroup software libraries. This access should be restricted to the BBS staff and yourself.

DOSGKEY **Key required to get DOS files via FTP.**
SYSOP Owning this key allows users to "get" DOS files from your system via FTP. What we mean by "DOS files" is any file that is on your drive or drives. This option is related to the DOSVKEY option. Only you or your staff should be able to download files from your various drives.

DOSPKEY **Key required to put DOS files via FTP.**
SYSOP Owning this key allows users to "put" DOS files fin your system via FTP. What we mean by "DOS files" is any file that is on your drive or drives. This option is related to the DOSVKEY option. Only you or your staff should be able to upload files to your various drives. This key also limits the deletion and the overwriting of files and the creation and destruction of directories.

WEBFKEY **Key required for full access to WEBHOME dirs.**
SYSOP In addition to the /library and /dos hierarchies, FTPD also supports direct access to the webpages directories used by TCPWEB2. If a user has the key defined below, then they will be able to do anything they want in this hierarchy. Normally, only SYSOPS are allowed to do that. The name of that hierarchy is **/webhome**. If **WEBFKEY is left EMPTY, then this feature will be disabled**. Note that this /webhome **directory is not available to users unless you use a third party product like WebMaster or WebBlaster mentioned earlier. They have not yet implemented this new structure. You should stay in touch with our support BBS to find out if/when the implementation will be done by the various ISV's**. The /webhome hierarchy or "pseudo-directory" is accessible to those with the **MASTER key**, even if you are not running a home-page maintenance product.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Level 4 - System options configuration

- From the main configuration menu (CNF), select **F4 - Configuration options**
- Press on F8 - Search, type TCPFTPD.MSG
- The first item you should find is the **FTPONL** parameter.
- Edit each item as described below, moving from item to item using the arrow keys.
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu.

FTPONL **Allow FTP access to the files on your Worldgroup.**
YES Set this option to YES to enable the FTP Server, to allow access to your MajorBBS/Worldgroup system.

FTPREJ **Send a reject message to FTP callers.**
NO Should your FTP server be shutdown (FTPONL is set to **NO)**, **setting this option to YES** will make the FTP server warn the caller that FTP access is disabled. The FTP server will immediately close the connection with the caller afterwards. If you set this option to **NO** and **FTPONL is set to NO,** the FTP server will ignore any incoming calls to port #21. **This option is visible only if FTPONL is set to NO.**

MAXFTPD **Maximum number of incoming FTP connections to allow.**
16 Incoming connections to your FTP server use channels from the incoming Telnet channel pool defined in your hardware configure (BBSMAJOR.MSG, level 1 hardware configuration). They also use the internal TCP Handles or "sockets", limited to 256 in the standard version of MajorTCP/IP, and 1024 in the unlimited version. Each user that accesses your FTP site will use 1 incoming telnet from channel pool (hence, one license off of a six-pack), and 1 TCP Handle. An extra TCP Handle is used for the actual file transfer. **This option is visible if FTPONL is set to YES.**

MAXANON **Maximum number of anonymous FTP users.**
16 Anonymous FTP access allows you to make some Library files available to all callers, even those who haven't signed up and picked a User-ID. Users do this by connecting to your Worldgroup using FTP and typing "ANONYMOUS" in place of a User-ID, and their Internet Email address in place of a password. See the off-line Security and Accounting options (especially ANONCLS) for configuring anonymous user access to your Worldgroup. **This option is visible if FTPONL is set to YES.**

MAXDFER **Maximum number of simultaneous FTP server transfers.**
16 FTP server allows Internet users to send and receive files between the user and your BBS. Depending on your bandwidth, a large number of file transfers could eat up much of your available bandwidth. This option limits the number of users who can transfer files simultaneously. **This value is different from the MAXFTPD value. In the first case, we fix the maximum number of people who can connect to your FTP site. Here, we actually limit the actual number of simultaneous file transfers.** You can set both MAXFTPD and MAXDFER to the same value if you wish. **This option is visible if FTPONL is set to YES.**

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

FTPDMSS **Maximum Segment Size of FTPD packets (MSS).**
0 The FTPD MSS allows you to set the maximum size of FTPD packets send (or received). A smaller packet size will reduce the impact of FTPD transfers on overall speed, but will reduce the average throughput of the FTPD server. Leaving this to zero will make the FTPD server use the MSS that is defined in tcplibm.msg, option MSS. **See the definition of the MSS in the "Installing the core modules" section of the manual.** If you're running MajorTCP/IP over a 28.8k modem SLIP/CSLIP/PPP connection to your provider, a small MSS is best (256 to 512). If you're running over a faster link, leave this value to 0. MajorTCP/IP will then use the global MSS setting.

OBUFSIZ **FTPD-Data output socket buffer size.**
2048 This sets the size of the output buffer for FTPD sockets. The larger, the better the performance of the FTPD server. However, this also increase the amount of memory taken for each FTPD socket. Note that this only applies to the data transfer sockets, not the control sockets. **Check out the Performance Optimization section in the annex for further details.**

LIBPFX FTP **Directory prefix for File Libraries.**
/library All File Libraries appear to FTP users as subdirectories of a "master" Library directory. For example, if you use "/library", then here's how Library names and FTP directories compare:

Library	FTP-syntax
MAIN	/library/main
WINDOWS	/library/windows
GAMES	/library/games

This option is visible if FTPONL is set to YES.

FDCASE **Convert FTP server file path names to what case?**
LOWER Unix systems typically represent most files and directories in lower case. Your Worldgroup will always ignore case in what users type, but here you can decide how to display files and directories. Choose LOWER to mimic Unix systems. Choose UPPER to mimic DOS. Chose NONE to display items in their natural case (which is often upper case anyway). **This option is visible if FTPONL is set to YES.**

FDSLASH **Display UNIX style slash (/) or DOS slash (\).**
UNIX The BBS will always accept either forward slashes or backward slashes to separate file and directory names. This option specifies what will usually be displayed to users. Pick UNIX to see file path names with forward slashes, or DOS for backward slashes. **This option is visible if FTPONL is set to YES.**

ANONUID **Aliases for "anonymous" User-ID.**
anonymous If the word you specify here is typed-in by an FTP user in place of a User-ID, the user will be offered anonymous FTP access to your Worldgroup server. In the big majority of cases, the most used alias is "anonymous". "FTP" is a good alternative. **This option is visible if FTPONL is set to YES.**

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

GALFANON **Record anonymous FTP info in text file.**
tcpfanon.log This is the name of a text file that will accumulate information on anonymous FTP callers to your Worldgroup. Some long E-mail addresses, specified voluntarily by users as part of anonymous login, may be truncated to fit within the 29-character User-ID. But up to 80-characters of that address can be recorded here in this file, along with other information. See the level 6 Text Block GALFREC for the format of the information in this log file. To disable writing to the log file, type <F2> to clear this option. **This option is visible if FTPONL is set to YES.**

FDALONA **Record anonymous FTP "logons" in Audit Trail,**
NO This option tells MajorTCP/IP to log all anonymous FTP connections. **Set this option to YES to enable this**. If you want to log Secured FTP logons as well (where the user uses his UserID and Password), **This option is visible if FTPONL is set to YES.**

FDAABT **Audit anonymous FTP time and bytes at end of session.**
NO **Set this option to YES** to record the duration in minutes of anonymous FTP sessions, as well as the number of bytes transferred over control and data connections **This option is visible if FTPONL is set to YES.**

FDASBT **Audit secured FTP time and bytes at end of session.**
NO **Set this option to YES** to record the duration in minutes of secured FTP sessions, as well as the number of bytes transferred over control and data connections. **This option is visible if FTPONL is set to YES.**

FDAGET **Record FTP file get's in Audit Trail.**
NO **Set this option to YES** to record every "get" of a file via FTP in the Audit Trail. **This option is visible if FTPONL is set to YES.**

FDAPUT **Record FTP file put's in Audit Trail.**
NO **Set this option to YES** to record every "put" of a file via FTP in the Audit Trail. **This option is visible if FTPONL is set to YES.**

FDAFOP **Record other FTP file operations in Audit Trail.**
NO Set this option to YES to record the deletion or renaming of DOS files, or the creation or removal of DOS subdirectories by FTP users. Normally these operations should be reserved for the Sysop. See the level 3 Security and Accounting Options. **This option is visible if FTPONL is set to YES.**

DOSPFX **FTP directory prefix for DOS drives.**
/dos For the Sysop to access DOS files via FTP, a virtual "tree" structure will be made to represent the collection of directory trees of several different DOS drives. Assuming you set this option to "/dos", then here are some examples for DOS syntax versus FTP syntax:

Example DOS directory	FTP-syntax directory
D:\	/dos/d
C:\WGSERV	/dos/c/wgserv
Z:\NET\SYS	/dos/z/net/sys

This option is visible if FTPONL is set to YES.

DOSFDRV **DOS drives to allow FTP access.**
C You can specify a string of letters that represent the DOS drives for which you want to allow Sysop-level FTP access to. This access is restricted with the DOSVKEY, DOSGKEY, and DOSPKEY. **This option is visible if FTPONL is set to YES.**

Answer	if you want to:
c	only allow access to drive C:
cde	allow access to drives C:, D: and E:
cuvwxyz	allow access to drives C: and U: through Z:

DFTDIR **Default directory for FTP callers.**
/ This option is where you enter the default or work directory for FTP callers. By default, we set this to the "root" directory. Someone typing an "ls" or "dir" who only has normal access or anonymous access would only see the /library subdirectory under this root directory, the content of which is locked depending on the keyrings you've assigned to either class of users. On the other hand, someone with sysop access would see the /library subdirectory and the /dos subdirectory, the latter giving access to any drive specified in the **DOSFRV** parameter and their contents. **This option is visible if FTPONL is set to YES.**

FANCHK **Checking on anonymous FTP e-mail address.**
NONE Enter SYNTAX if you want anonymous FTP e-mail addresses checked for syntax, and rejected if not possibly a valid e-mail address. Otherwise, enter NONE if you want no checking whatsoever on anonymous FTP user e-mail addresses.
This option is visible if FTPONL is set to YES.

FTPDMULT **Activate FTPD Multi-Homing functions.**
YES This FTP server is compatible with MajorTCP/IP's Multi-Homing functionality. If you enable Multi-Homing support for FTP Server, then all anonymous users coming in on a specific Multi-Homing address will be using a class specific for that Multi-Homing address. The exact class used will be computed this way. Let's assume that ANONCLS is set to DEMO. If someone comes in on the base BBS's IP address (anonymously), they'll be in the DEMO class. If they come in, say, to address x.x.x.20, and it is part of your multi-homing group, then they will be in the DEMO020 class. If they come in on address x.x.x.210 then they would be in the class DEMO210. If the class doesn't exist, then the access is denied. **This option is visible if FTPONL is set to YES. See the "Advanced Issues: Multi-Homing" section of this manual for more details.**

ENABWHOM **Enable access to user home page directories.**
YES This FTPD server has been enhanced to work with third party user-home pages management packages so that eligible users are allowed to access their home page directories under the /webhome hierarchy)

If you are using a user-home page management package that has been modified to take advantage of this feature and want to enable it, set ENABWHOM to YES and also check the next options. Note that it is the responsibility of the user home- page management package to specify which directories the user has access to, so be very careful and check that all is fine before making this public.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

NOTE: Even if you are not running a home-page management system, someone with the master key always has access to the /webhome directory.

