
Proxy*Server*

Internet Access / Firewall

Dual Ethernet ProxyServer

Model MTPSR1-120

User Guide

User Guide

88301500 Revision A

Dual Ethernet ProxyServer (Model No MTPSR1-120)

This publication may not be reproduced, in whole or in part, without prior expressed written permission from Multi-Tech Systems, Inc. All rights reserved.

Copyright © 1998, by Multi-Tech Systems, Inc.

Multi-Tech Systems, Inc. makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, Multi-Tech Systems, Inc. reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of Multi-Tech Systems, Inc. to notify any person or organization of such revisions or changes.

Record of Revisions

Revision	Description
A (9/4/98)	Manual released. All pages at revision A.

Patents

This Product is covered by one or more of the following U.S. Patent Numbers: **5.301.274; 5.309.562; 5.355.365; 5.355.653; 5.452.289; 5.453.986**. Other Patents Pending.

TRADEMARK

Trademark of Multi-Tech Systems, Inc. is the Multi-Tech logo.
Windows is a registered trademark of Microsoft.

Multi-Tech Systems, Inc.
2205 Woodale Drive
Mounds View, Minnesota 55112
(612) 785-3500 or (800) 328-9717
Fax 612-785-9874
Tech Support (800) 972-2439
Internet Address: <http://www.multitech.com>
Fax-Back (612) 717-5888

Contents

Chapter 1 - Introduction and Description

Introduction	6
Preview of this Guide	6
Front Panel Description	8
Back Panel Description	9
RS232/V.35 Connector	9
Ethernet 1 and 2 10Base-T Connectors	9
Command Connector	9
Power Connector	9
Specifications	10
Ethernet Ports	10
Command Port	10
WAN Link	10
Electrical/Physical	10

Chapter 2 - Installation

Safety Warnings	12
Unpacking Your ProxyServer	12
V.35 Shunt Procedure	13
Cabling Your ProxyServer	14

Chapter 3 - Software Loading and Configuration

Loading Your Software	18
IP Port Configuration	20
Default WAN Link Configuration	21

Chapter 4 - Firewall Software

Introduction	24
Typical Applications	24
Configuration 1 - Cable/DSL Modem	24
Configuration 2 - Existing Dual-LAN with Router	26
Configuration 3 - New Dual-LAN with T1 DSU	27
Firewall Program Group	29
Firewall Configuration	31
Changing IP Parameters	32
Changing WAN Port Parameters	34
Adding Proxy Applications	35
Enabling the DHCP Server	36
Enabling PPP/SLIP	37
Applications	39
Statistics	39
Filtering	40

Chapter 5 - Remote Configuration and Management

Introduction	42
Modem-Based Remote Configuration Procedure	42
LAN-Based Remote Configuration Procedure	44
Windows Sockets Compliant TCP/IP Stack	44
Remote Management	46
Telnet	46
WEB Management	48

Chapter 6 - Warranty, Service and Tech Support

Introduction	50
Limited Warranty	50
On-line Warranty Registration	50
Tech Support	51
Recording ProxyServer Information	51
Service	52
The Multi-Tech BBS	53
To Log on to the Multi-Tech BBS	53
To Download a File	53
About CompuServe	54
About the Internet	54
About the Multi-Tech Fax-Back Service	54

Appendixes

Appendix A - TCP/IP (Transmission Control Protocol/Internet Protocol) Description	56
-----------------------------------------------------------------------------------------	----

Index

ProxyServer

Internet Access / Firewall

Chapter 1 - Introduction and Description

Introduction

Welcome to Multi-Tech's new Dual Ethernet ProxyServer, model number MTPSR1-120, a high speed Internet access device that provides firewall protection to your corporate (secured) LAN and allows Internet access to the Internet Services Network (public LAN) that resides outside the firewall. Internet access can be provided through new technologies, such as cable or DSL modems, connecting to an existing high speed public LAN, or connecting the RS232 WAN port on the back of the unit that allows Internet access up to T1/E1 access speeds. The Dual Ethernet ProxyServer provides two Ethernet connections that implement firewall protection and gateway security for your LAN resources and provides megabit data transfer rates (up to 20 times faster than a 56K modem) for your Internet access.

The Dual Ethernet ProxyServer provides two Ethernet 10Base-T ports which connect your private secured LAN to the LAN 1 connection and the Internet Services Network resources to the LAN 2 connection, and a Command port for configuration. An additional RS232/V.35 port is provided for an alternate connection to an external WAN for connecting your secure corporate LAN directly to an ISP. System management is provided through the command port using bundled Windows® software which provides easy-to-use configuration menus.

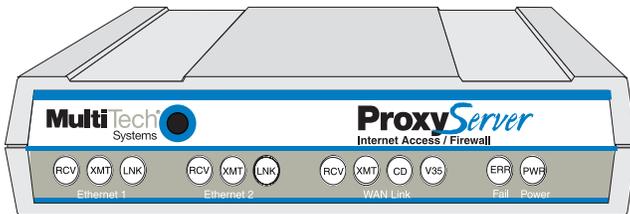


Figure 1-1. Dual Ethernet ProxyServer

Preview of this Guide

This guide describes the ProxyServer and tells you how to install and configure the unit. The information contained in each chapter is as follows:

Chapter 1 - Introduction and Description

Chapter 1 describes the Dual Ethernet ProxyServer. Descriptions of Transmission Control Protocol/Internet Protocol (TCP/IP) and Internet Protocol (IP), front panel indicators, and back panel connectors are provided. In addition, a list of relevant specifications is provided at the end of the chapter.

Chapter 2 - Installation

[Chapter 2](#) provides information on unpacking and cabling your ProxyServer. The installation procedure describes each cable connection.

Chapter 3 - Software Loading and Configuration

[Chapter 3](#) provides instructions for software loading and initial configuration. The ProxyServer software diskettes are Windows® based. Later chapters, as well as your on-line help program will describe the ProxyServer software in more detail.

Chapter 4 - ProxyServer Software

[Chapter 4](#) describes the ProxyServer software package designed for the Windows® environment. This chapter describes the ProxyServer software from an applications standpoint, and in so doing, not every screen is shown, nor is each field within a screen defined. For explanations and parameters of each field within a dialog box please refer to the on-line help system provided within the software.

Chapter 5 - Remote Configuration and Management

[Chapter 5](#) provides procedures for changing the configuration of a remote ProxyServer. Remote configuration allows you to change the configuration of a unit by simply connecting two modems between the two ProxyServers and remotely controlling the unit. In addition, remote management utilities such as Telnet and Web-based management of the ProxyServer

Chapter 6 - Warranty, Service and Tech Support

[Chapter 6](#) provides instructions on getting service for your ProxyServer at the factory, a statement of the limited warranty, information about our Internet presence, and space for recording information about your ProxyServer prior to calling Multi-Tech's Technical Support.

Appendixes

[Appendix A](#) - TCP/IP (Transmission Control Protocol/Internet Protocol) Description

Front Panel Description

The front panel, shown in Figure 1-2, contains four groups of LEDs that provide the status of the LAN connection, link activity, and general status of the ProxyServer. The Ethernet 1 and Ethernet 2 LEDs display the activity of the public and private LANs, in whether the ProxyServer is connected to the LAN, transmitting or receiving packets, and if a collision is in progress. The WAN Link LEDs display the status of the RS232/V.35 WAN link, that can optionally be connected to an external DCE device, in whether the link is ready to transmit or receive serial data, and if an external communications device with a V.35 interface is connected to the ProxyServer. The last group of LEDs indicate whether the self test passed or failed and if the power On/Off switch on the back of the ProxyServer is turned On.

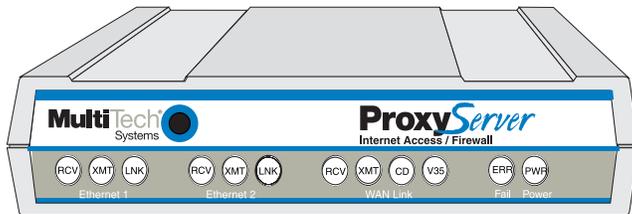


Figure 1-2. Front Panel

ETHERNET 1 and 2

- RCV** Receive Data indicator blinks when packets are being received from the private (Ethernet 1) or public (Ethernet 2) LANs.
- XMT** Transmit Data indicator blinks when packets are being transmitted to the private (Ethernet 1) or public (Ethernet 2) LANs.
- LNK** Link indicator lights when the Ethernet link senses voltage from a concentrator or external device.

WAN Link

- RCV** Receive Data indicator blinks when packets are being sent to the local area network.
- XMT** Transmit Data indicator blinks when packets are being transmitted from the local area network.
- CD** Carrier Detect indicator lights when a carrier signal is detected on the WAN link.
- V35** V.35 indicator lights when internal shunt is set for V.35 operation.

Fail

- ERR** Error indicator lights when the ProxyServer is booting or downloading setup.

Power

- PWR** Power indicator lights when power is applied to the ProxyServer.

Back Panel Description

The cable connections for the ProxyServer are made at the back panel. In addition to the Power connector, Three groups of connectors are used on the ProxyServer: the Command Port, Ethernet 1 & 2 (10BASET) and RS232/V.35. The cable connections are shown in Figure 1-3 and defined in the following groups.

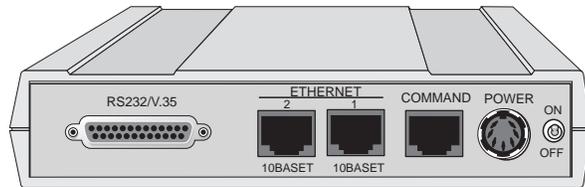


Figure 1-3. Back Panel

RS232/V.35 Connector

The RS232/V.35 (DB-25) connector is used to connect the ProxyServer to an external modem, DSU, or other Data Communications Equipment (DCE). This connection can be either RS232C (default) or V.35. If the connection is V.35, then the shunt must be moved from the default RS232 position to the V.35 position (for details on this procedure, refer to [Chapter 2 - V.35 Shunt Procedure](#)).

Ethernet 1 and 2 10Base-T Connectors

The Ethernet 10Base-T connectors are used to connect the ProxyServer to a LAN using unshielded twisted cable. Ethernet 1 connects the private LAN, and Ethernet 2 connects the public LAN. These connectors are RJ-45 jacks.

Command Connector

The Command connector is used to configure the ProxyServer using a PC with a serial port and running Windows® software. The Command connector is an RJ-45 jack and a short adapter cable is provided to convert to a standard serial port DB-25 female connector.

Power Connector

The Power connector is used to connect the external power supply to the ProxyServer. The Power connector is a 6-pin circular DIN connector. A separate power cord is connected to the power supply and the live AC grounded outlet.

Specifications

- Protocols - Point-To-Point Protocol (PPP), and Serial Line Internet Protocol (SLIP)

Ethernet Ports

- Two Ethernet Interface - 10Base-T (twisted pair) RJ-45 connectors.

Command Port

- Single 19.2K bps asynchronous Command Port using a short RJ-45 to DB-25 cable with a DB-25 female connector

WAN Link

- One RS232/V.35 port connector.

Electrical/Physical

- Voltage - 115 VAC (Standard), 240 Volts AC (Optional)
- Frequency - 47 to 63 Hz
- Power Consumption - 10 Watts
- Dimensions - 1.625" high x 6" wide x 9" deep
5.63cm high x 22.34cm wide x 33.51cm deep
- Weight - 2 pounds (.92 kg)

ProxyServer

Internet Access / Firewall

Chapter 2 - Installation

Safety Warnings

1. Never install telephone wiring during a lightning storm.
2. Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.
3. Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
4. Use caution when installing or modifying telephone lines.
5. Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electrical shock from lightning.
6. Do not use the telephone to report a gas leak in the vicinity of the leak.

Unpacking Your ProxyServer

The shipping box contains the Dual Ethernet ProxyServer, external power supply, power cord, Command Port (DB-25 to RJ-45) cable, your Quick Start Guide, and three diskettes (i.e., the ProxyServer User Guide, and the ProxyServer Software). Inspect the contents for signs of any shipping damage. If damage is observed, do not power up the unit, contact Multi-Tech's Technical Support for advice (refer to [Chapter 6](#)). If no damage is observed, place the ProxyServer in its final location and continue with the next section.

