MajorTCP/IP

TCP/IP Connectivity Software

for The MajorBBS and Worldgroup

by Vircom Inc.

Installation Guide
(Advanced Features addendum)

1997
v2.20-X

[Vircom Inc's MajorTCP/IP Advanced Features Addendum, © Copyright 1997 Vircom Inc.]

TABLE OF CONTENTS

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.

Last revised June 3rd, 1997

- Added Email alias Filter. You define an alias filter file in **ALSSPCF** (TCPSMTP.MSG, level 4 config). This file is reloaded automatically every 5 minutes. Usefull for multi-homing. Check in the SMTP section of the manual for more details. The main function of this alias filter is it lets you do something like this:

  sales@domain1.com sales_domain1
  sales@domain2.com sales_domain2
  sales@yourdomain.com sales_yourdomain

  As you can see, you can now have more than one "sales" account on your system, with each one pointing at a different "real" user. SMTP will redirect email to the appropriate account as per the settings of the alias file.

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.

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 YES and IMGLOC to YES** 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.

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.

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.

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.

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

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.

[Vircom Inc's MajorTCP/IP Advanced Features Addendum, © Copyright 1997 Vircom Inc.]

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 Advanced Features Addendum, © 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 4** configuration options 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 Advanced Features Addendum, © 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 revised october 9th, 1997

- Accounts created on the DMA server via a DMA connection will have their birthdate set to 01/01/01.
- 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.

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.

The DMA password is case sensitive, so make sure that the DMA password used in the Rlogin string used on the main BBS matches exactly, including case, the password set in the DMAPWD field in TCPLIBM.MSG, level 3 configuration of the DMA Server.

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.

[Vircom Inc's MajorTCP/IP Advanced Features Addendum, © Copyright 1997 Vircom Inc.]

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. Warning: This password is case-sensitive, make sure that it matches exactly the value in DMAPWD on the DMA Server, including case.**
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**.

[Vircom Inc’s MajorTCP/IP Advanced Features Addendum, © Copyright 1997 Vircom Inc.]

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.

[Vircom Inc's MajorTCP/IP Advanced Features Addendum, © Copyright 1997 Vircom Inc.]

Advanced Features: HTML parsing for TCPWEB2

Overview

HTML parsing is the latest feature added to MajorTCP/IP's web server. The essence of it is that TCPWEB2 will scan HTML files matching specific conditions to replace variables with text. The text can come from several different sources:

- **Generic text variables:** information provided before the page to parse is called up.
- **BBS text variables**: lets you display any text variable in MBBS/Worldgroup.
- **Special-case variables**: used for specific purposes, like ACTIVE-X telnet autologins.

In order for a HTML file to be parsed in this way, the following conditions must be met:

- **PARSENAB** in **TCPWEB2.MSG**, level 4 configuration must be set to **YES.**

- **PARSEURI** must be set to a directory under the current webpages directory specified in WEB2PATH under TCPWEB2.MSG, level 4 config. For instance: if we assume that **WEB2PATH** is set to the default **/wgserv/tcpweb2**, which means **web pages** reside under **/wgserv/tcpweb2/webpages** ... if you set **PARSEURI to /parse.dir/ (the default setting),** pages that will need parsing will be under **/wgserv/tcpweb2/webpages/parse.dir/.**

- The page to be parsed must have a **.SHT** extention.

What is the reason for the directory specified in **PARSEURI?** It was felt that if we just parsed any **.SHT** files, any user-webpage management software would allow users to use the parsing. This power shouldn't be put in any ordinary user's hand, since the accessible text variables can include some that are sensitive in nature. Furthermore, trying to parse a non-existent text variable can cause a GP. So you should protect the PARSEURI directory to prevent people from accessing it from the web. In the example above, you would want to add an entry in your **access.ctl** file like: **parse.dir/.**

NOTE: The resulting output from the .SHT scanning/parsing MUST NOT EXCEED 16K. TCPWEB2 does an in-memory scan and the maximum buffer size for TCPWEB2 is 16K.

Variable types available

A page that is eligible to be parsed will first be scanned by TCPWEB2 for "variables" that need to be replaced. A variable is specified by enclosing it between curly braces {}. Variables can be ANYWHERE in the .SHT file and they will be replaced with the text associated to the variable.

Generic text variables

Generic variable can be defined on the fly on the parent page and passed to a destination page that will be parsed by TCPWEB2 via a special URL**.. These variables use the prefix wv! before the variable name on the destination page.** Generic variables are used to create a single child page that changes depending on which button a person clicks on the parent page. This avoids having to create a separate child page for each URL selected if the function of the destination page is always the same.