This option is visible if FTPONL is set to YES.

WHOMTV1 **First Dir Text Variable**

TCP_UWB_HOME This text variable (**TCP_UWB_HOME**) will be used (if not blank) by FTPD to query the user-home page management package for the home-page directory that has been assigned to the current user. It should normally be left to the default, but is programmable in case it's needed. **Visible only if ENAGWHOM is set to YES.**

WHOMTV2 **First Dir Text Variable**

TCP_UWB2_HOME This text variable (**TCP_UWB2_HOME**) will be used (if not blank) by FTPD to query the user-home page management package for the home-page directory that has been assigned to the current user. Should normally be left to the default, but is programmable in case it's needed. If the first one (WHOMTV1) returns no directory, then this second one will be used. **Visible only if ENABWHOM is set to YES.**

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

FTP Access control

In this section, we will try to cover the three different types of access one can setup with the FTP server. There are three modes that interest us: ***secured FTP access***, ***SYSOP FTP access***, and ***anonymous FTP access.*** We will use this configuration as an example:

Available File Libraries with associated keys and FTP server locations

Library name	Key to access	Location via the FTP server
WINDOWS	PAYING	/library/windows
MS-DOS	PAYING	/library/ms-dos
MACINTOSH	PAYING	/library/macintosh
GAMES	PAYING	/library/games
ADVERTISING	FREE	/library/advertising
FAQS	FREE	/library/faqs
MISC	FREE	/library/misc

In this example **LIBPFX in TCPFTPD.MSG, level 4 config, is set to /library.** This means that all libraries appear under the /library "directory". This isn't a real physical directory per see on your drive. It's a "logical" directory under which we can locate all the libraries under. The physical location of the real libraries is unimportant. Even though the library directory doesn't exist on your hard-disk, someone who wants to access say, the FAQS library via your FTP server would need to do a **cd /library/faqs** to access it.

Restricted to sysop-only directories:

Drive C	SYSOP	/dos/c/somedir
Drive D	SYSOP	/dos/d/somedir
Drive E	SYSOP	/dos/e/somedir

Here, **DOSPFX (TCPFTPD.MSG, level 4 config) is set to /dos.** All DOS drives will appear under the /dos directory. Like the /library "directory", the /dos directory is a "logical" directory. It doesn't exist physically on your hard-disk. It serves simply as a means to differentiate your DOS directories from other "logical" groupings (like /library). The **DOSFDRV parameter (TCPFTPD.MSG, level 4 config) is set to to cde.** This parameters lets you specify which drives are accessible to FTP users with SYSOP access.

What this all means is this: say one of your BBS staff members with the SYSOP key wants to go into the C:\WGSERV directory to download some product's MSG file. He would use the following command to change directory: **cd /dos/c/wgserv.**

Secured FTP access

Secured FTP access limits access to your FTP site to people who own an account on your system. This means that they need to own a valid UserID and Password on your BBS, which they will use to logon to your FTP server. They also need the various keys required to be able to access your FTP site. On the BBS side, you obviously need to make sure that the class the user in question belongs to has the proper keys to the various libraries you want to make available to Secured FTP users. To give an account secured FTP access, this is what you need to do:

- Give the user the key corresponding to the **FTPKEY** parameter in **TCPFTPD.MSG, level 3 configuration**.

- Make sure the **LIBKEY is blank** in **TCPFTPD.MSG, level 3 configuration**. This means that MajorTCP/IP will default to the key settings for the various libraries. If the user accessing the FTP site doesn't have the key in his keyring for a particular library, the library will be invisible and innacessible for him.

- Make sure the user has the appropriate keys in his keyring to access the desired libraries. Lets say for the sake of argument, the user has the PAYING key. Furthermore, he has the same key-ring as new users and hence, inherits the FREE key. The user should therefore have access to all the libraries in the example, without gaining access to the DOS directories.

Assuming everything is properly configured, a secured FTP user would use an FTP client to access your FTP site. Once connected, he would be queried for a username and password. He would then enter his BBS **userID OR internet ID if using the internet alias file** and password on your system. **Once logged-in, the user typing "dir" or "ls" at the prompt should see this first:**

```
200 Data connection to 199.84.216.2 on port 1743.
150 List of files and subdirectories to follow:
dr-xr-xr-x  1 .    .          0 Dec 11  1995 library

226 End of list.  1 items.
```

The first character of the dr-xr-xr-x string indicates that this is a directory (if it starts with a d, it indicates a directory. If the first character is blanc, it's a file). Our user types **cd library** to access that directory. Afterwards, **he types ls to find out the contents of the library directory**.

```
200 Data connection to 199.84.216.2 on port 1744.
150 List of files and subdirectories to follow:
dr-xr-xr-x  1 .    .          0 Dec 11  1995 windows
dr-xr-xr-x  1 .    .          0 Dec 11  1995 msdos
dr-xr-xr-x  1 .    .          0 Dec 11  1995 macintosh
dr-xr-xr-x  1 .    .          0 Dec 11  1995 games
dr-xr-xr-x  1 .    .          0 Dec 11  1995 advertising
drwxrwxrwx  1 .    .          0 Dec 11  1995 misc
dr-xr-xr-x  1 .    .          0 Dec 11  1995 faqs

226 End of List.  7 items.
```

As you can see, the user sees all the libraries he has access to as per the example. In the case of the "misc" directory, the user even has write access (drwxrwxrwx, the 'w's indicate write-access), this means that the user has whatever key that allows him to write (upload) to that particular directory. (we added it to his keyring).

To summarize: if the first character is blank, it's a file. If it's a 'd', it's a directory. The 'r' in the string indicates read-access, the 'w' indicates write-access. The 'x' is another indicator that means that this is a directory.

Finally, the user can do a "cd" to go into any of the listed libraries and use the binary command to indicate that this will be a binary download, and then use the get <filename> command to actually do the download.

Sysop FTP access

Sysop FTP access can potentially make your entire hard-disk accessible via FTP. This sort of access should only be given to your most trusted members of your staff. If your system is running multiple drives, it is possible for you to restrict access to certain drives though, which does enhance security somewhat. To grant a user sysop-level access to your FTP site, follow these steps:

- Give the user the key entered in the **FTPKEY** parameter in **TCPFTPD.MSG, level 3 configuration.**

- Make sure the user has the keys associated with **DOSVKEY, DOSGKEY and DOSPKEY parameters in TCPFTPD.MSG, level 3 config**. **The DOSVKEY** lets the user in question **view the file**, it makes it visible to him. The **DOSGKEY** lets the user **GET** or download the file. Finally, the **DOSPKEY** lets the user **PUT** or upload files. This last key also allows the user to create, rename and delete files and directories.

- If the user (sysop/staff) has all of the above plus the various keyrings required to access the libraries as per the user with secured FTP access, he/she should be able to go into the libraries AND navigate the various drives and the subdirectories on them. Since this is a very powerful and dangerous feature, you must consider for a while if you can trust the person with that sort of access.

If we follow the example illustrated in the case of **Secured FTP access** users, someone with sysop access would login to the FTP server in the same fashion, using their UserID and Password on the system. Once logged-in, if the person types “ls” or “dir”, the result should be a little different than in the Secured FTP example.

```
200 Data connection to 199.84.216.2 on port 1748.
150 List of files and subdirectories to follow:
dr-xr-xr-x  1 .    .          0 Dec 11  1995 library
dr-xr-xr-x  1 .    .          0 Jan  1  1970 dos

226 End of list.  2 items.
```

We’ve already seen an example of library directory access. In this example then, the user changes directory into the **dos** directory using the **cd dos** command. Afterwards, he types **ls** at the prompt.

```
200 Data connection to 199.84.216.2 on port 1751.
150 List of files and subdirectories to follow:
drwxrwxrwx  1 .    .          0 Jan  1  1970 c
drwxrwxrwx  1 .    .          0 Jan  1  1970 d
drwxrwxrwx  1 .    .          0 Jan  1  1970 e

226 End of list.  3 items.
```

The user decides to peruse drive c. He types **cd c.** Afterwards, he types **ls** at the prompt.

```
200 Data connection to 199.84.216.2 on port 1752.
150 List of files and subdirectories to follow:
drwxrwxrwx  1 .    .          0 Jun 27  1992 dos
drwxrwxrwx  1 .    .          0 Jul 11  1993 wgserv
-rw-rw-rw-  1 .    .        248 Dec 11  1995 autoexec.bat
-rw-rw-rw-  1 .    .         49 Apr  5  1994 config.sys

226 End of list.  4 items.
```

As you can see, this user with sysop access can upload and download files into the dos and wgserv directory. Furthermore, he could change the autoexec.bat and config.sys files. Since drive c has the drwxrwxrwx access string, the user could also create or delete directories on the C drive.

Give SYSOP access with extreme caution.

Anonymous FTP access

Anonymous FTP access is a service many FTP servers offer these days to provide access to free download areas. Anonymous do not require an account on your system. Instead, they login with the userID “anonymous”, and a password corresponding to their E-mail address. To enable anonymous access to your system, you should follow these steps:

- Set **ANON to YES in TCPFTPD.MSG, level 3 configuration**. This will permit the system to accept anonymous logons to your FTP site.

- Set **ANONCLS (in TCPFTPD.MSG, level 3 config) to the name of a special CLASS** you will create to allow a restricted form of library address to anyone logging on to your FTP site. In this class, you would put the appropriate keys and keyrings to provide minimal (or desired) access to the software libraries. In this case, the ANONYMOUS class (a fictional class) contains the ‘FREE” key. If anonymous users connect to your FTP site, they should be able to download files from those libraries with the FREE key only.

- It should now be possible for anonymous callers to login to our FTP site and access the ADVERTISING, FAQS and MISC libraries, while everything else remains invisible.

Example: if the user types **cd /library** and does an **ls** after logging on, these are the libraries he should have access to:

```
200 Data connection to 199.84.216.2 on port 1744.
150 List of files and subdirectories to follow:
dr-xr-xr-x  1 .    .          0 Dec 11  1995 advertising
dr-xr-xr-x  1 .    .          0 Dec 11  1995 misc
dr-xr-xr-x  1 .    .          0 Dec 11  1995 faqs

226 End of List.  3 items.
```

Creating a WWW link to something on your FTP server

It's possible to create a link from a web page to a file on your FTP server. You can use two methods. One is with an anonymous FTP account, the other is to a predifined account with username and password.

Lets say you had a file in the MISC directory containing your system's FAQ (Frequently-Asked Questions and Answers) called **mybbs.faq**, and you wanted to allow someone to download it from your FTP site via a click of the mouse from your web page. This is how the HTML code would look like for this example:

<A HREF="ftp://yourbbs.com/library/misc/mybbs.faq>Download our FAQ</A>

When the person clicks on "Download our FAQ", the web browser will automatically grab the mybbs.faq file from the MISC library on your FTP server.

The general form the URL would take is:

ftp://yourdomain.com/library/library-name/filename.ext

You can also have a URL where the system will allow the user to logon via an account on your system. In this case, the user will need to supply a password to the machine in question:

ftp://userid@yourdomain.com/library/library-name/filename.ext

<A HREF="ftp://charles@yourbbs.com/library/misc/mybbs.faq">Click here for FAQ</A>
In this example, the person clicking on "Click here for FAQ" would be queried for the password of the charles account on the BBS before being able to get the mybbs.faq file.