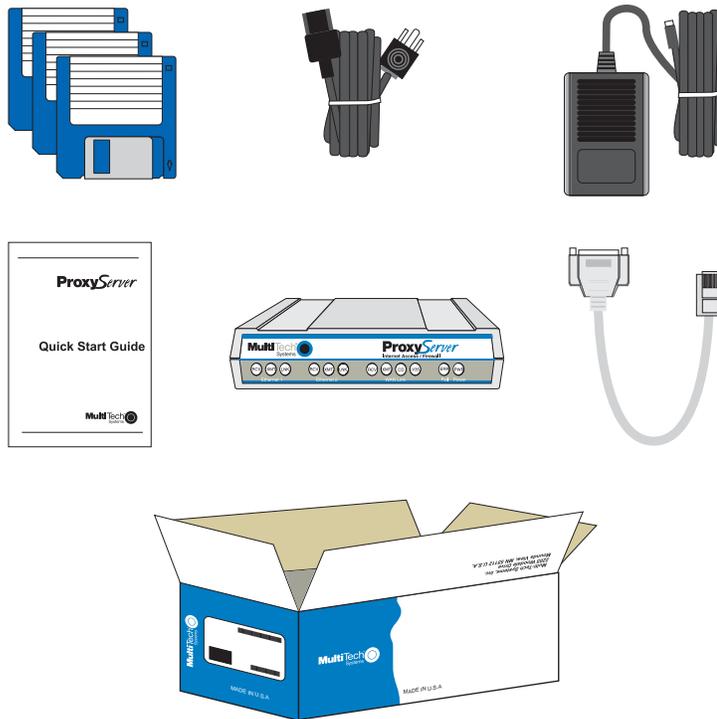


Figure 2-1. Unpacking

V.35 Shunt Procedure

If you are using an external DCE device on the WAN RS232/V.35 port, and the connection will be a V.35 connection, the internal shunt must be moved from the RS232C (default) position prior to cabling and power-up. The following steps detail the procedures for switching the shunt.

Step Procedure

- 1 Ensure that the external power supply is disconnected from the ProxyServer.
- 2 Turn the ProxyServer over and remove the cabinet mounting screw from the chassis.

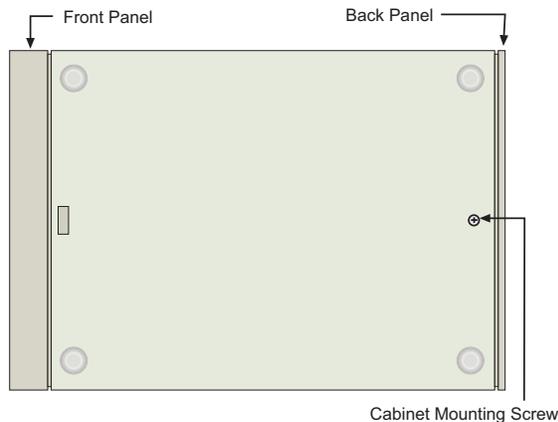


Figure 2-2. Cabinet Mounting Screw

- 3 Being sure to support the back panel, turn the ProxyServer right-side-up, tilt the back panel down, and slide the circuit board out of the chassis.
- 4 Place the unit on a flat, grounded surface with the LED's facing you.
- 5 Pry the shunt out of the RS232 position, and insert it in the V.35 position.

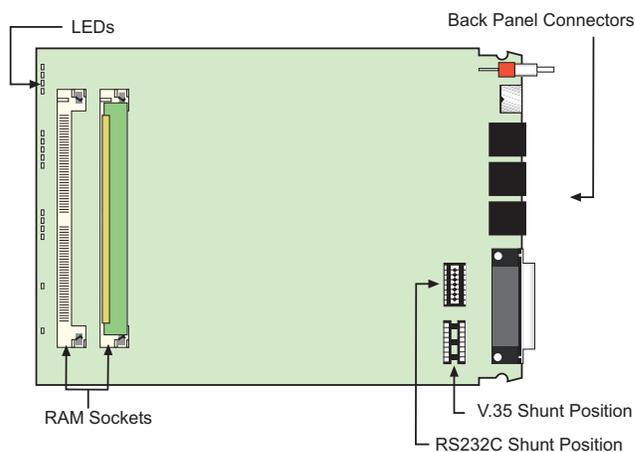


Figure 2-3. Shunt Positions

- 6 Align the board with the guide slots on the inside of the chassis and carefully slide the board back into the chassis.
- 7 Being sure to support the back panel, turn the ProxyServer over again, and replace the cabinet mounting screw.
- 8 Turn the ProxyServer right-side-up again and proceed to the next section to connect the cables.

Cabling Your ProxyServer

Cabling your ProxyServer involves making the proper Power, Command Port, and two Ethernet connections. An optional WAN connection is provided to connect to an external WAN device. Figure 2-4 shows the back panel connectors and the associated cable connections, and the table that follows details the procedures for connecting the cables to your ProxyServer.

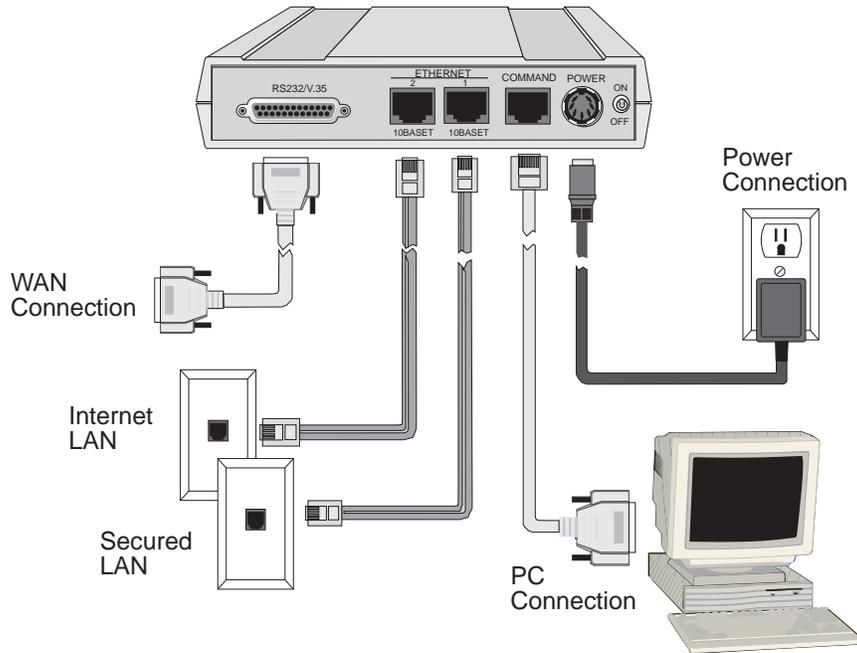


Figure 2-4. Cable Connections

Cabling Procedure

- | Step | Procedure |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | Connect one end of the power supply to a live AC outlet and connect the other end to the ProxyServer as shown in Figure 2-4. The power connector is a 6-pin circular DIN connector. |
| 2. | Connect the ProxyServer to a PC by using the short RJ-45 to DB-25 (female) cable provided in your unit. Plug the RJ-45 end of the cable into the Command port of the ProxyServer and the other end into the RS-232 cable from the PC serial port. See Figure 2-4. |
| 3. | To connect your secure (private) LAN, connect one end of an RJ-45 (UTP) cable to the LAN 1 connector on the back of the ProxyServer. Connect the other end of the cable to your private LAN. |
| 4. | To connect a cable modem, DSL modem, or your Internet (public) LAN, connect one end of an RJ-45 (UTP) cable to the LAN 2 connector on the back of the ProxyServer. Proceed to step 6. |

Table 2-1. (cont'd.)

Step	Procedure
5.	<p>If a cable modem, DSL modem, or your Internet LAN is being used, no cable connection will be made to the RS232/V.35 connector on the back of the ProxyServer.</p> <p>If the RS232/V.35 connector on the ProxyServer is going to be connected to a WAN device (i.e., connecting your secure (private) LAN to an ISP, connect one end of an RS232 or V.35 interface cable to the RS232/V.35 connector on the back of the ProxyServer. Connect the other end of this cable to the WAN device.</p>
6.	<p>Turn on power to the ProxyServer by placing the ON/OFF switch on the back panel to the ON position. Wait for the Fail LED on the ProxyServer to go OFF before proceeding. This may take a couple of minutes to go OFF.</p>

At this time your ProxyServer is completely cabled. Proceed to [Chapter 3](#) to load the Firewall software.

ProxyServer

Internet Access / Firewall

Chapter 3 - Software Loading and Configuration

Loading Your Software

The following loading procedure does not provide every screen or option in the process of installing the Firewall software. The assumption is that the installation is being performed by a technical person with a thorough knowledge of Windows and the software loading process. Additional information on the Firewall software is provided in the Chapter 4, and in the on-line help provided with your Firewall software.

1. Run Windows on the PC connected to the Command Port.
2. Insert the ProxyServer diskette labeled *Disk 1* into the disk drive on the PC connected to the Command port.
3. **Win3.1 users** - In Program Manager click **File | Run**. In the Run dialog box, type **a:\setup** or **b:\setup** (depending on the location of your floppy disk drive) in the Command Line field and then click **OK**.

Win95 users - click **Start | Run**. In the Run dialog box click on the down arrow and choose **a:\setup** or **b:\setup** (depending on the location of your floppy disk drive) in the Command Line field and then click **OK**.



4. Follow the on-screen instructions to install your Firewall software.

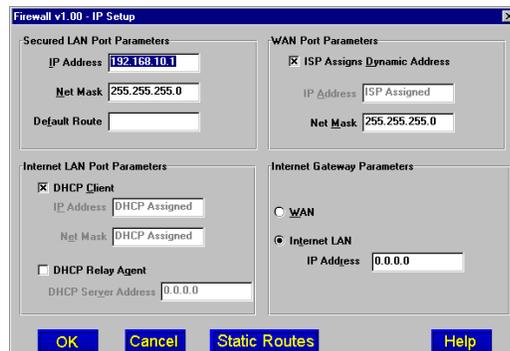


IP Port Configuration

This dialog allows for the configuration of IP parameters that are generally applicable to IP proxying on all ports.

- The **Secured LAN Port Parameters** have to be changed to your private (secure) LAN parameters. Enter your Secured LAN Port IP Address in the IP Address field, followed by the Net Mask in its field, and finally the Default Route IP address.

The Secured LAN Port IP Address can be an unregistered IP address. The Internet LAN port IP address and the Gateway IP address must be in the same IP network.



- The **Internet LAN Port Parameters** depend on how LAN 2 on the ProxyServer is configured. If a DHCP Server is providing IP addresses, click on the OK button and proceed to step 13.

If a DHCP Server is **not** providing the IP address, then click on the **DHCP Client** option and the IP Address and Net Mask fields become active. Enter your valid Public LAN IP address in the **IP Address** field, also, enter your valid **Net Mask** in its field.

DHCP Relay Agent does not apply.

- If a cable modem, DSL modem, or your public (Internet) LAN is connected to LAN 2 on the ProxyServer, the **WAN Port Parameters** are not required.

The **WAN Port Parameters** are only required if a device is connected to the RS-232/V.35 connector on the back of the ProxyServer. If your ISP for your local (secured LAN) dynamically assigns the **WAN port IP addresses**, you do not have to do anything for the WAN Port Parameters. Proceed to the step 12.

If a static WAN Port IP address needs to be assigned, click on the **ISP assigns Dynamic Address** check box to disable the feature, then click on the **IP Address** field and enter your registered WAN Port IP address. Also, enter the **Net Mask** for WAN port.

- If a DHCP Server is not providing the IP addresses in step 9 and a cable modem, DSL modem, or your public (Internet) LAN is connected to LAN 2 on your ProxyServer, then click on the Internet LAN IP Address field and enter the valid Gateway IP address (i.e., the IP address of the cable or DSL modem, or your public (Internet) LAN router's address).

If a static WAN Port IP was assigned in step 10 and the Internet access is through the RS232 connection on the back of the ProxyServer, then click on the **Internet Gateway Parameters WAN** option.

- Click **OK**.