Lets say for instance that you want to create a page with links to different MUDs (multi-user dungeons). You want this page to call up another page that will do the telnet itself, with a small description on the top of the page telling the user where he's being telnetted to, without having to create a separate "telnet" page for each MUD.

Normally ... the links on the calling page would look like this:

```
<a href="http://www.domain.com/sendmud1.htm">Go to SuperMUD page</A>
<a href="http://www.domain.com/sendmud2.htm">Go to OrdinaryMUD page</A>
<a href="http://www.domain.com/sendmud3.htm">Go to KiddyMUD page</A>
```

And then, you'd need to create a page for each MUD that would essentially display say, the name of the MUD, a description and the telnet link to the MUD itself.

```
This link should carry you to the awesome SuperMUD Multi-User Dungeon.  If you
don't have a telnet client, you can find one on the <a href="http://www.tucows.com>tucows</a> website.<P>
<a href="telnet:supermud.com 2222">click here to telnet to SuperMUD</A>
```

Overall, in this example, you'd need to create parent page (the main page) and three child pages, one for each MUD. This isn't very efficient.

Using HTML parsing, you could create the parent page with the following links instead:

```
<a href= "http://www.domain.com/parse.dir/sendmud.sht?host=supermud.com%202222&name=SuperMUD>
Go to SuperMUD page </a>
<a href= "http://www.domain.com/parse.dir/sendmud.sht?host=ordinarymud.com%202222&name=OrdinaryMUD>
Go to OrdinaryMUD page </a>
<a href= "http://www.domain.com/parse.dir/sendmud.sht?host=kiddymud.com%202222&name=KiddyMUD>
Go to KiddyMUD page </a>
```

As you can see in the special URL, we always call the same page, namely SENDMUD.SHT. The extra stuff after the question marks (?) would then be passed to the SENDMUD.SHT page under the /parse.dir/ directory.

In SENDMUD.SHT, you would find:

```
This link should carry you to the awesome {wv!name} Multi-User Dungeon.  If you
don't have a telnet client, you can find one on the <a href="http://www.tucows.com>tucows</a> website.<P>
<A HREF="telnet://{wv!host}>Go to {wv!name}</A>
```

So now, all you have is the parent page and one child page: sendmud.sht. That's two pages less than the original example. This is just one small sample of what can be done with generic variables.

Lets look at the URL from the parent page more closely:

http://www.domain.com/parse.dir/sendmud.sht?host=supermud.com%202222&name=SuperMUD

http://www.domain.com/parse.dir/sendmud.sht calls up the sendmud.sht web page to be parsed.

The **?** (question mark) separates the parameters to be passed to the sendmud.sht page from the beginning of the URL. Everything after the question mark identifies the parameters to pass. The & (ampersand) is used to separate each parameter, and the %20 is used to insert a space in the parameter.

For instance, to access the SuperMUD, you need to do a telnet to supermud.com on port 2222, which would look like **supermud.com 2222**, but since you can't put a space in a URL, you modify the line by replacing the space with %20. The host becomes supermud.com%202222.

host=supermud.com%202222 assigns the value **supermud.com 2222** to the variable **host**

name=SuperMUD assigns the value SuperMUD to the variable **name**

When someone clicks on the URL, what happens then is we call up sendmud.sht with host=supermud 2222 and name=SuperMUD. The sendmud.sht gets called and parsed by TCPWEB2. It replaces the

{wv!name} with SuperMUD and **{wv!host} with supermud.com 2222.** The result on the user's screen would look like so:

This link should carry you to the awesome SuperMUD Multi-User Dungeon. If you don't have a telnet client, you can find one on the **tucows** website.

Go to SuperMUD

Essentially, this lets you create pages that change depending on what URL a person clicks.

BBS text variables

HTML parsing lets you create special web pages that can examine or display information available from various BBS text variables. For instance, when running Radius (another vircom product) with MajorTCP/IP, a text variable is available that lets you see who is connected to the terminal servers called TCPRAD_SHOWUSR. HTML parsing makes it possible to create a web page that, when called, would display the people who are connected to your terminal servers. Nothing special needs to be done on the parent page. To specify a MajorBBS/Worldgroup text variable, you use **{tv!tvar_name}** in the **.SHT** file.