You can even have the password pre-coded into the URL:

ftp://userid:password@yourdomain.com/library/library-name/filename.ext

<A HREF="ftp://charles:cleo@yourbbs.com/library/misc/mybbs.faq">Click here for FAQ</A>
In this example, the person clicking on "Click here for FAQ" would get the file mybbs.faq immediately, because the URL already has the username and password required to access the ftp site through that account. Note that this method is not recommended due to the security problems this type of FTP access could cause.

Limitations of MajorTCP/IP's FTP Server

- Doesn't allow overwrites or deletes of files in file libraries, It will however allow it for LIB-OPS in DOS-only file libraries.
- Will not work with CD roms. You should mark any library that refers to a CD rom directory as being a CD rom library, so that MajorTCP/IP will skip those directories.

These two problems will be adressed in future versions.

Advanced Features: multi-homing capability

This is the first of a series of advanced features that will be added to MajorTCP/IP. Contrary to the rest of MajorTCP/IP's documentation, we assume here that you have a solid grasp of MajorBBS/Worldgroup operations and understand the various issues pertaining to domain names and internic registration. This section was last revised on June 15, 1996.

Multi-homing Overview

Multi-homing lets you transform your system into multiple virtual BBS. This means that your BBS can disguise itself to suit your client's needs. A growth industry was created recently by the desire for companies to have their own domain name, with associated Web and E-mail services. Unfortunately, up until the latest version of MajorTCP/IP, it wasn't possible to offer such personalized services except through a "fake" multi-homing scheme, accomplished via an alias of the primary domain name of the BBS corresponding to the client's desired domain name, a web page directory for the client and use of a POP3 mail-reader so any outgoing mail is labeled as coming from the aliased domain name.

With the new version of MajorTCP/IP comes the capability of offering true multi-hosting capability. Multi-hosting covers five aspects of BBS virtuality.

SMTP E-mail Virtual Domains

The domain added to the User ID on outgoing E-mails can now be different based on the user's class. Combined with MajorTCP/IP's multiple host aliases, it is now possible to truly handle mail for different domains. The limit of 20 domains is also removed to allow a large number of virtual mail domains running on the same Worldgroup server.

This means that the SMTP module can be configured to accept a large number of domain names we're accepting E-mail for. In addition, specific user classes can be set so that any Email they send out using the SMTP module will go out under a specific domain: If a company called **Widgets Inc**. wants to receive and send E-mail using your BBS as if all mail was coming from **widgets.com,** it can. Incoming mail destined for the **president of widgets.com** will not be rejected, as **widgets.com** will be regarded as a proper alias of **yourdomain.com**. Furthermore, any mail sent by the **president of widget.com** will be labeled as coming from **widget.com**, not **yoursystem.com**.

Telnet/RLogin Virtual Domains

Your Worldgroup server can now be configured to listen to multiple IP addresses. This provides a powerful method of hosting multiple virtual BBS on the same Worldgroup server. When a Telnet/RLogin connection is opened, MajorTCP/IP defines a pseudo-key based on the IP address called. Used in concert with products such as High Water Mark's "Virtual User", different login screens and menu trees could be displayed. This capability requires that you assign one IP address of your class C (or range of IP addresses available) to this use for each company that requests this capability.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Lets assume your BBS is located at 199.84.216.2, and you own the entire class C (from 199.84.216.0 to 199.84.216.255). You assign the **widgets.com domain name** the IP **199.84.216.20**. If someone telnets to **widgets.com**, they will hit your BBS through the 199.84.216.20 IP address. A text variable will indicate this upon log-in. Using autoselect menus, you could conceivably create a totally different menu hierarchy for users coming from that IP address, basically making your BBS into a virtual BBS.

WWW Virtual Domain

Based on the IP address the WWW request came for, web pages stored in different directories will be transmitted to the browser. Since the information is kept in distinct directory tree structure for each IP address, maintenance of the client's web site becomes an easy task. This capability requires that you assign one IP address of your class C (or range of IP addresses available) to this use for each company that requests this capability. The same way we know from which IP address someone tries to connect to, we know what IP address they are using to gain access to the web server. All we do is assign a different directory tree for that IP.

What this means is that a person trying to do an **http://widgets.com/** will get the index.htm page of the directory tree assigned to **widgets.com** (199.84.216.20) **,** instead of the previous case where widgets.com simply pointed to your BBS IP address which meant no differentiation between domain name aliases and the IP address. That forced you to put the client's web pages in a subdirectory of your only directory tree for web pages. The URL would look like **http://widgets.com/hisdir/** instead, which is a bit strange, if the system is supposed to pretend to be a standalone web server for **widgets.com**.

FTP Server Multi-homing

MajorTCP/IP's new FTP server supports anonymous access multi-homing. That means that you could operate various libraries for companies that want to be hosted on your system, and make them accessible to their domain names via FTP. This feature however only works for anonymous FTP access.

Multi-Homing and Murkwork's Worldsock

When using WorldSock, all users are normally using the same IP address which is the base BBS IP address. This works fine for most applications, but some (like CuSeeMe) require their own address.

We've added an API to MajorTCP/IP that will enable Murkworks to change Worldsock so that it can assign IP addresses to individual users. The IP address will come from the "**multi" group defined further** in this section. Murkworks has confirmed that they have adapted multi-homing to provite dynamic IP addressing to Worldsock users.

Installation procedure for multi-homing

Each multi-homing option is totally optional. Feel free to use only those options you need.

STEP	Description	Done
#1	Configure SMTP E-mail Multi-Homing / Virtual Domains	
#2	Configure the IP range for Telnet/RLogin and WWW Multi-homing	
#3	Configure WWW Multi-Homing	
#4	Configure Telnet/RLogin Multi-Homing	
#5	Configure FTP Multi-Homing	
#6*	Check out the Sample system configuration for Multi-Homing	

* Step #6 isn't really a step, more of a suggestion in case you need a concrete example configuration-wise.

Configure SMTP E-mail Multi-Homing / Virtual Domains

Normally, SMTP processes mail that is only addressed to you base BBS hostname + domain name as specified in TCPLIBM.MSG, level 1 hardware configuration. E-mail addressed to other domain names will be promptly rejected. That's not very usefull if you want to be able to handle multiple domain names.

E-mail multi-homing involves extra domain names that will either point at your BBS IP address or an IP address from your class C that MUST be processed in the same fashion mail is processed for your BBS domain name. To this end, you need to create the host alias file identifying all the domain names that correspond to your BBS. These domain names are called **"domain name aliases".**

Prepare MajorTCP/IP for the SMTP Host Alias File.

This step tells SMTP which file is going to contain the various domain names that the BBS will be handling mail for.

- From the CNF, go to **level 4 configuration options.**
- Press on **F8 - Search.** Look for **SMAL01**. It should be found under **TCPSMTP.MSG**.
- At the SMAL01 parameter, type in $ followed by the filename of your SMTP Host alias file. We use on our own support BBS the name of **TCPSMHAL.TXT**, so we wrote **$TCPSMHAL.TXT** in the **SMAL01** parameter.
- Note that doing this disables any other alias entered in **SMAL02 to SMAL20** if you have any. You'll have to transfer these to the alias file.
- Go to DOS.

Create the SMTP Host Alias File

Fire up an ascii text editor (like Dos Edit) and create the file defined in the **SMAL01** parameter.
This is the format the file should take with an example:

Format of the file:

host1 [class]
host2 [class]
host3 [class]
host4 [class]

hostn: a hostname.domainname that is to be considered as another alias for the BBS. We will accept all email addressed to this hostname.domainname as mail for users on the BBS. If it begins with a '*', only the characters after the '*' will be matched.
Example: gm.gamemaster.qc.ca, *.gamemaster.qc.ca

[Class: OPTIONAL] If a user is in this class at the time SMTP tries to send the email out, the email will be sent out using the hostname listed above. You do not want to use this feature with wildcard ('*') domains. **Example:** gm.gamemaster.qc.ca HOURLY

Example:

```
gm.gamemaster.qc.ca HOURLY
bbs.vircom.com VIRCOM_STAFF
widget.com WIDGET_USER
www.vircom.com
```

Those in the HOURLY class will have their E-mail labeled as coming from gm.gamemaster.qc.ca. Those in the VIRCOM_STAFF class will see their E-mail labeled as coming from bbs.vircom.com. Those in the WIDGET_USER class will see their E-mail labeled as coming from the widget.com system. Finally, the last line simply indicates another alias of the BBS'es domain name. No class means that no mail will be labeled as coming from www.vircom.com. (except for the base HOSTNAME and DOMNAME where, if a user doesn't have any of the mentionned classes, his mail will be label as coming from the HOSTNAME+DOMNAME in TCPLIBM.MSG, or SMTPFROM in TCPSMTP.MSG).

Register the alias or aliases.

You'll need to ask your provider to add each domain alias to his DNS servers (the configuration of which is beyond the scope of our support). These alias domains will need to be routed to your BBS. This would usually be done by defining an MX record of priority 0 pointing to your BBS for each alias defined. Furthermore, these domain name aliases will need to be registered on the internic, something your provider can do for you. For more information about domain name registration, try **http://rs.internic.net/.**

If your clients only require E-mail multi-homing, you will not need to assign a different IP address for that particular domain. However, if your client will require Virtual Telnets/RLogins or a Virtual Web Site, then you'll need to have the client registered under the IP address you will assign him from your class C. E-mail will need to be routed to your primary BBS IP by your provider through the MX records.

Configure the IP range for Telnet/RLogin and WWW Multi-homing

This feature lets your BBS TCP/IP Servers listen to multiple IP addresses at the same time. Some servers (WEB2, Telnet/RLogin) have been modified to take special advantage of this.

Follow these steps to tell the BBS to use multiple-IP addresses:

- Go to **level 1 - hardware configuration**
- Press **F8 - Search** to Find the Special Configuration options **CFGTXT01**
- Go to the first available option (usually **CFGTXT01**)
- Type in **multi:lowip/highip**, where **lowip is the Lowest IP address** MajorTCP/IP will use for the IP multi-domains and **highip is the highest IP address**. This is in addition to the normal IP address of the BBS. **This range must not overlap with the ranges assigned in the SLIP/CSLIP/PPP server** (see **SLIPDLOW/SLIPDHGH and SLIPSLOW/SLIPSHGH in TCPSLIP.MSG, level 4 configuration**). Results are unpredictable if they overlap. Only enter the last digits of the range.

Example:

System owns the entire 199.84.216.XXX class C.

```
MYIPADDR    TCPLIBM.MSG (CNF1) 199.84.216.2
GATEWAY1    TCPLIBM.MSG (CNF1) 199.84.216.1
SLIPNET     TCPSLIP.MSG (CNF4)  199.84.216.0
SLIPDLOW    TCPSLIP.MSG (CNF4)  100
SLIPDHGH    TCPSLIP.MSG (CNF4)  175
SLIPSLOW    TCPSLIP.MSG (CNF4)  176
SLIPSHGH    TCPSLIP.MSG (CNF4)  254

CFGTXT01    TCPLIBM.MSG (CNF1) multi:10/50
```

Say, for the 199.84.216.X class C address, we have 199.84.216.100 to 175 assigned for dynamic IP allocation, and 176 to 254 for static IP allocation in the SLIP/CSLIP/PPP server.
We select the range from 199.84.216.10 to 199.84.216.50 as the range of IP addresses we'll allocate for multi-homing. **That means that we'll enter multi:10/50** in the CFGTXTXX parameter in TCPLIBM.MSG, level 1 hardware config.