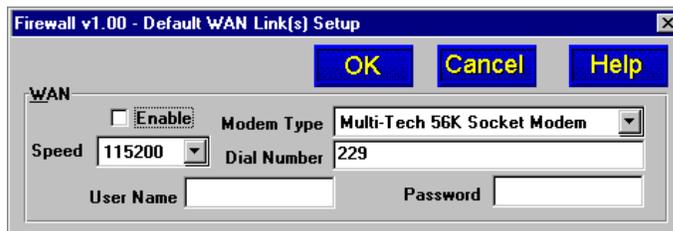
Default WAN Link Configuration

The default WAN Link(s) Setup dialog box is only used if a device is connected to the RS-232/V.35 connector on the back panel of the ProxyServer. This connection allows your private (secured) LAN to be connected to a local ISP for Internet service.

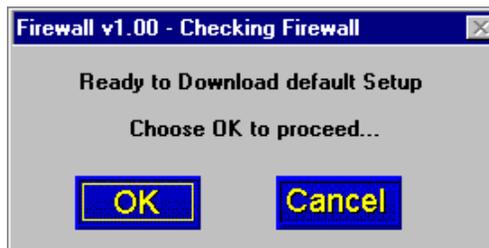
If a cable modem, DSL modem, or your public (Internet) LAN is connected to LAN 2, then the Default WAN Link has to be disabled.

13. If a cable modem, DSL modem, or Internet LAN is connected to LAN 2, click on the Enable option to disable the WAN port. Click **OK** and proceed to step 18 to download the default setup.

If a device is connected to the RS-232/V.35 connector on the back of the ProxyServer, proceed to step 14.

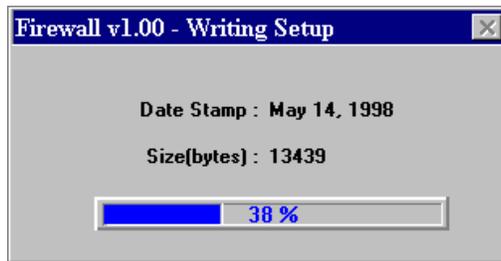


14. Click on the down arrow for the **Modem Type** and choose the device from the listing that is connected to the RS-232/V.35 connector.
15. Click on **Dial Number** and enter the telephone number supplied by your ISP. The telephone number can be a standard local number and it can include a long distance prefix.
16. Click on **User Name** and enter your user name that you negotiated with your ISP. The User Name can be up to 40 alphanumeric characters. The User Name is not case sensitive.
17. Click on **Password** and enter your password that you negotiated with your ISP. The password can be up to 15 alphanumeric character and also is not case sensitive.
18. Turn on power to the ProxyServer and the checking ProxyServer dialog box is displayed.



The Setup utility is "Ready to Download default Setup Choose OK to proceed." Click **OK** to proceed.

19. The Writing Setup dialog box is displayed as the setup configuration is written to the ProxyServer.



20. Check to ensure that the FAIL LED on the ProxyServer is Off after the download is complete and the ProxyServer is rebooted.
21. **Win3.1 users** - you are returned to your Program Manager where the Firewall Program Group and Program Item (Windows icons) have been created.
Win95 users - you are returned to the Firewall folder which will be visible on your desktop.

ProxyServer

Internet Access / Firewall

Chapter 4 - Firewall Software

Introduction

This chapter describes the Firewall software used in the Dual Ethernet ProxyServer. It begins with the description of three typical applications for the ProxyServer. These configuration examples are followed by a description of the Firewall program group, and examples of how to add some of the advanced features provided with the software.

Typical Applications

This section describes three typical applications for the Dual Ethernet ProxyServer. This is done with the assumption that the unit will be configured for a particular application during the initial installation. The three examples include a detailed diagram, along with a description of the process involved in setting up the configuration shown.

The first of the applications uses the ProxyServer to connect your private LAN to the Internet using a cable or Digital Subscriber Line (DSL) modem, providing high speed Internet access. The second application ties your private LAN and public Internet Services Network (e.g., your existing public LAN) through its router to the Internet. The third application is similar to the second, but uses a Data Communications Equipment (DCE) device—in this example, a T1 DSU—connected to the RS232 port on the back of the ProxyServer to connect to the Internet.

Configuration 1 - Cable/DSL Modem

In the configuration shown in Figure 4-1, the Dual Ethernet ProxyServer is connected to the private LAN via the **LAN 1** connection of the back of the ProxyServer. Connection to the Internet is then provided by the cable or DSL modem by connecting the Ethernet connector on the modem to the **LAN 2** connection on the ProxyServer.

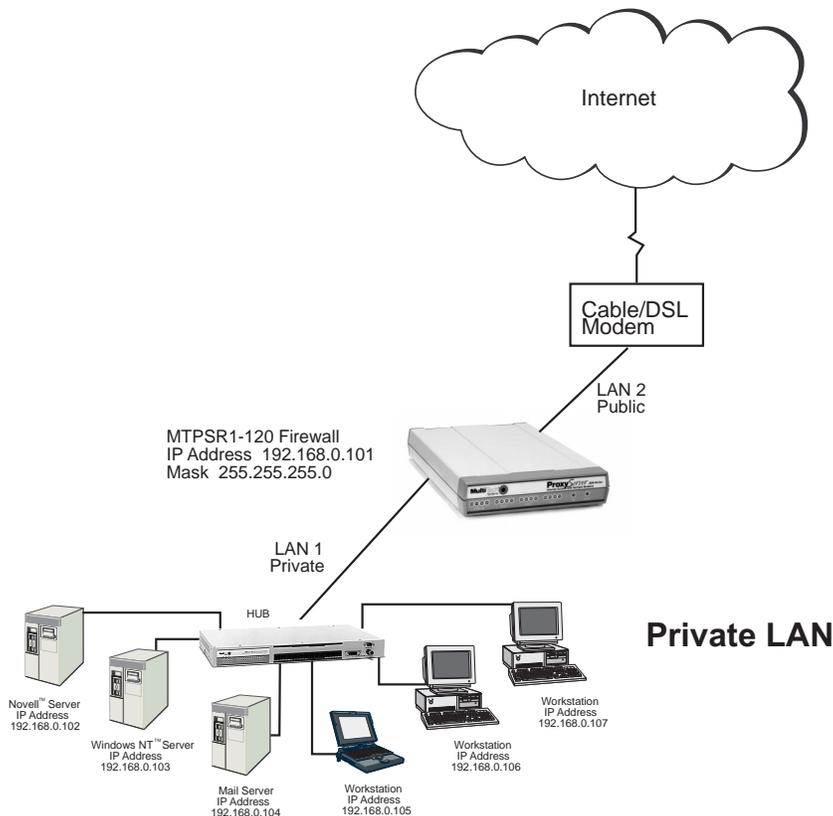


Figure 4-1. Cable/DSL Modem Configuration

During the loading of the Firewall software, the **Secured LAN Port Parameters** group (in the IP Setup dialog box) was configured to include an unregistered **IP Address** of 192.168.0.101 and default **Net Mask** of 255.255.255.0 for the private LAN (LAN 1). The **Internet LAN Port Parameters** group was configured with the **DHCP Client** option active. This enables the Internet Services Provider (ISP) to dynamically provide the registered Internet IP addresses. If a static IP addressing scheme is provided by the ISP, then the DHCP Client field in the Internet LAN Port Parameters group is deactivated and the IP Address field becomes active. The static IP address is then entered in this field.

Firewall v1.00 - IP Setup

Section	Field	Value
Secured LAN Port Parameters	IP Address	192.168.0.101
	Net Mask	255.255.255.0
	Default Route	
WAN Port Parameters	ISP Assigns Dynamic Address	<input checked="" type="checkbox"/>
	IP Address	ISP Assigned
	Net Mask	255.255.255.0
Internet LAN Port Parameters	DHCP Client	<input checked="" type="checkbox"/>
	IP Address	DHCP Assigned
	Net Mask	DHCP Assigned
	DHCP Relay Agent	<input type="checkbox"/>
Internet Gateway Parameters	WAN	<input type="radio"/>
	Internet LAN	<input checked="" type="radio"/>
	IP Address	0.0.0.0

Buttons: OK, Cancel, Static Routes, Help

Configuration 2 - Existing Dual-LAN with Router

Another typical configuration ties the private LAN (LAN 1) to an existing Internet Services Network, which already provides Internet services. This configuration provides firewall and gateway security for the LAN users, and supports Internet access restrictions based on IP address, client protocols, or a list of forbidden sites.

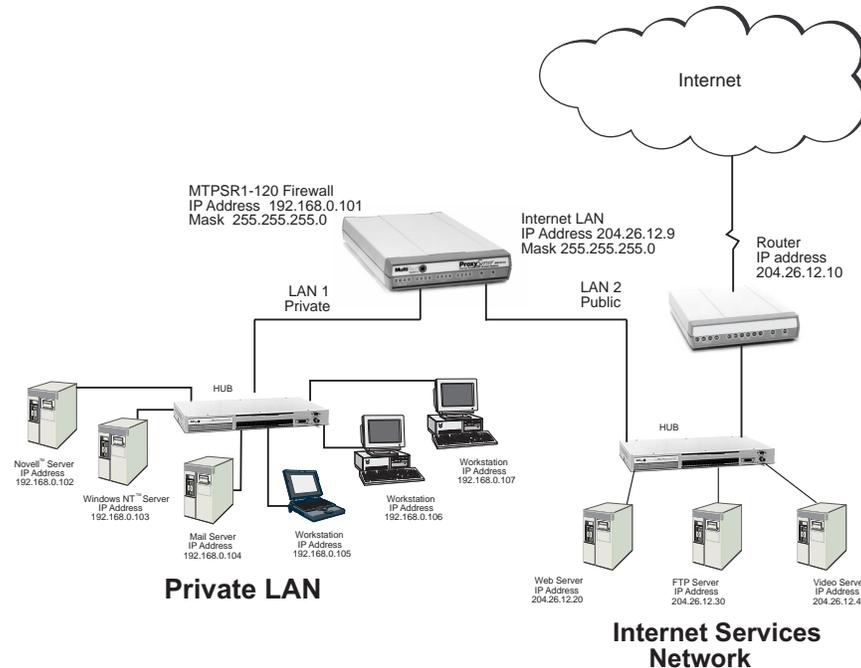
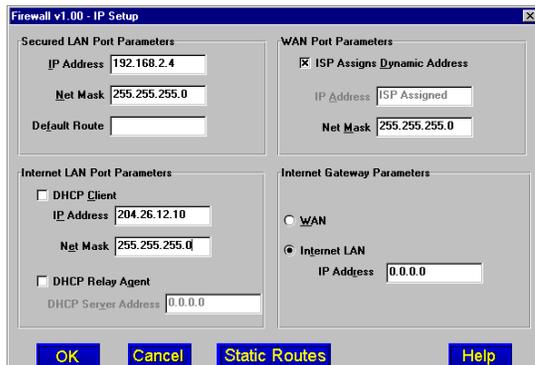


Figure 4-2. Existing Dual-LAN with Router Configuration

In the configuration shown in Figure 4-2, the ProxyServer is connected to the private LAN via the **LAN 1** connection of the back of the ProxyServer. The Internet Services Network, or public LAN, is connected to the **LAN 2** connector on the back of the unit. Connection to the Internet is then provided by the existing router connected to the Internet Services Network.

During the loading of the Firewall software, the **Secured LAN Port Parameters** group (in the IP Setup dialog box) was configured to include an **IP Address** of 192.168.0.101, and a default **Net Mask** of 255.255.255.0 for the private LAN (LAN 1). The **Internet LAN Port Parameters** group was configured with the **DHCP Client** option disabled, and the static **IP Address** of 204.26.12.10 was entered. This address is the existing static IP address that had already been assigned to the Internet Services Network router. A **Net Mask** of 255.255.255.0 was then entered to complete the configuration of the public LAN (LAN 2).



Configuration 3 - New Dual-LAN with T1 DSU

The final typical configuration adds Internet services to existing LAN users. With this configuration, the private LAN (LAN 1) is secured by the firewall while the Internet Services Network is outside the firewall allowing Internet users to access the public LAN (LAN 2) resources, such as the Web, FTP, etc. servers. The Internet connection is provided with a T1 DSU connected to the RS232 connection on the back of the unit.