Here's an example: **{tv!system_name}** will be replaced with the content of the SYSTEM_NAME text variable. Note that USAPTR is temporarily set to the current user (if we have one) during text variable evaluation. Use at your own risk, it's quite easy to GP your system by using the wrong Text Variable at the wrong time.

Another example: Lets create a page that will display radius users as illustrated above called **showusr.sht.** The page itself would be under the /parse.dir/ directory.

```
<HTML>
  <HEAD>
    <TITLE>GM users on the net</TITLE>
  </HEAD>
<BODY>
<H2>The following people from Widget BBS<BR>are currently surfing the net:</H2>
{tv!tcprad_showusr}
</BODY>
</HTML>
```

A parent page with the URL http://www.domain.com/parse.dir/showusr.sht calls showusr.sht. When the person brings up showusr.sht using the URL above, the contents of **TCPRAD_SHOWUSR** will replace the {**tv!tcprad_showusr}** statement in the child page. This is the result:

The following people from Widget BBS
are currently surfing the net:

(TS157:Mirabel) TCP/IP Radius
(TS163:Pixel) TCP/IP Radius
(TS172:Pipers) TCP/IP Radius
(TS173:Hiromi) TCP/IP Radius
(TS150:Forsaken) TCP/IP Radius

Special-case variables

Special-case variables were designed for a specific purpose in mind. Right now, MajorTCP/IP's web page parsing only supports two variables that are specifically used with ACTIVE-X telnet autologins. More variables will be added in the future.

{userid} returns the userid of the currently authenticated user (or N/A)
{password} returns the password (encrypted) for this user (or N/A)

Example of an autologin page

Our ActiveX telnet client now supports a feature called autologin. When a person uses the ActiveX telnet client to logon to the BBS via a web page, we can pass the {userid} and {password} to the telnet client if the user is coming from a local IP address (either one assigned from the SLIP/CSLIP/PPP Server or a terminal server identified with Radius). This way, the person doesn't need to type in his username and password to log-on. This feature is used in conjunction with the PortGo facility which lets a user wind up in a specific application from a telnet to the BBS via a specific port number.

Active-X telnet and PortGo are vircom products sold separately

For our example, we'll assume that you have two possible links. One sending link on the parent page that calls the Active-X telnet page sending the user to Tele-Arena on Port #20000. The other link does the same, but sends the user to TradeWars on Port #20001. We decided to split the host name and the port number for clarity.

The links on the parent page would look like this:

```
<A href="http://www.domain.com/parse.dir/axtelnet.sht"?host=domain.com&port=20000>
  Go to Tele-Arena
</A>
<A href="http://www.domain.com/parse.dir/axtelnet.sht"?host=domain.com&port=20001>
  Go to TradeWars
</A>
```

On the Active-X telnet page, you would have the following lines:
Note that we don't show the entire active-x telnet page, only the relevant parts

```
<OBJECT ID="axtelnet" WIDTH=650 HEIGHT=385
 CLASSID="CLSID:7C403F22-DB56-11D0-8F68-0000C04453DC"
 codebase="/axtelnet/axtelnet.CAB#version=1,0,1,5">
[> Snipped some object parameters <]
   <PARAM NAME="SecuritySERVER" VALUE="207.96.243.2">
   <PARAM NAME="Hosts" VALUE="{wv!host} {wv!port}">
[> Snipped more parameters <]
   <PARAM NAME="DoConnect" VALUE="{wv!host} {wv!port}">
   <PARAM NAME="UserID" VALUE="{userid}">
   <PARAM NAME="WebP" VALUE="{password}">

<EMBED NAME="axtelnet" WIDTH=650 HEIGHT=385
 CLASSID="CLSID:7C403F22-DB56-11D0-8F68-0000C04453DC"
 TYPE="application/oleobject"
 codebase="/axtelnet/axtelnet.CAB#version=1,0,1,5"
[> Snipped some object parameters <]
    PARAM_Hosts="{wv!host} {wv!port}"
    PARAM_DoConnect="{wv!host} {wv!port}"
[> Snipped more parameters <]
    PARAM_UserID="{userid}"
    PARAM_WebP="{password}"
    PARAM_Prompts=":  @:  ">
</OBJECT>
```

If you look closely at the page, not only do we provide the host and port to access the relevant games, but the {userid} and {password} parameters will grab the user's userid and password directly via the Active-X security server. That means that if the person telnetted in from a local IP (either via the SLIP/CSLIP/PPP Server or from an IP on a terminal server used by the BBS via Radius), the user won't be asked a username and password. He'll telnet directly into the game.