You'll need to define hostname.domainnames for each IP that you will allocate to various clients who want their own domain name. You'll have to deal with your provider to add these to his DNS server and to register these domains with the Internic. Don't forget what was mentionned in the SMTP E-mail multi-homing section about the MX records as well if you want these users to be able to send and receive E-mail under their own domain name.

Configure WWW Multi-Homing

Before we wrote the Multi-Homing components for the web server, those of you that are selling domain names for the WWW were probably using this technique to do “pseudo-multi-homing”:

Let's say your World-Wide-Web server address is **www.yourdomain.com.** Your customer (Widget Inc.) wants to have a page on your server. Before multi-homing, his URL would most likely be **http://www.widget.com/info** or **http://www.widget.com/info/index.htm**. Although you created an alias for www.yourdomain.com that’s called www.widget.com, you need to put the client’s pages in a subdirectory that must be accessed explicitly.

Most customers would rather have their pages accessible directly without having to specify a subdirectory. They would prefer that their URL looked like **http://www.widget.com**.

This is now possible.

We’ll use the example in STEP #2 (widget.com), using one of the IP addresses from the multi:lowip/highip range to illustrate the process.

Assign an IP address to www.widget.com

You'll first get one IP address from your multi range (the multi:lowip/highip mentionned in the previous chapter), and assign it to www.widget.com in your provider’s DNS name server. (Of course, you'll have to register the domain by talking to your provider and the internic ...), We'll assume that you want to assign **199.84.216.45 to www.widget.com as per the example in STEP #2.**

Configure the default web page directory for the new IP address

The WWW server will now automatically serve a different default (home) directory for this IP address. What this means is that, instead of looking for pages in the standard **TCPWEB2\WEBPAGES** directory, all pages retrieved via **www.widget.com** will be taken from the **TCPWEB2\WEBPAGES.045** directory. **If the directory doesn’t exist, you’ll need to create it by hand under TCPWEB2.**

Example:

If the domain name will be pointing at **199.84.216.45**, the directory is **WEBPAGES.045** If the domain name is pointing at **199.84.216.220**, the directory is **WEBPAGES.220**

You can use multi-homing with the **WEBACCESS.LOG** file and the **IMAGEMAP**s as well. Normally, WEBACCESS.LOG is stored in the TCPWEB2 directory, and most image maps will be stored in the TCPWEB2\IMAGEMAP directory. To make sure that both the web access logs and the image maps will be used directly from the new directory created for the domain name selected, **set LOGLOC to NO and IMGLOC to NO** in **TCPWEB2.MSG, level 4 configuration**. In our last example, this means that both the **webaccess log and imagemaps** will be found in the **WEBPAGES.045 directory, under the TCPWEB2** directory.

Add access control (optional)

You will probably want to protect your **webaccess.log** with a key, if you have set **LOGLOC** to **NO** in **TCPWEB2.MSG, level 4 configuration**.. The format of the access.ctl file has been expanded so that you can specify to which IP address the page you're trying to protect belongs to. The format is now:

```
page key [IP]
page key [IP]
page key [IP]
```

Example:

```
INDEX.HTM  WIDGKEY 45
COMMENT.HTM WIDGKEY 45
FILE.ZIP WIDGETKEY 45
```

This will protect the TCPWEB2\WEBPAGES.045\index.htm, with the key WIDGKEY. Also the comment.htm and the file.zip file.

If you use 0 as the IP, all pages of that name, for all IPs, will be protected. If you don't put anything, it protects only for the base IP of the BBS.

Identify your web server for proper directory redirection.

You need to create a file, called **TCPW2HST.TXT** that defines all the hosts names the Web2 server will be using. It's a text file, in the directory **TCPWEB2**, that has the following format. For more information, see the **WEB2HOST** option in **TCPWEB2** documentation, level 4 configuration.

```
<IP1> <HOSTNAME1>
<IP2> <HOSTNAME2>
  ‘’              ‘’
```

Example:

```
199.84.216.2 www.vircom.com
199.84.216.20 www.widget.com
199.84.216.30 www.thisco.com
```

The "hostname" is what will be used on a redirection when the server hit is on that IP address. The BBS' base IP address doesn't have to be defined here (and will be ignored if it is) and always uses WEB2HOST or HOSTNAME/DOMNAME if WEB2HOST is empty in TCPWEB2.MSG, level 4 configuration.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Configure Telnet/RLogin Multi-Homing

These two servers will accept calls on all IP addresses listed in the multi: command. In addition, you can see which IP address the user telneted to in the /TCPID command while the user is online. This address is also defined in the TCP_CALLED_IP text variable and can be keyed using the _TCP_CIP#nnn pseudo key.

Example: If you wanted an auto-select page to be selected only when the user telneted to 199.84.216.45 (or the domain associated with this IP address), then you would used the key _TCP_CIP#45 to key the auto-select page.

The applications of these features are vast. One can conceive a virtual BBS that would look totally different depending on which IP address the user telneted to. We'll try to make a list of ISV add-ons that can be used to help doing this.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

A real world example: alternate TOP menu for someone coming from an alternate IP

Lets assume for argument's sake that the IP address of 199.84.216.45 is the IP address assigned to the widgets.com domain name as per the previous paragraphs. We want to offer users of Widgets an alternate TOP menu that they will see when logging onto the BBS.

The key to verify would be **_TCP_CIP#45**. Someone getting this key would obtain the TOP2 menu instead of the the TOP menu.

1. Startup the system and go into your menu tree.

From the CNF menu, pick option #2, Design Menu Tree

2. Create the TOPDEF menu page

The **TOPDEF** page would become the default TOP page that would be called by the original **TOP** page. You need to copy all the options you have in your normal **TOP** menu to this menu because the **TOP** menu will be turned into an autoselect menu. (Teleconference, Forums, Email, so on and so forth ...)

3. Create the TOP45 menu page

The **TOP45** menu page is the menu that will be called for people telnetting in from the 199.84.216.45 IP address (as per example). This menu can contain whatever options you want, including options from the original TOP menu.

4. Modify the TOP menu

- In the "Is this an autoselect menu" option, set it to **YES**.
- Delete all the options in the **TOP** menu (Teleconference, Forums ...).
- Create the first option
  - Select character ..... Unimportant.
  - Short description ..... **"Widget alternate menu"**
  - Key required ..... **_TCP_CIP#45**
  - If user has no key ..... **Dim Option**
  - Destination page **TOP45**
  - Save this option ..... **YES**
- Create the second option
  - Select character ..... Unimportant.
  - Short description ..... **"Default main menu"**
  - Key required .....
  - If user has no key ..... **Dim Option**
  - Destination page ..... **TOPDEF**
  - Save this option ..... **YES**
- You're done!

The new TOP menu would work this way. If the person logs in via the **.45** IP address,
he is assigned the _TCP_CIP#45 key that will automatically force him into the TOP45 menu, which is the menu specific to Widget BBS. If however, the user doesn't have the _TCP_CIP#45 key, he will automatically get the TOPDEF menu which is simply a carbon copy of the original TOP menu, before we turned it into an auto-select page. Using this example, you could have as many different "TOP" menus as you have individual companies using your multi-homing services.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Configure FTP Multi-Homing

With the birth of MajorTCP/IP's FTP server, we decided to add multi-homing capability to the new module from the outset. What multi-homing allows with the new FTP server is the ability to offer anonymous user access tailored to the various subdomain names that are assigned to your system. What this means is that, if say, as per the previous examples, someone accesses the ftp site at 199.84.216.30 (widget.com instead of vircom.com which is .2) as an anonymous, he will be placed in a special class from the outset. All you need to do then is to define these classes with personalized keyrings that grant access to libraries that may or may not be exclusive to the company that has the subdomain name.

For more information about the FTP server, check out "STEP #15: Configuring the FTP server" in this manual. FTP Multi-homing only works with anonymous FTP access.

Here's a setup example:

Say your system is called something.com and is at the 199.84.216.2 IP address. You've defined as your multi:low/high range from .20 to .30 (multi:20/30). The somecorp.com domain name was assigned to the 199.84.216.20 IP address. Someone doing an FTP access to the somecorp.com domain name would thus be coming in at the 199.84.216.20 IP address.

The user logs in as anonymous with the password corresponding to his E-mail address. Automatically, MajorTCP/IP will put this user in a special class. The class for anonymous users is defined in the ANONCLS parameter in TCPFTPD.MSG, level 4 configuration. In our case, the default is DEMO. When a user connects via multi-homing, in this example on the .20, the class the person is put in is DEMO020. That means that you could create these classes on your system with individualized keyrings granting access to a selected list of libraries on your system. An anonymous user logging on to the .210 would therefore be in the DEMO210 class.

To setup multi-homing, follow these steps:

- Turn on FTPD multi-homing by setting FTPDMULT to YES in TCPFTPD.MSG, level 4 configuration.

- Note down the setting of ANONCLS in TCPFTPD.MSG, level 4 config. By default, this value is set to the "DEMO" class. That means that people logging via the .30 would be put in the DEMO030 class, people logging on via the .100 would be in the DEMO100 class. If you change ANONCLS say to a new class say "ANON", that means that people coming in from the .30 would be in the ANON030 class and people coming in from the .100 would be in the ANON100 class.

- Create the classes (example: ANON030 and ANON100), assign them those keys that will grant access to the appropriate file libraries depending on what your clients with the multi-homed domain names want to grant access to (probably a corporate library exclusive to them on your system for instance).

- That's it.

Sample system configuration for Multi-Homing

Following is an example of a **Multi-Homing** setup, step by step. Please note that the values here are entered solely as examples, and should not be used on your own system except for "generic" values, like the Netmask which is almost the same for everyone.

Before starting

Let's assume that these are the settings in your system:

Option Name	CNF	Value		Option Name	CNF	Value
MYIPADDR	Lvl 1	199.84.216.2		**SLIPNET**	Lvl 4	199.84.216.0
NETMASK	Lvl 1	255.255.255.0		**SLIPDLOW**	Lvl 4	100
GATEWAY1	Lvl 1	199.84.216.1		**SLIPDHGH**	Lvl 4	150
PRIDNS	Lvl 1	199.84.216.1		**SLIPSLOW**	Lvl 4	200
HOSTNAME	Lvl 1	bbs		**SLIPSHGH**	Lvl 4	254
DOMNAME	Lvl 1	widget.com				

The address you wish to allocate to your client is **199.84.216.100**. The domain name he will be registered under is **hisco.com**, and possibly also **www.hisco.com**. Take note that each domain name needs to be registered with **Internic**. For more information, please contact **Internic** on the Web at: **http://www.internic.net**.

Step #1 Make sure hisco.com and www.hisco.com are pointing at the right IP address

This means you will need to speak with your provider in order to have the address **199.84.216.100** assigned to your client's domain name(s). Both **hisco.com** and **www.hisco.com** should point to **199.84.216.100**.