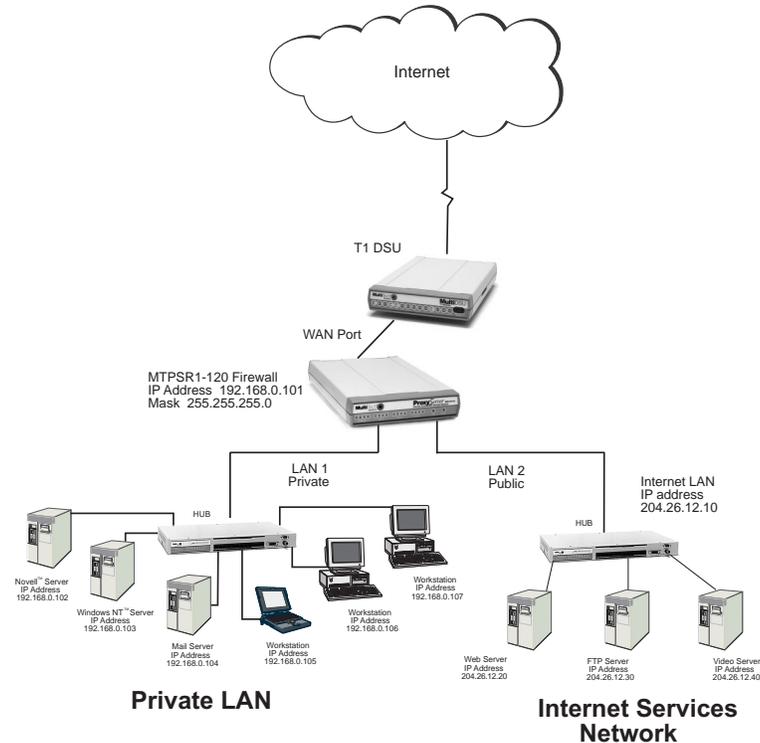
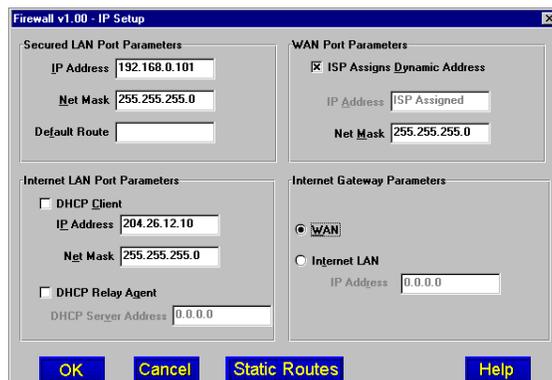


Figure 4-3. New Dual-LAN with T1 DSU Configuration

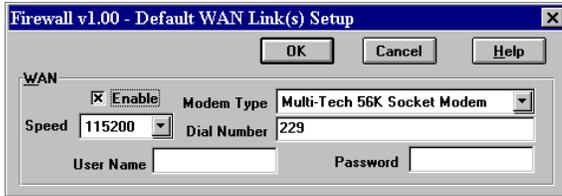
In the configuration shown in Figure 4-3, the ProxyServer is connected to the private LAN via the **LAN 1** connection of the back of the ProxyServer. The Internet Services Network, or public LAN, is connected to the **LAN 2** connector on the back of the unit. Connection to the Internet is then provided by a T1 DSU connected to the **RS232/V.35** connector on the back of the unit.

During the loading of the Firewall software, the **Secured LAN Port Parameters** group (in the IP Setup dialog box) was configured to include an unregistered **IP Address** of 192.168.0.101 and default **Net Mask** of 255.255.255.0 for the private LAN (LAN 1).



The **Internet LAN Port Parameters** group is either configured with the **DHCP Client** option active, enabling the ISP to dynamically provide the registered Internet IP addresses, or with the **DHCP Client** option disabled if a static IP addressing scheme is provided by the ISP. If the DHCP Client field is deactivated the static **IP Address** of 204.26.12.10 is then entered and the **WAN** option is checked in the **Internet Gateway Parameters** group.

In the **Default WAN Link Setup** dialog, the **WAN Enable** option is activated.



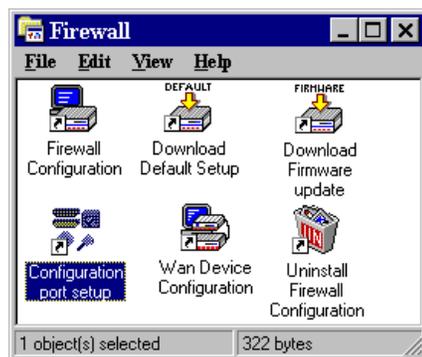
In the **Dial Number** field, the number for the ISP is entered and in the **User Name** and **Password** fields, the user name and password agreed upon with the ISP are entered.

The sections that follow provide examples of how to add some of the advanced features that enhance and build upon this basic setup.

Firewall Program Group

This section describes the advanced features of your Firewall software. The major configuration parameters are set when the software is loaded into your PC and the setup configuration is downloaded to the ProxyServer at the conclusion of the software installation. Our intent is not to cover every dialog box nor every field within a dialog box. The ProxyServer on-line help provided with your software provides such definitions, along with explanations of parameters and defaults where applicable. This constitutes a dynamic help system in that the information presented always relates to the dialog box or window that is currently open.

Your Firewall Program Group contains several applications which provide the maximum flexibility for configuration and use. These applications are also accessible in Windows by clicking **Start | Programs | Firewall | (application)**. The various options include Configuration Port Setup, Download Default Setup, Download Firmware Update, Firewall Configuration, Uninstall Firewall Configuration and Wan Device Configuration.



Firewall Configuration will be discussed in detail later in this chapter. A brief description of the other components is provided here:



Configuration port setup

Configuration Port Setup

The Configuration Port Setup program allows you to set up and configure the configuration port on your ProxyServer. This dialog is included in the initial installation process. Although parameters can be changed, be sure to note the current status of the software before making any alterations.

When you installed the Firewall software, you selected to configure the port as either an IP or COM Port. When COM Port is selected, you can assign the proper COM Port and define the modem Init String, Dial String, and various responses. If IP is selected, you can assign a static IP address or select one from the drop down list. For more information on each individual parameter, refer to the on-line help provided with the software.



Download Default Setup

Download Default Setup

This feature allows you to download the default settings, configured during installation, to the ProxyServer. If you are installing for the first time, you will download this setup at the end of the installation before operating the ProxyServer. If you have made changes to the Firewall Configuration and wish to revert to the default setup, you can do so through the Firewall Program Group.

Choose **Download Default Setup** to download the factory default settings. If the ProxyServer is running, you will be queried to reboot. Click **Yes** to continue with the download. You will then be presented with two dialogs including **IP Setup** and **Default WAN Link(s) Setup**. These screens will contain the original setup information. Click **OK** on each to accept the default settings, or make any necessary changes and then click **OK**. When prompted, click **OK** again to proceed with the download. The default setup will be written to the Firewall. This process may take a few minutes. When it is finished, you will be returned to Windows.



Download
Firmwar...

Download Firmware Update

This application allows you to update the firmware of the ProxyServer. This may be necessary in the case of repair or upgrade. To download the firmware update, choose **Download Firmware Update** from the **Firewall Program Group**, and the **Open** dialog box is displayed (if the ProxyServer is running, you will be queried to reboot to update firmware; click **OK** to proceed and the **Open** dialog will be displayed).

By default, the Firewall software will display the proper firmware from the Firewall folder. Double click on this file in the **File Name** list.

The Downloading Code dialog is displayed, which includes a status bar to monitor the download. When the download is complete the ProxyServer will reboot. This process will take several minutes. After rebooting, you will be returned to Windows.



Uninstall
Firewall Co...

Uninstall Firewall Configuration

Selecting Uninstall Firewall Configuration will allow you to completely remove all the components of the Firewall Program Group. Upon selecting this option your will be queried for confirmation. Click **Yes** to continue with the uninstall, or click **No** to abort.

Note: You will not be able to use the ProxyServer without Firewall Configuration. If you remove the components, you will need to reinstall the software. Refer to your *ProxyServer Firewall Quick Start Guide* for installation instructions.



Wan Device
Configuration

WAN Device Configuration

If you have an external WAN device connected to the WAN port of the ProxyServer, this application will open the Firewall Print Console, a terminal emulation program, that will allow configuration of the external device.

Firewall Configuration



To view or change your ProxyServer configuration in Windows 95, click on the **Start | Programs | Firewall | Firewall Configuration**. After loading, the **Firewall Setup** menu will appear.



The **Firewall Setup** menu consists of 13 buttons which allow you to display and change the protocol stacks, define the output of the ProxyServer, perform network management functions, test the communications link, print messages received from the target ProxyServer, and download setup information to the ProxyServer.

In the bottom row, there are two buttons to open the on-line Help system (Firewall Setup Help) and end (Exit) a Proxy configuration session.

Changing IP Parameters

The IP Setup dialog box establishes the IP addressing for your private LAN, Public LAN, and, if the Proxy Server is directly connected to the Internet, the WAN port. To change the IP Setup parameters that were configured during the initial setup, click on the **IP** button in the **Firewall Setup** menu. The **IP Setup** dialog is displayed.

The **Secured LAN Port Parameters** group is used to assign the Ethernet parameters of your private LAN (LAN 1) port. If a router is used to connect a second private LAN, the IP address of that router is also entered in this group.

IP Address - This field defines the IP address of the private LAN (LAN 1) port on the ProxyServer. This must be a unique host IP address that falls in the LAN IP network, and can be an unregistered address.

Net Mask - This field defines the Subnetwork Mask of the private LAN (LAN 1) port on the ProxyServer.

Default Route - This field defines the IP address of a router on the private LAN that connects a second private LAN to the ProxyServer.

The **Internet LAN Port Parameters** group is used to configure the public LAN (LAN 2) port. The parameters of this group will vary, depending on the LAN configuration. The Internet LAN Port Parameters group defines the static or dynamic addressing scheme for the public LAN (LAN 2)

DHCP Client - If this option is active, the Internet Services Provider (ISP) is able to dynamically provide the registered Internet IP addresses. If a static IP addressing scheme is provided by the ISP, then the DHCP Client option must be deactivated and the IP Address field becomes active. The static IP address is then entered in this field.

IP Address - If the DHCP Client option is active, this address is dynamically assigned by the ISP. If the DHCP Client is inactive, then the static IP address of the router connected to the Internet Services Network is entered in this field.

Net Mask - If the DHCP Client option is active, the Net Mask is dynamically assigned by the ISP. If the DHCP Client is inactive, then the Net Mask of the router connected to the Internet Services Network is entered in this field.

DHCP Relay Agent - Enabling this option allows the ProxyServer to relay IP address requests from the Internet to the DHCP server through the WAN. If this option is enabled, the DHCP Server Address field becomes active, and the IP address of the DHCP server must be entered.

DHCP Server Address - If the DHCP Relay Agent option is active, enter the IP address of the DHCP server in this field.

The **WAN Port Parameters** group is used to configure the WAN port, if enabled. The WAN port parameters are established when the ProxyServer is directly connected to the Internet via the RS232/V.35 connector on the back of the unit.

ISP Assigns Dynamic Address - Normally, the ISP assigns a dynamic address when the port comes up. If this is not the case, disable this option and assign a valid registered Internet address in the IP Address field.

IP Address - If dynamic addressing is enabled, this field is dynamically assigned by the ISP. If static addressing is enabled, enter a valid Internet address in this field.

Net Mask - Enter the Subnetwork Mask for the WAN port in this field.

The **Internet Gateway Parameters** group is used to configure the Internet gateway if used by the Internet LAN (LAN 2) port.

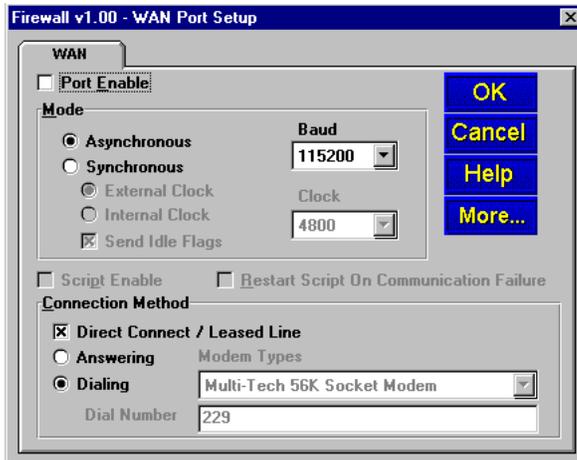
WAN - If a connection to the Internet Services Network is provided via a DCE device connected to the RS232/V.35 port on the back of the ProxyServer, then this option must be selected.

Internet LAN - If a connection to the Internet Services Network is provided through the Internet LAN (LAN 2), then this option must be selected. If the Internet LAN is configured as a DHCP Client, then the IP address will be dynamically assigned by the ISP. If the DHCP Client option is disabled, then a valid registered Internet address must be entered in the IP Address field.

IP Address - If the Internet LAN is configured as a DHCP Client, this address will be dynamically assigned by the ISP. If the DHCP Client option is disabled, the a valid registered Internet address must be entered in the IP Address field.

Changing WAN Port Parameters

In order to change the WAN port parameters of a DCE device connected to the RS232/V.35 connector on the ProxyServer, click on the **WAN** button in the **Firewall Setup** menu. The **WAN Port Setup** dialog box is displayed.



From this dialog, you can configure the parameters of the WAN port. To enable the WAN port, click on the **Port Enable** check box.

The **Mode** group allows you to configure the WAN interface to match the DCE device connected to the RS232/V.35 port on the ProxyServer. Options include **Asynchronous** or **Synchronous** mode. If asynchronous is chosen, you can select the proper **Baud** speed. If synchronous is chosen, **External Clocking** or **Internal Clocking** must be selected.

The **Connection Method** group allows you to configure the port as **Direct Connect/Leased Line**, **Answering** or **Dialing**, and allows you to select the **Modem Type** and **Dial Number** for the DCE device.

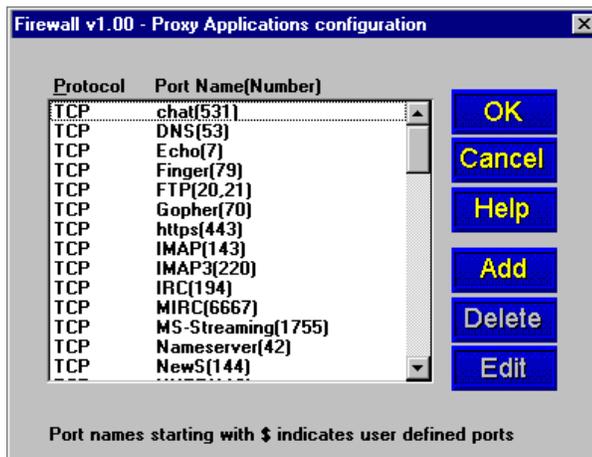
For a detailed description of each field, refer to the on-line help provided with your Firewall software.

Adding Proxy Applications

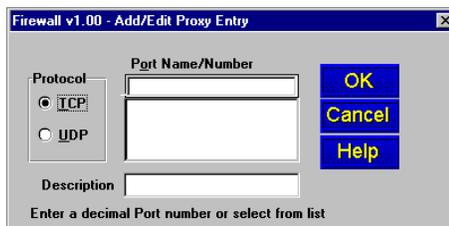
Certain software on your LAN may require a TCP or UDP port usage that is not currently supported by the ProxyServer. If this is the case, you must refer to the software documentation to determine the proper port usage and number. Without this information, the Proxy will not allow packets through to the Internet from the unknown software. Once the necessary information has been determined, you can add the application(s) to the supported list.

This list includes many of the most common port usages, however, not all are included because an increase in the number of port usages supported means a *possible* decrease in performance speed, and an increased security risk.

If you wish to add ProxyServer applications that are not currently supported, click on the **Proxy Server** button in the **Firewall Setup** menu. The **Proxy Applications Configuration** dialog box appears. This menu includes a list of all the applications currently supported by the ProxyServer.



Click on the **Add** button. The **Add/Edit Entry** dialog box appears.

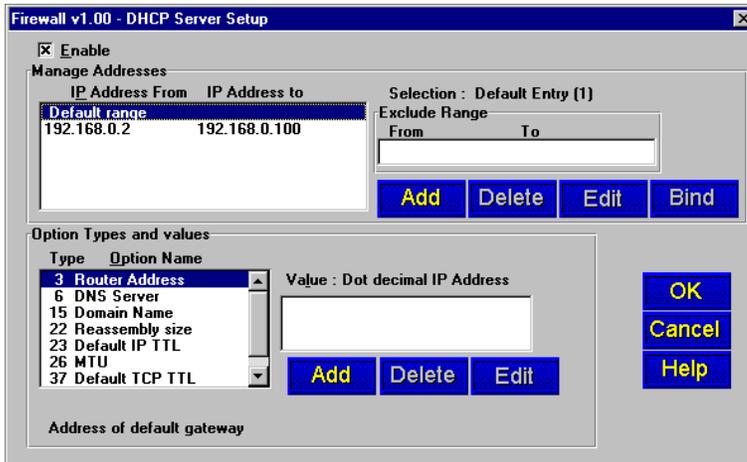


This dialog will allow you choose the desired protocol, and enter a **Port Name/Number** and **Description**. After you have entered these items, click on **OK** to add the port usage to the list of supported usages.

Enabling the DHCP Server

The DHCP Server feature of the ProxyServer manages all the IP address assignments on the private LAN. IP address management becomes completely transparent.

To enable the DHCP Server ability in the ProxyServer, click on the **DHCP Server** button in the **Firewall Setup** menu. The **DHCP Server Setup** dialog box appears.



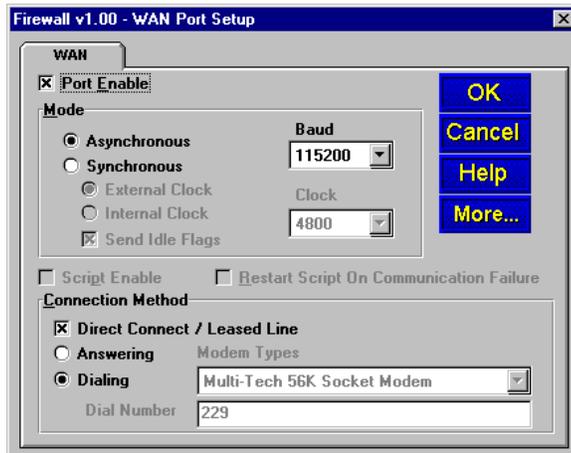
The **DHCP Server Setup** menu allows you to customize each client PC configuration from one central point. You can establish a range of client addresses in the **Manage Addresses** group. You can then exclude specific addresses from that range in the **Exclude Range** field. You can also add, delete, edit and bind addresses using the corresponding buttons in this group.

The **Option Types and Values** group on the bottom portion of the menu allows you to customize the configuration of the client platform. Again, you can add, delete and edit an option by highlighting it and clicking on the appropriate button. You cannot, however, edit or delete entries provided in the default list.

Enabling PPP/SLIP

If you wish to use Point to Point Protocol (PPP) or Serial Line IP Protocol (SLIP) on the WAN port, you can enable in the PPP/SLIP menu. In order to configure these options, you must first enable the WAN port.

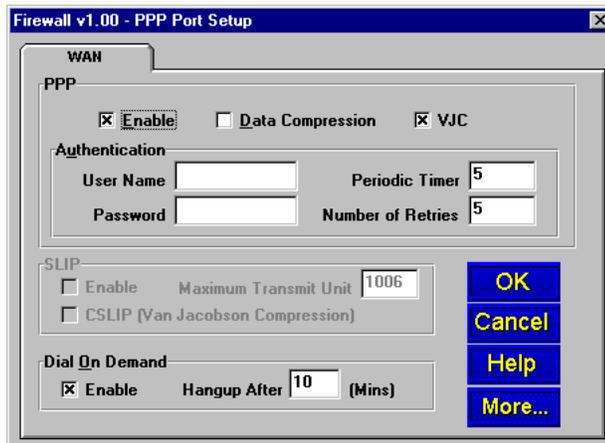
To enable the WAN port, click on the **WAN** button in the **Firewall Setup** menu. The **WAN Setup** dialog box appears.



Click on the **Port Enable** check box enable the WAN port. Click **OK**.

You are returned to the **Firewall Setup** menu. Click on **PPP/SLIP**. The **PPP Port Setup** menu is displayed.

Enabling PPP



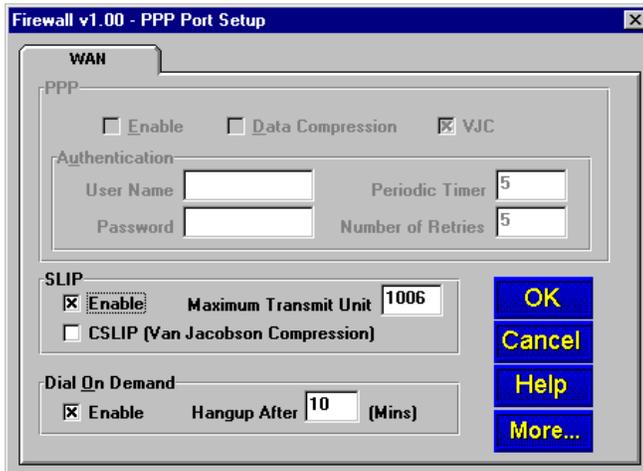
If you wish to configure the port for use with PPP, click on the **Enable** check box in the **PPP** group. Enter a valid **User Name** and **Password** and verify (or change) the **Periodic Timer** and **Number of Retries** (for definition and parameters of a specific field, refer to the on-line help).

By default, Dial On Demand is enabled. If you do not wish to use this feature, click on the **Enable** check box in the **Dial On Demand** group to disable it.

When you have finished the configuration, click **OK**. You are returned to the **Firewall Setup** menu. Click **Download Setup** to save the new configuration to the ProxyServer.

Enabling SLIP

If you wish to configure the port for use with SLIP, click on the Enable check box in the SLIP group.



The following message appears:



Click **OK**. This value was assigned in the initial software installation and was downloaded to the ProxyServer at the end of the installation. If you wish to verify or change the WAN IP address, click on **IP** in the **Firewall Setup** menu.

If you wish to make use of CSLIP (Van Jacobsen Compression), click on the **CSLIP (Van Jacobsen Compression)** check box to enable CSLIP. Verify (or change) the **Maximum Transmit Unit** value (for definition and parameters of a specific field, refer to the on-line help).

By default, Dial On Demand is enabled. If you do not wish to use this feature, click on the **Enable** check box in the **Dial On Demand** group to disable it.

When you have finished the configuration, click **OK**. You are returned to the **Firewall Setup** menu. Click **Download Setup** to save the new configuration to the ProxyServer.

Applications

In addition to local configuration, the ProxyServer supports various applications which allow it to be configured remotely from anywhere on the connected Internet. To manage these applications, click **Others** in the **Proxy Setup** menu.

The **Applications Setup** dialog box appears.

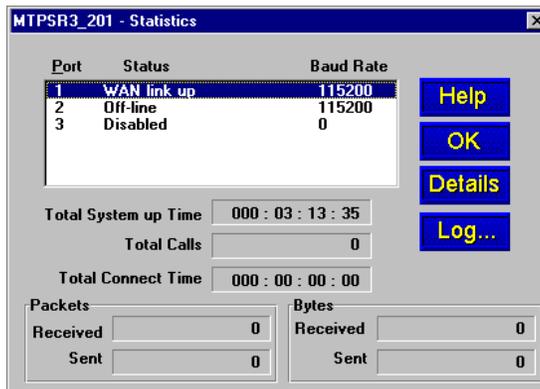


Enter a valid **Server Password** and **Server IP Address** (the IP address of the ProxyServer) and then verify that the desired applications are enabled. By default, the ProxyServer supports Telnet, TFTP, WEB, and Dumb Terminal management. If you wish to disable any of these applications, click the corresponding check box to disable support.

For more information on using these remote configuration applications, please refer to [Chapter 5](#).

Statistics

The ProxyServer is capable of providing statistics for each port and for the whole system. These statistics can be useful for troubleshooting and management purposes. To access this information, click **Statistics** in the **Proxy Setup** menu. The **Statistics** dialog box is displayed.



From this menu, you can query the details of a specific port or observe total system statistics such as Total System Up Time, and Total Calls. In addition, statistics can be saved to a log file for future use.