Step #2 Ajust the settings in your system before allocating multi-homing features

Let's say you want to allocate from **199.84.216.50** to **199.84.216.100** for multi-homing. The **100** overlaps with the settings of your **SLIPDLOW** configuration option unfortunately. So you'll need to tweak your settings as follows:

- Go inside **TCPSLIP.MSG, Level 4 Configuration**.
- **Press F8** and search for **SLIPDLOW**.
- **Change it to 101, instead of 100**

No overlap problem.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Step #3: Set the range of IP addresses that will be allocated to Multi-homing

- Go to **Level 1 Hardware configuration.**
- **Press F8** and search for **CFGTXT00 (under TCPLIBM.MSG).**
- Press **enter** to edit it.

As stated in the documentation, all that is required is the last digit of **IP**s, lowest and highest. Therefore in our example, the setting should be:

multi:50/100

Step #4: Create and edit the TCPSMHAL.TXT file

You need to change the **Level 4** option **SMAL01** to read the file **TCPSMHAL.TXT**. In order to do this, go to **Level 4 Configuration Options** and press **F8** to search **SMAL01**. At the **SMAL01** parameter, type in **$TCPSMHAL.TXT**.

The file **TCPSMHAL.TXT** should be located in your BBS directory (ex: C:\WGSERV). This is the current content of the file (Domain name and Class name):

hisco.com HISCO
www.hisco.com HISCO
bbs.widget.com
www.widget.com

When someone of **Widget BBS** replies to a message, the e-mail will be labelled as coming from **someone@widget.com**. But if a customer of **Widget BBS** is in the **HISCO** class, the e-mail will be labelled as coming from **someone@hisco.com**.

The other entries are there simply to identify all the other aliases the server goes by, so that mail will not bounce.

Don't forget to create a class called **HISCO**. Consult the **Worldgroup** manual on setting up classes.

Step #5: Identify your web server for proper directory redirection

There's a file in the **TCPWEB2** directory (C:\WGSERV\TCPWEB2) called **TCPW2HST.TXT** which must exists in order to identify all of the Web sites on your system. It should look like this (IP address and Domain Name):

199.84.216.2 www.widget.com
199.84.216.100 www.widget.com

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Step #6: Create the WEBPAGES.100 directory

In **TCPWEB2**, all your system's web pages would normally go in the **WEBPAGES** directory. For **hisco**, you must create the directory **WEBPAGES.100**, because their **IP** ends with **.100**. If the **IP** address was ending by a number lower than 100, for example .3, the directory name to create would be **WEBPAGES.003**. That's where all of **hisco**'s web pages will need to be. So, someone browsing **http://www.hisco.com** will get the **index.htm** file found in the **C:\WGSERV\TCPWEB2\WEBPAGES.100** directory.

Step #7: Change the ACCESS.CTL file

The **ACCESS.CTL** file is used to limit access to the web pages listed in this file. For example, to protect the **info.htm** and the **secret.htm** files with the **HISCOKEY** key, in the C:\WGSERV\TCPWEB2\WEBPAGES.100 directory, the **ACCESS.CTL** file should look like this:

info.htm HISCOKEY 100
secret.htm HISCOKEY 100

The first item is the file to protect. The second item is the key. The third item is the last digit of the IP address to identify in which webpages directory they belong to, in this example, **WEBPAGES.100**.

And, if you have a sub-directory in the **WEBPAGES.100** directory called **SECRETS** (C:\WGSERV\TCPWEB2\WEBPAGES.100\SECRETS) with a page in it called **ultrasec.htm**, the the line in the **ACCESS.CTL** file would look like this:

secrets\ultrasec.htm HISCOKEY 100

So this is how the entire file would look if we followed the example above:

info.htm HISCOKEY 100
secret.htm HISCOKEY 100
secrets\ultrasec.htm HISCOKEY 100

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Advanced Features: banning outside systems

Overview

MajorTCP/IP lets you setup a simple "firewall" that prevents specific systems on the internet from accessing your BBS. This is usefull to protect your system from attacks by malicious hackers who might attempt "mail-bombing" you or persist on trying to crack user accounts with passwords on your BBS via the internet. Note that this is a bidirectional block. **Users calling in from the banned systems cannot reach your BBS, nor can you reach their system.**

Basically, you can create a file called "TCPSITES.BAN" in the BBS directory (WGSERV or BBSV6) that will contain all the IP addresses that are banned from accessing your BBS. Any user trying to contact you from the IP addresses in that TCPSITES.BAN file will be unable to contact your system either directly via Telnet/RLogin or by E-mail.

Installation procedure for TCPSITES.BAN file

There are only two steps involved to create the TCPSITES.BAN file.

STEP	Description	Done
#1	Configure the TCPLIBM.MSG file	
#2	Create the TCPSITES.BAN file	

Configure the TCPLIBM.MSG file

You need to set the **BANMODE** parameter in **TCPLIBM.MSG**, **level 1** hardware config to the appropriate value (**NO**). This parameter tells MajorTCP/IP to use the **TCPSITES.BAN** as an exclusionary file. That means that any IP address in the TCPSITES.BAN file will prevent access to the BBS coming from those IP addresses.

Level 4 - System options configuration

- From the main configuration menu (CNF), select **F4 - Configuration options**
- Press on **F8 - Search**, type **BANMODE**
- Set BANMODE to NO. (Note that this is valid only in the Combo version. Setting BANMODE to NO on a DMA Server is innapropriate).
- Once done, press on **F10 Save and Exit** to go back to the main configuration menu.

BANMODE **Use TCPSITES.BAN to list allowed sites**.

NO You can define a TCPSITES.BAN file to list of sites that are not allowed any connectivity with the BBS. Or you can set BANMODE to yes, and use the TCPSITES.BAN file to list the sites that CAN communicate with the BBS. If you do so, only the listed sites can have any sort of connectivity with the BBS. The TCPSITES.BAN file can be created with a simple text editor. On each line, put the IP address of the site you want to ban (BANMODE=NO) or allow (BANMODE=YES). This feature lets you stop hacking attempts from a particular IP if your system finds itself under attack. The TCPSITES.BAN file has to be located in your BBS directory (WGSERV/BBSV6).

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Create the TCPSITES.BAN file

Go to DOS and fire up a text editor (like DOS Edit) and create the TCPSITES.BAN file. The file **must** be in the BBS directory. For Worldgroup, that's in the **WGSERV** directory. For MajorBBS 6.25, it's **BBSV6**.

Format of the file:

```
<IP address #1>
<IP address #2>
<IP address #3>
... so on and so forth
```

Example:

```
199.84.216.45
180.23.16.5
205.240.12.0
```

In this example, people trying to telnet in from the **199.84.216.45** or **180.23.16.5** IP addresses will not be able to connect to your system. **The 205.240.12.0 is special**. If you use a 0 at the end of an IP address as in the example, this **bans the entire class C**. This means in this particular example, people using **205.240.12.1 to 205.240.12.254** will be unable to connect to your system. This is particularly usefull if the offending user is connecting in PPP to that IP address and the provider at the other end allows SLIP/PPP dynamic access (hence, a range of IP addresses where the offending user connects to, not a single fixed IP address).

For the TCPSITES.BAN file to take effect, simply bring the system back online. If you edited the file on a network drive while the BBS was running on another machine, you can force MajorTCP/IP to read the TCPSITES.BAN file by using the "R" option under the TCPLIB sysop menu.

Advanced Features: DMA Server configuration

Last updated: December 9th 1996, Distributed MajorBBS Architecture V2.1 preliminary Docs.

- Added: **dmanoascpause** special configuration option to disable screen pausing when a user is in ASCII mode.

Note: The DMA server is a separate product that must be purchased separately. When you purchase MajorTCP/IP, you get a free DMA _client_ which allows you to connect to DMA Servers.

Overview

Definitions

DMA	Stands for "Distributed MajorBBS Architecture".
MasterBBS	Your main server, where your callers first connect.
DMA Server	The secondary server (sometimes referred to as a **SubBBS**), where some of your modules are actually located.

What is DMA?

DMA2.1 allows you to move modules from your ***MasterBBS*** onto a ***DMA Server***, and make these changes transparent to your users. **DMA2.1** takes care of automatically creating accounts when a user access facilities on the ***DMA server*** for the first time, permits transparent (invisible) logins and logouts and special echo control depending on the modules running on the ***DMA Server***. Furthermore, the **DMA server** will automatically whisk the user to whichever module you've specified on the **MasterBBS**. Security-wise, **DMA2.1** is a secure environment, as long as you set it up properly with prudence.

The benefits of operating a DMA Server are many:

- **Ability to go beyond the 16 megabyte barrier:** you can offload modules to the DMA Server, hence, splitting the load to two systems. Each could conceivably have 16 megs of RAM, making it possible for you to run 32 megs worth of modules.

- **Improved system performance:** by offloading heavy resource grabbers to a DMA Server, this improves performance on the MasterBBS.

- **Reduced downtime:** If you put your unstable modules on your DMA Server, this will reduce the amount of system downtime your system may occasionally suffer from. If the DMA Server crashes, the MasterBBS keeps running normally. This is especially useful with crash-prone games.

- **Ability to create networks of BBSes:** DMA technology has created a whole new industry of "Game Nets". You can let other MasterBBSes connect to your DMA Server, even over the internet. What this means is you could potentially have dozens of BBSes all sharing the same modules on your DMA server, making it possible to have large numbers of users in those modules, coming from all over the world.

This is just scratching the surface.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Multiple-Multiple Relationships

DMA2.1 supports multiple ***MasterBBSes*** having pages that point to multiple ***DMA Servers***. User-ID collision is prevented by using a **suffix** that is added to the userid of your users when using accounts on the ***DMA Server***. These suffixes are controlled by the ***MasterBBSes***. Suffix 0 is no-suffix. To prevent User-ID collision, you must limit the size of your User-IDs on the ***MasterBBSes*** to 27 characters.

Compatibility

DMA1.0 is still supported in the code, but no longer supported as a product. Once you have converted your ***DMA1.0 Server*** over, you should set Level 4 Option **DMAPH1** to **NO** in the file **TCPLIBM.MSG** on the ***DMA Server***.

DMA2.1 can be run on a **MajorBBS 6.25** or **WorldGroup** system. Furthermore, you need to be running **MajorTCP/IP version 1.78 or better on the MasterBBS**.

LICENSING

Your ***DMA Server 2.1*** License includes the right to copy your **MajorBBS/Worldgroup** system onto **one *DMA Server***. Note that you can only configure **Telnet channels** and **one** Lan channel on the ***DMA Server***. You are specifically prohibited from connecting modems onto a ***DMA Server***.

You must purchase **a copy of MajorTCP/IP's DMA Server** for **each** computer that is used as a ***DMA Server*** in a **DMA2.1 system**.

If you use **DMA** to run multiple copies of a module, you are probably violating the license that was allocated to you by the author of the module. Some products have limited distribution agreements based on geographical location that might be violated by the ability DMA technology gives you to allow outside systems to access your DMA Server's resources, irregardless of their physical location. Please contact the author of the respective software for more information.

Limitations of DMA

Currently, the DMA server will only let you offload modules that run in A/A (Ascii/Ansi) mode.
C/S modules that have an Ansi/Ascii interface should work as well.

Installation procedure for the DMA Server

Setting up a DMA server requires that you perform special configuration tasks on both the MasterBBS and the DMA Server. Simply follow these steps:

STEP	Description	Done
#1	Configure the security on the DMA Server	
#2	Configure the MSG files on the DMA Server	
#3	Configure the MSG files on the MasterBBS	
#4	Install/Move modules from the MasterBBS to the DMA Server	
#5	Setup the link from the MasterBBS to the DMA Server	

Configure the security on the DMA Server

The DMA Server will automatically refuse any ordinary telnet and rlogin calls from the outside world. That's because someone _must_ go through a MasterBBS to access a DMA Server. Furthermore, systems that are not listed in the TCPSITES.BAN file will not be able to access your DMA Server, even if the systems are using a DMA Client to attempt to connect to your system. Finally, systems that have a DMA client but do not have the proper DMA password to access your DMA Server will be refused connection.

Setting the TCPSITES.BAN file as a DMA Server access file

Set **BANMODE** to **YES in TCPLIBM.MSG, level 4 config**. on the ***DMA Server***. This tells the DMA Server to use the TCPSITES.BAN file as a listing of systems that will be allowed to connect to your system. Normally, when BANMODE is set to NO, the file is used to _prevent_ specific systems from connecting to your BBS. This is not what we want.

Create a file in your BBS directory called TCPSITES.BAN. Each line should contain the IP address of the systems that will be allowed to connect to your system. Here is the format of the file:

```
<IP address #1>
<IP address #2>
<IP address #3>
... so on and so forth
```

Example:

```
199.84.216.45
180.23.16.5
205.240.12.6
```

Each IP address in the file is a system that's allowed to connect to your DMA server. This assumes that they are using a DMA Client and they have the proper DMA Password to gain entry to your DMA Server.

Set the DMA Password on the DMA Server and the special Rlogin string on the MasterBBS.

For a MasterBBS to gain access to your DMA Server, it must know what the DMA Password is on your system. First though, you have to assign this password to the DMA Server. This is to prevent unauthorized access to the facilities on your DMA Server.

To **set the DMA Password on the DMA Server**, look for the DMAPWD option in level 3 configuration options, in the TCPLIBM.MSG file. Change the default value to whatever password you desire. The password can be up to 30 characters long.

On the MasterBBS, the password is given in the special Rlogin command string that establishes the connection between the MasterBBS and the DMA Server. The form the command string takes is as follows: **d dmapassword <other options ...>** For more details about this command string, check out the next sections of this chapter of the manual.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

It's strongly suggested that, should you run a DMA Server next to your MasterBBS, you should never let your users enter the Rlogin module without using a pre-programmed Rlogin page.

Set Master Key access to the DMA Server

Setting **DMAMAST to YES in TCPLIBM.MSG, level 3 accounting and security** will allow people holding the Master Key on the main BBS to have MASTER access to your DMA Server. If you're running your DMA server strictly for your own BBSes use, this is fine. However, if you're planning on granting access to your DMA Server resources to other BBSes on the net, DMAMAST should be set to NO, to prevent the sysops of those systems from tampering with your DMA Server's configuration. In any event, be very careful about who you give MASTER access to your DMA server.

Configure the DMA Access control file for multiple MasterBBS access

If you decide to offer access to multiple MasterBBSes (you want to create a Game-Net) to your DMA Server, it needs to be able to tell one system apart from another. We accomplish this by using an access control file that contains the IP address of the MasterBBS, and the one-character suffix the MasterBBS will be using to access your server. This prevents systems from using other system's prefixes. Some systems may have multiple prefixes so there's nothing wrong with having multiple prefix entries in here for a given IP address.

The file should be named **TCPDMACT.TXT**. The format of the file is:

```
# This is a comment.  Lines beginning with # are comments.
<IP address #1> <Prefix #1>
<IP address #2> <Prefix #2>
<IP address #3> <Prefix #3>
... so on and so forth
```

Example:

```
199.84.216.45 A
180.23.16.5 B
205.240.12.6 C
205.240.12.6 D
```

In this example, the first two system have a unique prefix. In the case of the 205.240.12.6 IP address, we have two prefixes assigned to this system.

MajorTCP/IP checks this file every 5 minutes for any changes. Once loaded, you should see a message in your DMA Server audit trail **"TCPLIB-DMA-I Loaded x Records".**

Experimental Option #1

If you put the word **DMAIPLOK** (Level 1, Special Configuration Options, **TCPLIBM.MSG CFGTXT00** to **CFGTXT09**, on the ***DMA Server***), an account will be allowed to log only if the account's address 3 field (can be edited in the user account editor) contains an IP address that matches the IP address of the caller. If the address 3 field doesn't match the IP address, the user will see "failed DMA login" and a message will be printed in the audit trail on the ***DMA Server***. If the address 3 field does not contain an IP address, or the **DMAIPLOK** is not enabled, then this is ignored. Note that starting with **DMA2.0**, the ***DMA Server*** automatically puts the IP address of the caller when creating the account in the address 3 field.

Experimental Option #2

If you put the word **DMAOLDRM** in one of the **TCPLIBM.MSG**, **Level 1 Special Configuration Options (CFGTXT00 to CFGTXT09) (on the DMA Server**), the DMA Server will automatically flag an account for deletion, (and print a message in the audit trail), if the creation date of the account on the **MasterBBS** is newer by more than 2 days than the creation date of the account on the **DMA Server**. Note that accounts that are exempt from deletion are exempted there too.

Configure the MSG files on the DMA Server

Before changing the configuration options on the DMA Server listed below, make sure that you can create new accounts on your **DMA Server**, and that they end up in a class that will give them access to all public features of the **DMA Server**. You should set accounts to be deleted after a certain period of non-usage.

Configuration Options to change on the DMA Server

- Set **ASKBDY** to **NO** in **BBSSUP.MSG**, **level 4 configuration** options.
- Set SUBBS to **YES** in **TCPLIBM.MSG**, **level 4 configuration** options.
- Set **DMASEQ** to the **sequence number** of your DMA Server if you are running multiple servers. If not, leave it to the default of 01. Each DMA Server you run has a different sequence number which generates a different activation code. DMASEQ is in TCPLIBM.MSG level 4 configuration options.
- Set **DMACODE** in **TCPLIBM.MSG, level 3 accounting and security** to the 8 character DMA 2.1 Server activation code you received for your DMA 2.1 server when you purchased the package.

Configuration option changes specific to MajorBBS 6.25

- Set **DFTPR2** to **NOTIFY** in GALMS.MSG, level 4 Configuration options.
- Set **SUPU2S** to **NO** in GALMS.MSG, level 4 Configuration options.
- Set **SUPE2U** to **NO** in GALMS.MSG, level 4 Configuration options.

Configuration option changes specific to Worldgroup

- Set **DFLONP** to **NEVER** in GALME.MSG, level 4 configuration options.
- Set **SUPU2S** to **NO** in GALME.MSG, level 4 configuration options.
- Set **SUPE2U** to **NO** in GALME.MSG, level 4 configuration options.
- Set **CLISRV** to **NO** in BBSMAJOR.MSG, level 4 configuration options.

NOTE: You should disable all **MajorTCP/IP** modules that you are not using on the **DMA Server**. A minimal configuration would be to have only **TCPLIB** enabled. That's the only module required on the **DMA Server**

Configure the MSG files on the MasterBBS

If you are sending more than one **MasterBBS** into the same **DMA Server** change **SGNUSZ** on the **MasterBBSes** to **27** in **BBSSUP.MSG, level 4 configuration**. You should also change **MAXCAT in BBSMAJOR.MSG, level 4 configuration to 20 at least.** Finally, you might want to set **DMALANG to YES in TCPRLGN.MSG, level 4 configuration** if you are connecting to a DMA server owned by someone else and are unsure of which language to use on login.

Install/Move modules from the MasterBBS to the DMA Server

- Just copy/install the module files over to the **DMA Server**. You may have to call the authors of the software to have the module transferred to the new **MajorBBS** registration number of the **DMA Server**. No Specific configuration changes are required for **DMA Server** operation. If the module has a configuration option for **DMA** or **SubBBS**, set that to NO. That was used with **DMA 1.0**.

- Create a Module page in the menu tree of that **DMA Server** that will point to the proper module. On **WorldGroup** systems, make sure you create this page in the "Terminal Mode" menus. This page must be accessible to users that are created on the **DMA Server**. This page can be an orphan page or can be attached to the menu tree.

- Start the **DMA Server**, log from the console, and make sure the module is working fine. Try it by logging into one of your test users that does have sysop privileges.

Setup the link from the MasterBBS to the DMA Server

Create an RLogin module page in an appropriate place in your menu tree, in both the Terminal and C/S mode if you are running WorldGroup. Protect it with the key your users must have to enter this module. Put the name of the module that you'll be using on the ***DMA Server*** as the name or description of that page to help users know what this page do.

Use the following procedure to create the Rlogin page on the MasterBBS

- From the main configuration menu (CNF), select **F2 - Design Menu Tree**
- Make sure that the menu item cursor is located in the menu you will create the option in.
- Select **F2 Edit** to change that menu page.
- Go to the menu options area and **add a new option**, say [T] for TradeWars (example)
- In the **EDIT OPTION** window ...

  - Short Description ..... could be “[T] Enter Trade Wars”
  - Key required for this option..... Lets say **NORMAL (or PAYING)**
  - Destination page..... could be called **TRADEWARS**
  - **Save the menu**. A new page in the menu tree should’ve been created.
- Move the cursor to the new page called **TRADEWARS.**
- Press **F2 Edit** to configure this module page.
  - Allow go to this page ..... should be set to **YES**
  - Key required ..... **NORMAL or PAYING.**
  - Select module window, you should chose the **RLogin Module**
  - Display header ..... should be set to **YES**
  - **The command string should be composed as below ...**
  - Save the resulting page.
- That’s it!

Details about the command string.

Enter a Command String in the page, using the following format:

d dmapassword suffix ipaddress luser ruser autolof autospc echo mode gopage #desc

d	Indicates DMA2.1
dmapassword	Value of DMAPWD on the destination **DMA Server**
suffix	Suffix of your BBS for multiple **MasterBBS**->**DMA Server** relationships. Set to 0 for no suffix.
ipaddress	IP (numeric) address of **DMA Server**
luser	Not used. Set to "." (just a period).
ruser	Username the user should log into on the remote system. Usually set to %u
autolof	If user should be automatically logged off from the **DMA Server** and brought back to the main BBS when he exits the module he was sent into. Usually set to Y.
autospc	Automatically turn the RLogin extended special commands off upon entering the module on the **DMA Server**. **Usually set to Y**.
echo	Determine the way the echo will be processed on this connection. **If set to Y**, echo is generated by the DMA Server. Usually set when mode = Binary or permanent binary. **If set to O**, echo is generated by the **MasterBBS**. Usually set when mode = Ascii. **If set to N**, the **DMA Server** will use whatever default echo is set for the **DMA Server**.
mode	**A** = Ascii. Used for line-based module, modules that always wait until you hit enter before processing the command. Example: Most RPG games like TeleArena, CrossRoads. This mode has the advantage of fast echos and also any globals the user type is executed on the **MasterBBS**. So they can still page and be paged from the **MasterBBS**.

	B = Binary. Modules that process keys one at a time, like the full screen editor, chatting, All commands typed are processed by the **DMA Server**. Pages, globals. In other words, everything takes place on the **DMA Server**. User is set to BUSYmode on the main BBS. **P =** Same as B, but permanent, 8 bit clean. Used for file transfers and modules like TW2002. Echo should usually be set to O or N for this mode.
gopage	Page that will be executed on the **DMA Server**. This must be a module page. (no menu or file pages). User must have access to this page.
#desc	Description that will appear in the online users listing on your **MasterBBS** if you use the TCP_RL_MOD or TCP_RL_MOD2 text variables in your global handlers on the **MasterBBS**.