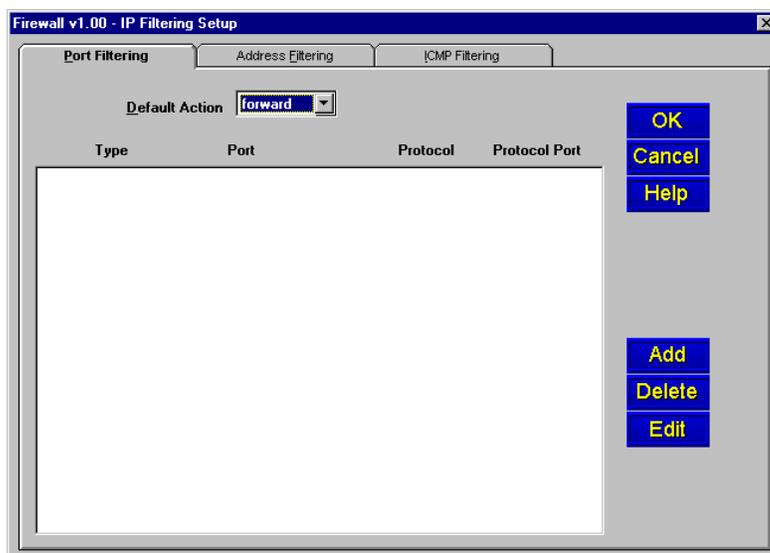
For more details and parameters about specific fields within the statistics dialog, refer to the on-line help.

Filtering

The IP Filtering Setup dialog provides tabs that let you configure the ProxyServer so that IP packets that are received by the server can be selectively filtered or forwarded based on their addresses or by the protocol ports to which they are destined.

The three filtering methods are:

- **IP Protocol Port Based Filtering** - In this method, IP packets can be filtered based on their specific purposes; e.g. Telnet packets (TCP based) or TFTP (UDP based) can be filtered or forwarded.
- **IP Address Based Filtering** - In this method, filtering is based on the source and destination IP addresses in the packet.
- **ICMP Filtering** - Separate filtering support is provided for specific kinds of received ICMP packets.



For a more detailed description of filtering, refer to the on-line help provided with your Firewall software.

ProxyServer

Internet Access / Firewall

Chapter 5 - Remote Configuration and Management

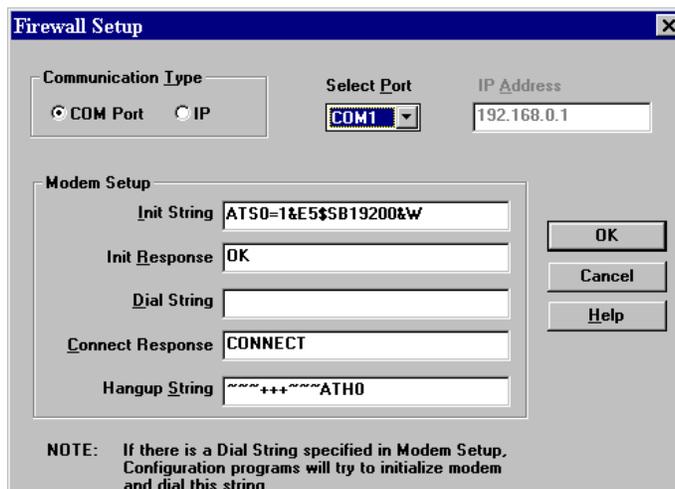
Introduction

This chapter provides procedures for changing the configuration of a remote unit. Remote configuration allows a PC at one site (local site) to dial a remote ProxyServer and change the configuration of that remote unit. Remote configuration can be accomplished either directly through the LAN or remotely using modems. To remotely configure a ProxyServer, a local PC needs to be connected to a dial-up line and the ProxyServer software configured to call the remote ProxyServer. The remote ProxyServer needs to have a modem connected to a dial-up line and the Command Port. Once the connection to the remote unit is made, you can change the configuration as you see fit. Once the configuration is changed, you can download the new configuration to the remote ProxyServer. Refer to the [Modem-Based Remote Configuration Procedure](#) to remotely configure a ProxyServer.

To configure the remote ProxyServer through the LAN, change the communication type to the IP based Trivial File Transfer Protocol (known as TFTP) and change the configuration as you see fit. Refer to the [LAN-Based Remote Configuration Procedure](#) in this chapter to configure a remote ProxyServer.

Modem-Based Remote Configuration Procedure

- 1 At the remote site, remove the serial cable from the PC to the Command Port connector on the back panel of the ProxyServer.
- 2 At the remote site, connect a special cable (Remote Configuration Cable) to the Command Port connector on the back panel of the ProxyServer and the RS232 connector on the modem. The special cable is a serial cable with male connectors on both ends.
Connect the modem to your local telephone line.
Provide your telephone number to the person verifying your configuration.
- 3 At the main site, connect your local PC to a modem that is connected to a dial-up line.
- 4 Install the ProxyServer software on the local PC. When installed, click **Start | Programs | Firewall | Configuration Port Setup**, or double click on the **Configuration Port** icon in the Firewall program group.
- 5 The Firewall Setup dialog box is displayed.



Verify that the **Communication Type** is set for **COM Port** and the **Select Port** field is set for the COM port of your local PC.

In the **Dial String** field, enter the AT command for dialing (ATDT) plus the phone number of the remote ProxyServer.

If your Modem Initialization String, Initialization Response, or Connect Response values are different than the defaults in the dialog box, refer to your modem user documentation and change the default values to match your modem.

Click **OK** when you are satisfied with your selections.

- 6 Run the Proxy Server Configuration program. Click **Start | Programs | Firewall | Firewall Configuration**, or double click on the **Firewall Configuration** icon in the Firewall program group.
- 7 The **Dialing Router** dialog box is displayed while software is dialing the remote ProxyServer.
- 8 The **Reading Setup** dialog box is displayed.
- 9 The **Firewall Setup** menu is displayed. This is the dialog box of the remote ProxyServer. Refer to the on-line help provided with your software for a description of each dialog box and field within a dialog box.



- 10 After you have changed the configuration of the remote ProxyServer, click **Download Setup** to update the configuration. The remote ProxyServer will be brought down, the new configuration written to the unit, and the unit will reboot.
- 11 Click **Exit** when the downloading is complete.
- 12 The **Hangup connection with Router?** dialog box is displayed
Click **Yes** to disconnect the phone connection to the remote site.
- 13 If the same telephone number is not going to be used again in the immediate future, you may want to remove it from the Port Setup dialog box.
- 14 At the remote site, reconnect the ProxyServer to the serial port of the PC and from the Firewall program group double click on the **Firewall Configuration** icon to verify that the ProxyServer is running.

LAN-Based Remote Configuration Procedure

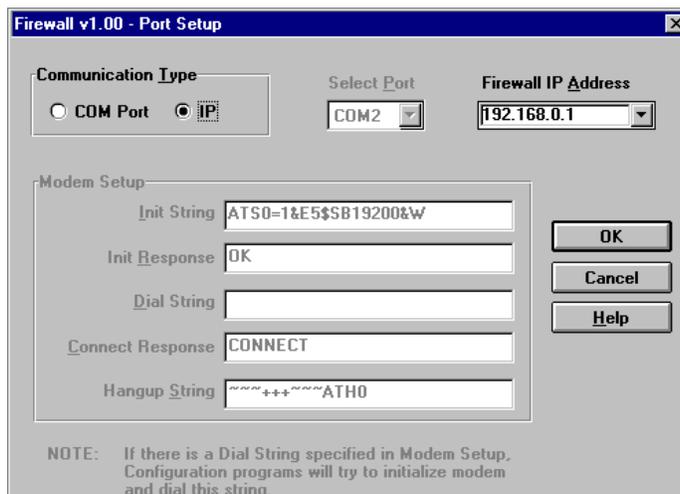
Windows Sockets Compliant TCP/IP Stack

The configuration program requires a Windows Sockets compliant TCP/IP stack. TCP/IP protocol software must be installed and functional before the configuration program can be used.

- 1 You must assign an Internet (IP) address for the PC and for each node that will be managed by the configuration program. Refer to the protocol software documentation for instructions on how to set the IP addresses.

Once you have completed this step, you should be able to use the protocol Ping command for the PC host name. You should also test the network interface configuration by Pinging another TCP/IP device that is connected to the network.

- 2 Install the Proxy Server software on the local PC. When installed click **Start | Programs | Firewall | Configuration Port Setup**, or double click on the **Configuration Port Setup** icon in the Firewall program group.
- 3 The Firewall Setup dialog box is displayed.



Verify that the **Communication Type** field is set **IP**.

In the **Router IP Address** field, enter the IP Address of the remote ProxyServer.

- 4 Click **OK** when you are satisfied with your selections.
- 5 Run the Proxy Server Configuration program. Click **Start | Programs | Firewall | Firewall Configuration**, or double click on the **Firewall Configuration** icon in the Firewall program group.

- 6 The **Firewall Setup** dialog box is displayed. This is the dialog box of the remote ProxyServer. Refer to the on-line help provided with your ProxyServer for the definition of each dialog box and field within a dialog box.



- 7 After you have changed the configuration of the remote ProxyServer, click **Download Setup** to update the configuration. The remote ProxyServer will be brought down, the new configuration written to the unit, and the unit will reboot.
- 8 Click **Exit** when the downloading is complete.
- 9 Double click on the **Firewall Configuration** icon in the Firewall program group to verify that the ProxyServer is running.

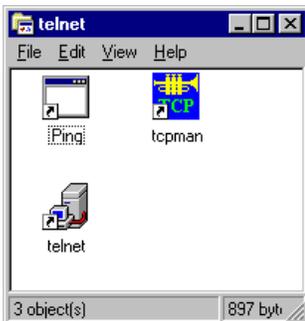
Remote Management

This section describes typical client applications that can be used to configure the ProxyServer remotely. It is important to note that although any subsequent changes to configuration can be made using these applications, the initial setup and configuration of the ProxyServer must be done on the local PC, using the ProxyServer software provided with your unit.

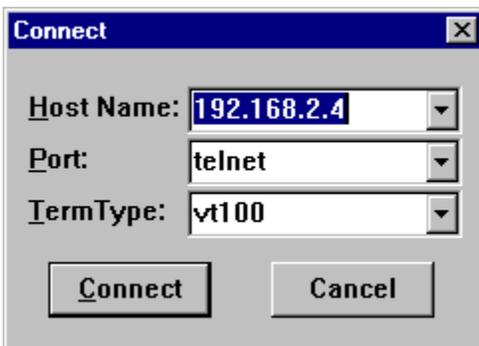
Although establishing access to the ProxyServer varies between applications, the configuration functions mirror those of the ProxyServer software. For more information on ProxyServer software, refer to [Chapter 4 - Proxy Server Software](#).

Telnet

A typical Telnet client application is described in this chapter. The Firewall ProxyServer has a built-in Telnet Server that enables Telnet client PCs to access the ProxyServer. A typical Telnet client is allowed to configure the ProxyServer and WAN devices. A typical TCP/IP program group is shown below with a Tcpman icon and a Telnet icon.



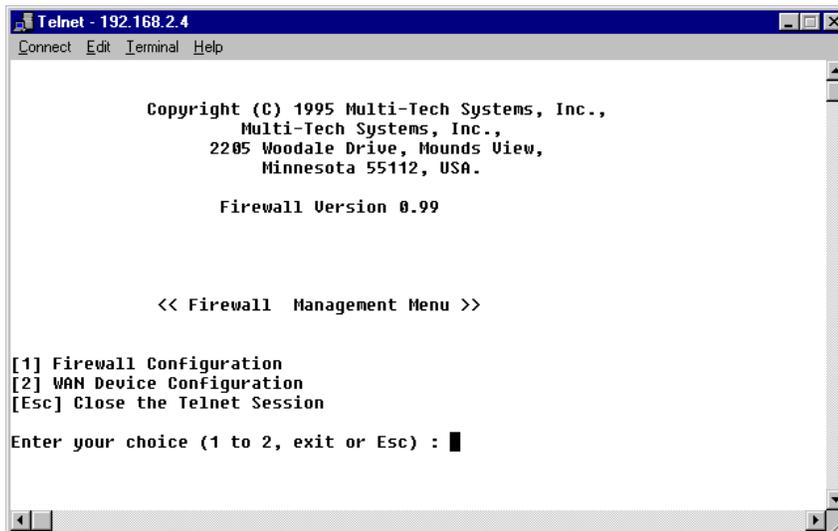
The TCP/IP stack has to be loaded before the Telnet client (a Windows application) will run, and the Telnet Server option has to be selected from the Applications Setup dialog box using Firewall Configuration (see Chapter 4 - Applications). Double click on the **Telnet** icon (or shortcut) and a blank Telnet screen is displayed. Click **Connect | Remote System** and the Connect dialog box is displayed. Select (or enter) a **Host Name** (the IP address of the ProxyServer). In this example, the Host Name is 192.168.2.4.