Some examples:

TeleArena
d dmapassword 0 111.111.111.111 . %u y y o a TA #TA_5.6

TradeWars
d dmapassword 0 111.111.111.111 . %u y y y p TW2002 #TW2002

FileLibrary
d dmapassword 0 111.111.111.111 . %u y y y p LIB #Library

Additional Notes

We added a new special configuration option **DMASTRICTCT**. When enabled, it requires that the **TCPDMACT.TXT** file be used and the IP address and suffix of the calling DMA client be listed there. (The default was that if it isn't there, any suffix would do).

Another new special configuration option, **dmanoascpause** will disable screen pausing during ASCII sessions.

To activate these features, all you need to do is go to **level 1 hardware configuration**, in **TCPLIBM.MSG**. Look for the first empty **CFGTXT** option (ranging from CFGTXT00 to CFGTXT09) and put in the **DMASTRICTCT** or **dmanoascpause** word there.

ANNEX

MAJORTCP/IP PERFORMANCE OPTIMIZATION

Basic system optimization

It is very hard to make performance recommendations, as no two systems serve the same purpose, run the same modules, use the same hardware, etc.

The solution to this is to explain the theory and give guidelines, instead of firm recommendations. Vircom does not guarantee any of the information below will have any impact on your system.

Before making any modification to your .MSG files, you should of course make a backup. You can zip TCP*.MSG or copy them to a sub-directory, for easy retrieval in case some changes made things worse than better.

It is obvious that any Internet client or server of MajorTCP/IP that has a rating in the number of concurrent users/sessions will have an impact on performance. This text assumes you have already configured these settings appropriately.

The objective of this primer is to explain the foggier configuration elements of the MajorTCP/IP message files.

TCPLIBM.MSG / Level 1 config

MSS This is used to control the number of bytes in each TCP packet. If you want to optimize your system for telnet or IRC traffic, you should reduce it to a value between 512-1024. If you're connected via a PPP/SLIP dial-up link to your provider, you can reduce this to a value between 256 and 512 even. (If your provider refers to "MTU" for your dial-up connection, this MSS is used to compute your system's MTU.)

A larger value increases the amount of data that can be transferred in each packet. Each packet has a header, thus a very short amount of time associated with their management. Larger packets reduce the impact of the overhead of TCP packets, hence increasing performance for file transfers. The drawback is that small packets, like telnet and IRC, have to wait longer in the queue before they can be processed. So if the emphasis of your system is on telnet/irc, packet sizes should be smaller while if the emphasis is on FTP, packet size should be larger.

This has no impact on PPP/SLIP traffic

TCPNEBUF By default 50, it should never be smaller than this value. This is the number of packets "Cache" so to speak. If you have lots of net-usage on your system, it's quite possible for MajorTCP/IP to run out of buffers when processing incoming and outgoing TCP/IP packets. Loss of packets due to insufficient buffers forces the target site to re-send them, thus slowing down your bandwidth. Increasing TCPNEBUF to 80, 100, or up to 200 can alleviate these problems. Each buffer uses 2k of RAM.

TCPLIBM.MSG / Level 4 config

DNSTMO This represents the number of seconds to wait after sending a DNS query to a name server. 15 would be too short for slower or congested links/name servers. As a timed-out DNS query switches to the secondary name server and re-issues that query, it would be advisable to watch for switches in DNS in the audit trail. If it happens too often, this value should be raised. It shouldn't be set above 60, as that would force the user to wait for 60 seconds if a legitimate problem happened with the DNS servers.

NBRES This is the number of DNS queries that can concurrently active at the same time. If your DNS servers are slow to answer, you could run out of those. As a rule of thumb, 1 buffer per 10 channels should be sufficient in most situations.

TICKMS By Default 40. The represent the length of time, in milliseconds, that MajorTCP/IP's stack can process data before it must again relinquish the control back to the Worldgroup main executive. Setting this value larger than 125 is risky, as it would mean other modules would have to wait up to 125ms (under heavy network load) before they can run a cycle. If another module is very timing sensitive, this could effectively compromise the stability of the system.

This is used to prioritize TCP/IP networking vs all other modules on the system. Recommended settings vary between 40 and 100.

***** Adjust with care, and by small increments *****

LOGWRT Set it to NO. This will leave the log files open, thus generating less disk I/O (as buffers and write cache will reduce the number of physical writes to the disk). Opening & closing files have a very negative impact on system performance.

TCPSLIP.MSG / Level 4 config

SLIPPRIO By default 10. It represents more or less the number of SLIP & PPP packets that will be processed in a single cycle (before relinquishing the control to the main executive). Setting this to 0 tells MajorTCP/IP to process *ALL* packets in the queue before relinquishing control. This really optimizes the PPP/SLIP server, but is a dangerous option if there are other modules running on the system that are timing-sensitive.

***** Adjust with care, and by small increments *****

SLIPFORN
SLIPFORE Set them to NO. This will reduce the disk I/O generated by someone who is using a script that does not capture the dynamically assigned IP address. This is actually a messy way out of the problem, as the user may experience other kinds of problems by using the wrong IP address. The real solution is to track these people down and equip them with the proper script so it captures the IP address properly.

SLIPTRL Set it to NO. This will remove the PPP START/END messages from the audit trail, reducing disk I/O, thus increasing overall performance. The drawback is the lack of auditing both for accounting and debugging purposes.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

TCPSMTP.MSG / Level 4 config

SMTPMAXO Set it to 1. This represents the number of concurrent outgoing email your SMTP server will process. Unless your system has an unusually high volume of outgoing email traffic, delaying an email a few minutes is preferable to swallowing the resources to get it out faster.

SMTPMSS Like the level 1 option MSS, this option determines the maximum number of bytes in each TCP packet. If you want to reduce the impact of SMTP traffic, you could set this to a lower value. If you are more concerned with getting the emails processed rapidly, set it to a larger value.

The maximum MSS of the SMTP server is limited by the global MSS, configured in level 1 (cf above).

SMTPHEAD Setting this value to anything else than 0 will record the SMTP header at the beginning of the body of incoming emails. This could be useful information for the reader, but in the most case it is just "noise" that could be done away with. Setting it to 0 will strip each email of its SMTP header, thus reducing the quantity of information written to disk.

SMTPLOG Set it to NO. This will remove all SMTP entries from the TCP/IP log file. The drawback is a lack of auditing for debugging purposes.

OUTCYC By default, this value is set to 30 seconds. An outgoing cycle generates disk I/O by looking at the queue of emails waiting to be processed. If you increase this field, you will tell the SMTP server to wait longer before checking if it must send an outgoing email.

***** Adjust with care, email backlog could build up *****

SMTPMXOC This is the number of emails to attempt to process within a single cycle, as defined in the above option. If you increase this to a value above 1, then your SMTP server will be processing emails faster, but also generate more disk I/O, thus slowing down the overall performance.

DBUGLVL This field is only relevant if you have your debugging turned on (see SMTPLOG above). If you do, this controls the amount of information that will be put in the log file for each email, 9 being the most, and 0 being none. If you need at least some SMTP information in your log, then tune it down to minimum level you can. Operating your system with this at 9 generates much more disk I/O than necessary (unless you are trying to track down a SMTP problem).

SMTPGPR By default, this value is set to 2. Increase it to spread out E-mail importing into the Galacticomm mail subsystem. Try values of 5, 10, so on and so forth. This is again, to reduce the load on the system due to disk I/O.

MAXISIZE You should put a limit to the size of incoming mail (including attachment). This would make sure you don't get users using E-mail for File Transfers of unreason-able size, hence tying up bandwidth and hitting SMTP processes unduly. A value of 1000 is equal to 1MB.

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

TCPPOP3.MSG / Level 4 config

POP3MXBU Emails on WG/MBBS are not stored in the same flat-file format as on Unix systems. That means any time a POP3 mail program requests the emails, it must go through a procedure to build this flat-file to transfer over to the POP3 mail agent. This is idle time between the moment the POP3 mailer asked for the emails and the time your system delivers it to them.

If your users are complaining their POP3 program are "timing out", then you may want to reduce this amount, forcing the POP3 server to start sending emails faster. This may adversely result in fewer emails being sent in each drop though. You could also instruct your users to increase the time-out setting of their POP3 programs, if it is configurable.

The "normal" range of this value is between 30 and 45 secs.

POP3LOG Set it to NO. This will remove all POP3 entries from the TCP/IP log file. The drawback is a lack of auditing for debugging purposes.

DBUGLVL This field is only relevant if you have your debugging turned on (see POP3LOG above). If you do, this controls the amount of information that will be put in the log file for each pop3 request, 9 being the most, and 0 being none. If you need at least some POP3 information in your log, then tune it down to minimum level you can. Operating your system with this at 9 generates much more disk I/O than necessary (unless you are trying to track down a POP3 problem).

TCPNNTPD.MSG / Level 4 config

NNTPMAX Set it to 1. Some ISP's have multiple news servers, who may attempt to feed you news at the same time. It is probably better to make the second news server wait, than getting the performance hit of two concurrent feeds.

NNTPEDLY Set it to 30. This is the interval (in minutes) to wait before checking for messages posted locally that need to be sent out on Usenet. It is better to have fewer checks (ie: disk I/O's).

NNTPMSS Like the level 1 option MSS, this option determines the maximum number of bytes in each TCP packet. If you want to reduce the impact of NNTP traffic, you could set this to a lower value. If you are more concerned with getting the news processed rapidly, set it to a larger value.

The maximum MSS of the NNTP server is limited by the global MSS, configured in level 1 (cf above).

NNTPLOG Set it to NO. This will remove all NNTP entries from the TCP/IP log file. The drawback is a lack of auditing for debugging purposes.

DBUGLVL This field is only relevant if you have your debugging turned on (see NNTPLOG above). If you do, this controls the amount of information that will be put in the log file for each news feed, 9 being the most, and 0 being none. If you need at least some NNTP information in your log, then tune it down to minimum level you can. Operating your system with this at 9 generates much more disk I/O than necessary (unless you are trying to track down a NNTP problem).

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

IMPCYC This sets the interval (in seconds) before the NNTP server will check its batches to see if it has articles to import in the local newsgroups. It is rare for news servers to exchange articles faster than once every 15 minutes, so it would be redundant to check more than once every ten minutes.

IMPSLOW You can increase this field to spread out the impact of importing news article into the Galacticomm forums. Try values of 5, 10, so on and so forth. This is again, to reduce the load on the system due to disk I/O.

DFTEXPY If your provider has multiple news server, the same news article could be submitted to your system by each server. To prevent posting it multiple times in the newsgroup, a history file is maintained. If your provider is using only one news server to feed you, you can set this to the minimum value to reduce the size of the history file. In any case, it is rare for the same article to be submitted to a news server with an interval over 48 hours, so this field should be set to 3-4 to be fairly safe.

TCPIRC.MSG / Level 3 config

DCCKEY You might want to restrict DCC transfers altogether. These munch up bandwidth like FTP transfers do.

TCPIRC.MSG / Level 4 config

LSTMIN Set it to 8-10 users instead per channel. This will reduce the load on your bandwidth when MajorTCP/IP tries to update the internal IRC channel list. Default is 5.

LSFREQ Update the list less often by increasing the value to 1800 seconds. Less impact on bandwidth. Default is 1200.

TCPFTPD.MSG / Level 4 config

FTPDMSS Like the level 1 option MSS, this option determines the maximum number of bytes in each TCP packet. If you want to reduce the impact of FTP traffic, you could set this to a lower value. If you are more concerned with getting the FTP requests processed rapidly, set it to a larger value.

The maximum MSS of the FTP server is limited by the global MSS, configured in level 1 (cf above).

FDAGET
FDAPUT
FDAFOP If you don't care on getting an audit of who has transferred files over FTP, then setting these to NO will stop the FTP server from logging the operations in the audit trail, reducing disk I/O (thus increasing overall performance).

TCPFTP.MSG / Level 4 config

FTPMSS Like the level 1 option MSS, this option determines the maximum number of bytes in each TCP packet. If you want to reduce the impact of FTP traffic, you could set this to a lower value. If you are more concerned with getting the FTP requests processed rapidly, set it to a larger value. The maximum MSS of the FTP client is limited by the global MSS, configured in level 1 (cf above).

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

TCPWEB2.MSG / Level 4 config

WEB2MSS Like the level 1 option MSS, this option determines the maximum number of bytes in each TCP packet. If you want to reduce the impact of WWW traffic, you could set this to a lower value. If you are more concerned with getting the WWW requests processed rapidly, set it to a larger value.

The maximum MSS of the Web2 server is limited by the global MSS, configured in level 1 (cf above).

AXSFIL
AGTFIL If you are not interested in generating statistics from the hits on your WWW server, then you could disable the logging of these information. The drawback is a lack of auditing for debugging purposes.

ERAFIL You could disable the error log as well, if you are really in a crunch for performance. This is dangerous as configuration errors on your Web2 server could go on for months without being noticed...

Performance optimization and Buffer Sizes

POP3, FTPD and WEB2 can now have their data transfer sockets buffer size configured. A larger buffer size will increase the performance of a data transfer over a slow (or laggy) link.

POP3: **POP3OBSZ in TCPPOP3.MSG**, **level 4** configuration options.
FTPD: **OBUFSIZ in TCPFTPD.MSG, level 4** configuration options.
WEB2: **OBUFSIZ in TCPWEB2.MSG, level 4** configuration options.

Generally speaking, the larger the round trip time of a packet, the more advantages you'll get from a larger buffer size. The default is 2048, which is what MajorTCP/IP was set to in the past.

You should probably increase by increments of 1K, or just use fixed values like 2048, 4096, 8192, 16394.

We've done some performance testing using FTP over a local Lan and a 128K ISDN compressed link. Over the local LAN, there was no performance increase when using a buffer size of 16K instead of 2K.

Over the ISDN link, the data transfers (both directions) were TWO to THREE times faster when using 16K buffers. We have not tested this over a PPP link.

Note that the tradeoff is that allocating more buffers does take more memory.

For example, if you have 20 concurrent WWW connections, increasing the buffer size from 2K to 16K will make WWW use 280K more of memory during the transfers (and only during the transfers). So it’s a good idea to tweak these values with the most extreme care.

[Vircom Inc’s MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

IRC SERVERS

EFnet IRC Servers

irc.cerf.net	irc.cnde.iastate.edu	chat.btinternet.com
eff.org	irc.ecn.uoknor.edu	irc.fi
irc.digex.net	irc.mo.net	irc.uib.no
irc.stanford.edu	irc.ecn.bgu.edu	irc.hitos.no
irc.aol.com	irc.colorado.edu	irc.pvv.unit.no
irc.uci.edu	irc.winternet.com	irc.ifi.uio.no
irc.frontiernet.net	irc.ilstu.edu	irc.powertech.no
irc.netcom.com	irc.cdc.net	sil.polytechnique.fr
irc.netcom.net.uk	irc.law.emory.edu	irc.enst.fr
irc.tw	irc.umn.edu	IRC.Eurecom.FR
irc.caltech.edu	irc.magic.mb.ca	irc.Univ-Lyon1.FR
irc.blackened.com	portal.mbnet.mb.ca	irc.wu-wien.ac.at
irc.best.net	irc.cs.mun.ca	uni-linz.ac.at
irc.bridge.net	irc.ais.net	itc.univie.ac.at
irc.ibm.net.il	irc2.ais.net	sunsite.auc.dk
irc.ac.il	irc.mcs.net	irc.nijenrode.nl
irc.voicenet.com	irc.io.org	irc.sci.kun.nl
irc.cs.rpi.edu	irc.calpoly.edu	irc.ic.ac.uk
irc.primenet.com	irc.rutgers.edu	irc.abdn.ac.uk
irc.portal.com	irc-2.texas.net	serv.cs.man.ac.uk
irc.columbia.edu	piglet.cc.utexas.edu	irc.be
irc.texas.net	anarchy.tamu.edu	dismayl.demon.co.uk
irc.phoenix.net	irc2.magic.ca	irc.it
irc.ionet.net	irc.vianet.on.ca	irc.span.ch
irc.neosoft.com	irc.stealth.net	irc.si
irc.gate.net	irc.pitt.edu	irc.felk.cvut.cz
irc2.uiuc.edu	joyce.eng.yale.edu	irc.cis.vutbr.cz
irc.cris.com	azure.acsu.buffalo.edu	irc.xs4all.nl
irc.umich.edu	irc.usa.pipeline.com	irc.ru
irc.mcgill.ca	irc.jp	irc.isnet.is
elk.nstn.ca	irc.se	irc.mimuw.edu.pl
irc.yorku.ca	irc.bt.net	irc.lublin.pl
irc.epix.net	irc.easynet.co.uk	irc.agh.edu.pl
irc.uiuc.edu	london.uk.pi.net	irc.put.poznan.pl

[Vircom Inc's MajorTCP/IP Installation Manual, © Copyright 1997 Vircom Inc.]

Undernet IRC Servers

montreal.qu.ca.undernet.org	ann-arbor.mi.us.undernet.org
Chicago.IL.US.Undernet.org	washington-r.dc.us.undernet.org
Chicago-1.IL.US.Undernet.org	SanDiego.CA.US.Undernet.org
Vancouver.BC.CA.Undernet.Org	washington.dc.us.undernet.org
channels.undernet.org	washington-1.dc.us.undernet.org
Uworld2.undernet.org	washington-2.dc.us.undernet.org
London.Uk.eu.Undernet.org	washington-3.dc.us.undernet.org
joplin.mo.us.undernet.org	washington-4.dc.us.undernet.org
Manhattan.KS.US.Undernet.Org	washington-8.dc.us.undernet.org
Austin.TX.US.UnderNET.ORG	washington-7.dc.us.undernet.org
Blacksburg.VA.US.Undernet.Org	washington-6.dc.us.undernet.org
StLouis.MO.US.UnderNet.org	washington-5.dc.us.undernet.org
lowell.ma.us.undernet.org	Santiago.CL.undernet.org
auckland.nz.undernet.org	Pittsburgh.PA.US.undernet.org
toronto.on.ca.undernet.org	Amsterdam.NL.EU.undernet.org
hamilton.on.ca.undernet.org	Espoo.Fi.Eu.UnderNet.Org
SanJose.CA.US.Undernet.Org	Ljubljana.Si.Eu.undernet.org
Norman.OK.US.undernet.org	Caen.Fr.Eu.UnderNet.org
okc.ok.us.undernet.org	Lulea.se.eu.undernet.org
channels2.undernet.org	Diemen.NL.EU.undernet.org
Uworld.undernet.org	phoenix.az.us.undernet.org

DALnet IRC Servers

phoenix.tx.us.dal.net	davis-2.ca.us.dal.net	glass.oh.us.dal.net
toronto.on.ca.dal.net	davis.ca.us.dal.net	toronto2.on.ca.dal.net
igc.fl.us.dal.net	rutgers.nj.us.dal.net	mis.ky.us.dal.net
services.dal.net	cin.il.us.dal.net	mindijari.ca.us.dal.net
groucho.ca.us.dal.net	skypoint.mn.us.dal.net	xgw.fi.dal.net
dragon.ut.us.dal.net	ohana.hi.us.dal.net	usd.sd.us.dal.net
uncc.nc.us.dal.net	megasoft.wa.us.dal.net	liberator.uk.dal.net
zhaneel.ia.us.dal.net		

Pseudo Keys and Text Variables

PSEUDO KEYS

Pseudo keys can be used with autoselect menus. Consult the MajorBBS/ Worldgroup Sysop's manual to know how to learn how to use autoselect menus.

Key Name	Function
_TCP_ISLIP	Flag that indicates that the current channel is using the SLIP/CSLIP/PPP server (Returns TRUE if the current usernum is in SLIP/CSLIP/PPP mode) This pseudo key is only used by modules programmed to interact with our SLIP/PPP server.
_TCP_ISTELNET	This pseudo key returns a value of TRUE if the current user is in via an incoming Telnet/RLogin call.
_TCP_RL_HIUID	This pseudo key returns a value of TRUE if the current user defined an internet alias using the Rlogin alias page (see the Rlogin section of this manual)
_TCP_CIP#nnn	Used with MultiHoming, to find out if the user came in on a specific IP address. nnn = last digit of the IP address from 1 to 254. (see the Multi-Homing section of this manual). Returns TRUE if the person is coming in via the IP address refered to by nnn.

TEXT VARIABLES

Text variables are used to display various information about the user currently logged-in and other information supplied by MajorTCP/IP. Consult the MajorBBS/ Worldgroup Sysop's manual to know how to learn how to use text variables in text blocks under CNF 6.

Variable Name	Description
TCP_MAILFROM	Shows what hostname.domainname will appear in internet E-mail sent by this user. Works with SMTP Multi-Homing too.
TCP_SLIP_U1	Used by modules that interact with our SLIP/CSLIP/PPP server (Real User ID of SLIP/CSLIP/PPP user based on usrnum)
TCP_SLIP_U2	Used by modules that interact with our SLIP/CSLIP/PPP server (Real User ID of SLIP/CSLIP/PPP user based on othusn)
NOW_HTTP	Used Internally by the Web2 server. Return the current date/time in HTTPD format.
WEBD_VERSION	Used Internally by the Web2 server, return the version of MajorTCP/IP.
HANGUP	Used sometimes on the DMA Server. If one tries to print this text variable, this tells the BBS to hangup the current channel.
TCP_IP	IP Address of incoming telnet/rlogin caller (IP address he calls from)
TCP_CALLED_IP	IP Address incoming telnet/rlogin caller called (used with Multi-Homing)
TCP_IDENTD	IDentD text we received for current user.
TCP_IP_PORT	TCP Port the incoming telnet/rlogin user called from
TCP_HOSTNAME	Content of TCPLIBM's level 1 HOSTNAME
TCP_DOMAINNAME	Content of TCPLIBM's level 1 DOMNAME
TCP_RL_IUID	Internet Alias of current user
TCP_RL_MOD	Used with DMA (and DMA for ICO) for module name substitution (based on othusn)
TCP_RL_MOD2	Used with DMA (and DMA for ICO) for module name substitution (based on usrnum)
TCP_BASE_IP	Used to display the current base IP address of the BBS.