When you enter a valid Host Name (IP address) and click on **Connect**, you are immediately connected to the target ProxyServer and the **Firewall Management Menu** screen is displayed.

Firewall Management Menu

The Firewall Management Menu provides two basic options: Firewall Configuration and WAN Device Configuration. A further option enables you to close the Telnet session from this menu by pressing the Esc key.



```

Telnet - 192.168.2.4
Connect Edit Terminal Help

Copyright (C) 1995 Multi-Tech Systems, Inc.,
Multi-Tech Systems, Inc.,
2205 Woodale Drive, Mounds View,
Minnesota 55112, USA.

Firewall Version 0.99

<< Firewall Management Menu >>

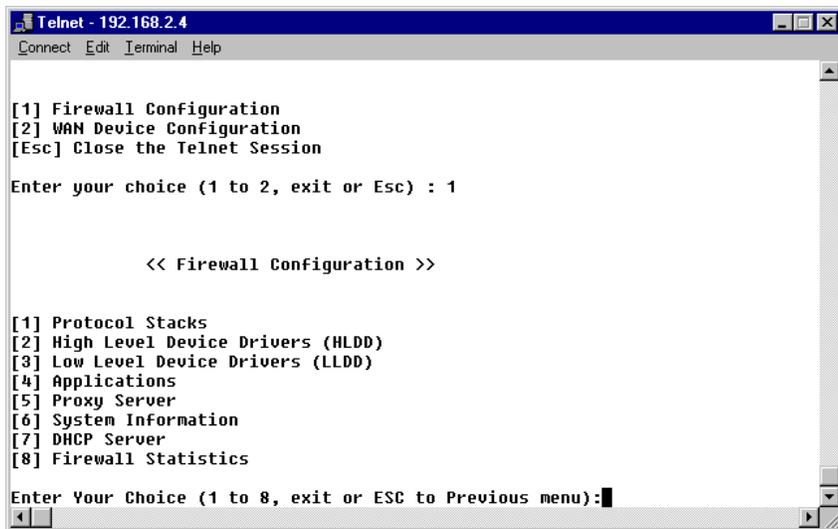
[1] Firewall Configuration
[2] WAN Device Configuration
[Esc] Close the Telnet Session

Enter your choice (1 to 2, exit or Esc) : █

```

Firewall Configuration

Selecting **Option 1** displays the **Firewall Configuration** menu with options that enable you to configure ProxyServer parameters and download settings. In addition, you can obtain statistics and system information, or reset the ProxyServer.



```

Telnet - 192.168.2.4
Connect Edit Terminal Help

[1] Firewall Configuration
[2] WAN Device Configuration
[Esc] Close the Telnet Session

Enter your choice (1 to 2, exit or Esc) : 1

<< Firewall Configuration >>

[1] Protocol Stacks
[2] High Level Device Drivers (HLDD)
[3] Low Level Device Drivers (LLDD)
[4] Applications
[5] Proxy Server
[6] System Information
[7] DHCP Server
[8] Firewall Statistics

Enter Your Choice (1 to 8, exit or ESC to Previous menu): █

```

For more details on Firewall configuration, refer to [Chapter 4 - Firewall Software](#), and the on-line helps.

WAN Device Configuration

Selecting **Option 2** displays the **WAN Device Configuration** options, which enable you to gain direct access to the DCE device on the WAN port.

WEB Management

The ProxyServer can be accessed, via a standard web-browser, from anywhere on the connected Internet. In order to provide this support, the **WEB Server** option has to be enabled in the **Applications Setup** dialog box (see [Chapter 4 - Firewall Software, Applications](#)).

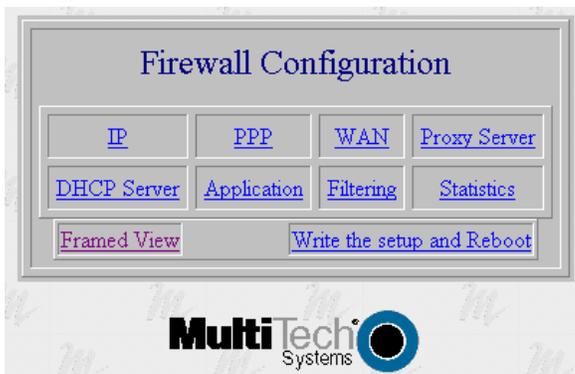
Once enabled, users can access the ProxyServer by entering its IP address in the destination field of their web browser. The following screen appears.



Click on the word 'login' to log in to the ProxyServer configuration program. The **Enter Network Password** screen is displayed.



Type **supervisor** in the **User Name** field (no password needed) and click **OK**. The **Firewall Configuration** screen is displayed.



From this screen you can access all the configuration options. Refer to [Chapter 4 - Firewall Software](#), for a description of the various options.

ProxyServer

Internet Access / Firewall

Chapter 6 - Warranty, Service and Tech Support

Introduction

This chapter starts out with statements about your Dual Ethernet ProxyServer 2-year warranty. The next section, Tech Support, should be read carefully if you have questions or problems with your ProxyServer. It includes the technical support telephone numbers, space for recording your product information, and an explanation of how to send in your ProxyServer should you require service. The final three sections explain how to use our bulletin board service (BBS), and get support through CompuServe and the Internet.

Limited Warranty

Multi-Tech Systems, Inc. ("MTS") warrants that its products will be free from defects in material or workmanship for a period of two years from the date of purchase, or if proof of purchase is not provided, two years from date of shipment. **MTS MAKES NO OTHER WARRANTY, EXPRESSED OR IMPLIED, AND ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE HEREBY DISCLAIMED.** This warranty does not apply to any products which have been damaged by lightning storms, water, or power surges or which have been neglected, altered, abused, used for a purpose other than the one for which they were manufactured, repaired by the customer or any party without MTS's written authorization, or used in any manner inconsistent with MTS's instructions.

MTS's entire obligation under this warranty shall be limited (at MTS's option) to repair or replacement of any products which prove to be defective within the warranty period, or, at MTS's option, issuance of a refund of the purchase price. Defective products must be returned by Customer to MTS's factory transportation prepaid.

MTS WILL NOT BE LIABLE FOR CONSEQUENTIAL DAMAGES AND UNDER NO CIRCUMSTANCES WILL ITS LIABILITY EXCEED THE PURCHASE PRICE FOR DEFECTIVE PRODUCTS.

On-line Warranty Registration

To register your ProxyServer on-line, click on the following link:

<http://www.multitech.com/register>

Tech Support

Multi-Tech has an excellent staff of technical support personnel available to help you get the most out of your Multi-Tech product. If you have any questions about the operation of this unit, call 1-800-972-2439. Please fill out the ProxyServer information (below), and have it available when you call. If your ProxyServer requires service, the tech support specialist will guide you on how to send in your ProxyServer (refer to the next section).

Recording ProxyServer Information

Please fill in the following information on your Multi-Tech ProxyServer. This will help tech support in answering your questions. (The same information is requested on the Warranty Registration Card.)

Model No.: _____

Serial No.: _____

Software Version: _____

The model and serial numbers are on the bottom of your ProxyServer.

Please note the type of external link device that is connected to your ProxyServer before calling tech support. Also, note the status of your ProxyServer including LED indicators, screen messages, diagnostic test results, DIP-Switch settings, problems with a specific application, etc. Use the space below to note the ProxyServer status:

Service

If your tech support specialist decides that service is required, your ProxyServer may be sent (freight prepaid) to our factory. Return shipping charges will be paid by Multi-Tech Systems.

Include the following with your ProxyServer:

- a description of the problem.
- return billing and return shipping addresses.
- contact name and phone number.
- check or purchase order number for payment if the ProxyServer is out of warranty. (Check with your technical support specialist for the standard repair charge for your ProxyServer).
- if possible, note the name of the technical support specialist with whom you spoke.

If you need to inquire about the status of the returned product, be prepared to provide the **serial number** of the product sent.

Send your ProxyServer to this address:

MULTI-TECH SYSTEMS, INC.

2205 WOODALE DRIVE

MOUNDS VIEW, MINNESOTA 55112

ATTN: SERVICE OR REPAIRS

You should also check with the supplier of your ProxyServer on the availability of local service and/or loaner units in your part of the country.

The Multi-Tech BBS

For customers who do not have Internet access, Multi-Tech maintains a bulletin board system (BBS). Information available from the BBS includes new product information, product upgrade files, and problem-solving tips. The phone number for the Multi-Tech BBS is (800) 392-2432 (USA and Canada) or (612) 785-3702 (international and local).

The BBS can be accessed by any asynchronous modem operating at 1200 bps to 56K bps at a setting of 8 bits, no parity, and 1 stop bit (8-N-1).

To Log on to the Multi-Tech BBS

1. Set your communications program to **8-N-1**.
2. Dial our BBS at (800) 392-2432 (USA and Canada) or (612) 785-3702 (international and local).
3. At the prompts, type your first name, last name, and password; then press ENTER. If you are a first time caller, the BBS asks if your name is spelled correctly. If you answer yes, a questionnaire appears. You must complete the questionnaire to use the BBS on your first call.
4. Press ENTER until the Main Menu appears. From the Main Menu you have access to two areas: the Files Menu and News. For help on menu commands, type **?**.

To Download a File

If you know the file name

1. From the Main Menu, type **F** to access the Files Menu, then type **D**.
2. Enter the name of the file you wish to download from the BBS.
3. If a password is required, enter the password.
4. Answer **Y** or **N** to the automatic logoff question.
5. Select a file transfer protocol by typing the indicated letter, such as **Z** for Zmodem (the recommended protocol).
6. If you select Zmodem, the transfer will begin automatically. If you select another protocol, you may have to initiate the transfer yourself. (In most data communications programs, the PAGE DOWN key initiates the download.)
7. When the download is complete, press ENTER to return to the File Menu.
8. To exit the BBS, type **G** and press ENTER.

If you don't know the file name

1. From the Main Menu, type **F** to access the Files Menu. For a list of file areas, type **L**, press ENTER, then type **L** and press ENTER again. (If you do not type the second **L**, you will list all of the files on the BBS.)
2. Mark each file area you would like to examine by typing its list number and pressing ENTER.
3. Enter **L** to list all the files in the selected file areas. Enter **C** to go forward in the file list and **P** to go back.
4. To mark one or more files for download, type **M**, press ENTER, type the list numbers of the files, and press ENTER again.

5. Enter **D**. You will see a list of the files you have marked. Enter **E** if you would like to edit the list; otherwise enter **D** again to start the download process.
6. Select a file transfer protocol by typing the indicated letter, such as **Z** for Zmodem (the recommended protocol).
7. If you select Zmodem, the file will transfer automatically. If you select another protocol, you may have to initiate the transfer yourself. (In most data communications programs, the PAGE DOWN key initiates the download.)
8. When the download is complete, press ENTER to return to the File Menu.
9. To exit the BBS, type **G** and press ENTER.

About CompuServe

In addition to the BBS, Multi-Tech provides support through CompuServe's Modem Vendor Forum (GO MODEMVEN). Refer to your CompuServe documentation for special operating procedures.

About the Internet

Multi-Tech is a commercial user on the Internet, and we retrieve messages from our customers on a periodic basis. If you prefer to receive technical support via the Internet, you can contact Tech Support at the following address:

http://www.multitech.com/_forms/email_tech_support.htm

Multi-Tech's presence includes a Web site at:

<http://www.multitech.com>

and an ftp site at:

<ftp://ftp.multitech.com>

About the Multi-Tech Fax-Back Service

Multi-Tech's fax-back system provides 24-hour access to sales, marketing, and technical literature. Dial 612-717-5888, follow the voice prompts, and request document number 10 for a catalog of available documents. For convenience, have your fax number handy:

_____. From the catalog of available documents, you can order newsletters, white papers, press releases, etc. from the sales and marketing index (pages 1-4), or order basic modem operation and troubleshooting guides from the technical support and engineering index. Just enter the applicable FB Doc. # from the left column of the catalog.

ProxyServer

Internet Access / Firewall

Appendixes

Appendix A - TCP/IP (Transmission Control Protocol/Internet Protocol) Description

TCP/IP is a protocol suite and related applications developed for the U.S. Department of Defense in the 1970s and 1980s specifically to permit different types of computers to communicate and exchange information with one another. TCP/IP is currently mandated as an official U.S. Department of Defense protocol and is also widely used in the UNIX community.

Before you install TCP/IP on your network, you need to establish your Internet addressing strategy. First, choose a domain name for your company. A domain name is the unique Internet name, usually the name of your business, that identifies your company. For example, Multi-Tech's domain name is multitech.com (.com indicates this is a commercial organization; .edu denotes educational organizations, .gov denotes government organizations). Next, determine how many IP addresses you'll need. This depends on how many individual network segments you have, and how many systems on each segment need to be connected to the Internet. You'll need an IP address for each network interface on each computer and hardware device.

IP addresses are 32 bits long and come in two types: network and host. Network addresses come in five classes: A, B, C, D, and E. Each class of network address is allocated a certain number of host addresses. For example, a class B network can have a maximum of 65,534 hosts, while a class C network can have only 254. The class A and B addresses have been exhausted, and the class D and E addresses are reserved for special use. Consequently, companies now seeking an Internet connection are limited to class C addresses.

Early IP implementations ran on hosts commonly interconnected by Ethernet local area networks (LAN). Every transmission on the LAN contains the local network, or medium access control (MAC), address of the source and destination nodes. The MAC address is 48-bits in length and is non-hierarchical; MAC addresses are never the same as IP addresses.

When a host needs to send a datagram to another host on the same network, the sending application must know both the IP and MAC addresses of the intended receiver. Unfortunately, the IP process may not know the MAC address of the receiver. The Address Resolution Protocol (ARP), described in RFC 826 (<http://info.internet.isi.edu:80/in-notes/rfc/files/rfc826.txt>) provides a mechanism for a host to determine a receiver's MAC address from the IP address. In the process, the host sends an ARP packet in a frame containing the MAC broadcast address; and then the ARP request advertises the destination IP address and asks for the associated MAC address. The station on the LAN that recognizes its own IP address will send an ARP response with its own MAC address. An ARP message is carried directly in an IP datagram.

Other address resolution procedures have also been defined, including those which allow a diskless processor to determine its IP address from its MAC address (Reverse ARP, or RARP), provides a mapping between an IP address and a frame relay virtual circuit identifier (Inverse ARP, or InARP), and provides a mapping between an IP address and ATM virtual path/channel identifiers (ATMARP).

The TCP/IP protocol suite comprises two protocols that correspond roughly to the OSI Transport and Session Layers; these protocols are called the Transmission Control Protocol and the User Datagram Protocol (UDP). Individual applications are referred to by a port identifier in TCP/UDP messages. The port identifier and IP address together form a "socket". Well-known port numbers on the server side of a connection include 20 (FTP data transfer), 21 (FTP control), 23 (Telnet), 25 (SMTP), 43 (whois), 70 (Gopher), 79 (finger), and 80 (HTTP).

TCP, described in RFC 793 (<http://info.internet.isi.edu:80/in-notes/rfc/files/rfc793.txt>) provides a virtual circuit (connection-oriented) communication service across the network. TCP includes rules for formatting messages, establishing and terminating virtual circuits, sequencing, flow control, and error correction. Most of the applications in the TCP/IP suite operate over the "reliable" transport service provided by TCP.

UDP, described in RFC 768 (<http://info.internet.isi.edu:80/in-notes/rfc/files/rfc768.txt>) provides an end-to-end datagram (connectionless) service. Some applications, such as those that involve a simple query and response, are better suited to the datagram service of UDP because there is no time lost to virtual circuit establishment and termination. UDP's primary function is to add a port number to the IP address to provide a socket for the application.

The Application Layer protocols are examples of common TCP/IP applications and utilities, which include:

- Telnet (Telecommunication Network): a virtual terminal protocol allowing a user logged on to one TCP/IP host to access other hosts on the network, described in RFC 854 (<http://info.internet.isi.edu:80/in-notes/rfc/files/rfc854.txt>).
- FTP: the File Transfer Protocol allows a user to transfer files between local and remote host computers per RFC 959 (<http://info.internet.isi.edu:80/in-notes/rfc/files/rfc959.txt>).
- Archie: a utility that allows a user to search all registered anonymous FTP sites for files on a specified topic.
- Gopher: a tool that allows users to search through data repositories using a menu-driven, hierarchical interface, with links to other sites, per RFC 1436 (<http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1436.txt>).
- SMTP: the Simple Mail Transfer Protocol is the standard protocol for the exchange of electronic mail over the Internet, per RFC 821 (<http://info.internet.isi.edu:80/in-notes/rfc/files/rfc821.txt>).
- HTTP: the Hypertext Transfer Protocol is the basis for exchange of information over the World Wide Web (WWW). Various versions of HTTP are in use over the Internet, with HTTP version 1.0, per RFC 1945 (<http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1945.txt>) being the most current.
- HTML: WWW pages are written in the Hypertext Markup Language (HTML), an ASCII-based, platform-independent formatting language, per RFC 1866 (<http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1866.txt>).
- Finger: used to determine the status of other hosts and/or users, per RFC 1288 (<http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1288.txt>).
- POP: the Post Office Protocol defines a simple interface between a user's mail reader software and an electronic mail server; the current version is POP3, described in RFC 1460 (<http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1460.txt>).
- DNS: the Domain Name System defines the structure of Internet names and their association with IP addresses, as well as the association of mail, name, and other servers with domains.
- SNMP: the Simple Network Management Protocol defines procedures and management information databases for managing TCP/IP-based network devices. SNMP, defined by RFC 1157 (<http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1157.txt>) is widely deployed in local and wide area network. SNMP Version 2 (SNMPv2), per RFC 1441 (<http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1441.txt>) adds security mechanisms that are missing in SNMP, but is also more complex.
- Ping: a utility that allows a user at one system to determine the status of other hosts and the latency in getting a message to that host. Ping uses ICMP Echo messages.
- Whois/NICNAME: Utilities that search databases for information about Internet domain and domain contact information, per RFC 954 (<http://info.internet.isi.edu:80/in-notes/rfc/files/rfc954.txt>).
- Traceroute: a tool that displays the route that packets will take when traveling to a remote host.

Internet Protocol (IP)

IP is the Internet standard protocol that tracks Internetwork node addresses, routes outgoing messages and recognizes incoming messages, allowing a message to cross multiple networks on the way to its final destination. The IPv6 Control Protocol (IPV6CP) is responsible for configuring, enabling, and disabling the IPv6 protocol modules on both ends of the point-to-point link. IPV6CP uses the same packet exchange mechanism as the Link Control Protocol (LCP). IPV6CP packets are not exchanged until PPP has reached the Network-Layer Protocol phase. IPV6CP packets received before this phase is reached are silently discarded. (See also TCP/IP.)

Before you install TCP/IP on your network, you need to establish your Internet addressing strategy. You first choose a domain name for your company. A domain name is the unique Internet name, usually the name of your business, that identifies your company. For example, Multi-Tech's domain name is multitech.com (where .com indicates this is a commercial organization; .edu denotes educational organizations, .gov denotes government organizations). Next, you determine how many IP addresses you'll need. This depends on how many individual network segments you have, and how many systems on each segment need to be connected to the Internet. You need an IP address for each network interface on each computer and hardware device.

IP addresses are 32 bits long and come in two types: network and host. Network addresses come in five classes: A, B, C, D, and E. Each class of network address is allocated a certain number of host addresses. For example, a class B network can have a maximum of 65,534 hosts, while a class C network can have only 254. The class A and B addresses have been exhausted, and the class D and E addresses are reserved for special use. Consequently, companies now seeking an Internet connection are limited to class C addresses. The current demand for Internet connections will exhaust the current stock of 32-bit IP addresses. In response, Internet architects have proposed the next generation of IP addresses, Ipng (IP Next Generation). It will feature 16-byte addressing, surpassing the capacities of 32-bit IP. Still in its design phase, IPng is not expected to be widely deployed before late 1997.

An IP address can serve only a single physical network. Therefore, if your organization has multiple physical networks, you must make them appear as one to external users. This is done via "subnetting", a complex procedure best left to ISPs and others experienced in IP addressing. Since IP addresses and domain names have no inherent connection, they are mapped together in databases stored on Domain Name Servers (DNS). If you decide to let an Internet Service Provider (ISP) administer your DNS server, the ISP can assist you with the domain name and IP address assignment necessary to configure your company's site-specific system information. Domain names and IP addresses are granted by the InterNIC. To check the availability of a specific name or to obtain more information, call the InterNIC at (703)742-4777, or visit the InterNIC web site at <http://www.internic.com>.

Index F

A

About CompuServe	54
About the Internet	54
About the Multi-Tech Fax-Back Service	54
Adding Proxy Applications	35
Applications	39
Archie	57

B

Back Panel	9
Connectors	9
BBS	53

C

Cabinet Mounting Screw	13
Cabling Your ProxyServer	14
Changing IP Parameters	32
Changing WAN Port Parameters	34
Command Connector	9
CompuServe	54
Configuration Port Setup	29
Connectors	9
10Base-T	9
Command	9
Ethernet 1 and 2	9
Power	9
RS232/V.35	9

D

Data Communications Equipment	9
DCE. <i>See</i> Data Communications Equipment	
Default WAN Link Configuration	21
DHCP Client	20, 32
DHCP Relay Agent	20, 32
DHCP Server	36
DNS	57
Download Default Setup	29
Download Firmware Update	30

E

Enabling PPP/SLIP	37
Enabling the DHCP Server	36
Ethernet 1 and 2 Connectors	9

Fax-Back Service	54
Filtering	40
Finger	57
Firewall Configuration	31
Firewall Program Group	29
Firewall Software	24
Front Panel	8
LEDs	8
FTP	57

G

Gopher	57
--------------	----

H

HTML	57
HTTP	57

I

Internet	54
Internet Gateway Parameters	33
Internet LAN Port Parameters	20, 32
Internet Protocol	56, 58
Internet Services Network	6
IP	58
IP Parameters	32
IP Port Configuration	20

L

LEDs	8
ETHERNET 1 and 2	8
Fail	8
Power	8
WAN Link	8
Limited Warranty	50
Loading Your Software	18

O

On-line Warranty Registration	50
-------------------------------------	----

P

Ping	57
POP	57
Power Connector	9
PPP/SLIP	37
Program Group	29
Proxy Applications	35

R

Remote Configuration	42
LAN-Based Procedure	44
Modem-Based Procedure	42
Remote Management	46
Telnet	46
WEB Management	48
RS232/V.35 Connector	9

S

Safety Warnings	12
Secured LAN Port Parameters	20, 32
Service	52
Shunt Positions	13
SMTP	57
SNMP	57
Software	24
Applications	39
Configuration Port Setup	29
DHCP Server	36
Download Default Setup	29
Download Firmware Update	30
Filtering	40
Firewall Configuration	31
IP Parameters	32
Loading	18
PPP/SLIP	37
Program Group	29
Proxy Applications	35
Statistics	39
Uninstall Firewall Configuration	30
WAN Device Configuration	30
WAN Port Parameters	34
Specifications	10
Statistics	39

T

TCP/IP	56
Tech Support	51
Technical Specifications	10
Telnet	46, 57
The Multi-Tech BBS	53
Traceroute	57
Transmission Control Protocol	56
Typical Applications	24
Configuration 1 - Cable/DSL Modem	24
Configuration 2 - Existing Dual-LAN with Router	26
Configuration 3 - New Dual-LAN with T1 DSU	27

U

Uninstall Firewall Configuration	30
Unpacking Your ProxyServer	12

V

V.35 Shunt	13
V.35 Shunt Procedure	13

W

WAN Device Configuration	30
WAN Port Parameters	20, 33, 34
Warranty	50
On-line Warranty Registration	50
WEB Management	48
Whois/NICNAME	57