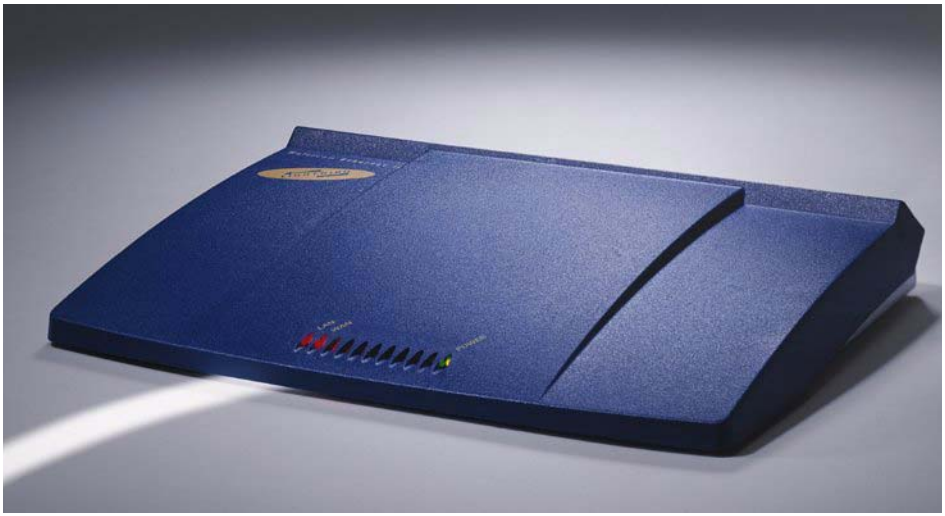
MultiCom Firewall



User's Manual

For Firmware 3.7 -10/19/04

LIGHTNING Instrumentation SA

Avenue des Boveresses 50
Lausanne, Vaud 1010
Switzerland
Phone +41.21.654.2000
Fax +41.21.654.2001
http://www.lightning.ch
info@lightning.ch

APLIWARE SA

rue du Grand-Pré 70
1222 Geneva 2
Switzerland
Phone +41.22.918.3610
Fax +41.22.918.3695
http://www.apliware.com
info@apliware.com

Copyright, Warranty, Liability

Copyright

The technical information in this document is proprietary to LIGHNTING S.A. and APLIWARE S.A. and the recipient has a personal, non-exclusive and non-transferable license to use this information solely with the use of LIGHNTING S.A. and APLIWARE S.A. products.

The information in this document is subject to change without notice. Revisions may be issued at any time.

Trademarks

MultiCom and Lightning are registered trademarks of LIGHTNING Instrumentation SA. Stac LZS and Hi/fn are registered trademarks of Hi/fn, Inc. All other company, brand and product names may be registered trademarks or trademarks of their respective companies and are hereby recognized.

Revisions

This publication and the information herein is furnished AS IS, subject to change without notice, and should not be construed as a commitment by LIGHNTING S.A. and APLIWARE S.A. Furthermore, LIGHNTING S.A. and APLIWARE S.A. assumes no responsibility or liability for any errors or inaccuracies, makes no warranty of any kind (express, implied or statutory) with respect to this publication, and expressly disclaims any and all warranties of merchantability, fitness for particular purposes and noninfringement of third-party right.

Warranty

NO WARRANTIES ARE EXTENDED BY THIS DOCUMENT. The only product warranties made by LIGHNTING S.A. and APLIWARE S.A., if any, are set forth in the agreed terms and

conditions for the purchase of LIGHNTING S.A. and APLIWARE S.A. products. LIGHNTING S.A. and APLIWARE S.A. declaims liability for any and all direct and indirect damages that may result from publication or use of this document and/or its contents.

LIGHNTING S.A. and APLIWARE S.A. warrants all hardware products of its manufacture to be free from defects in material and workmanship for 12 months from date of delivery. Upon prompt notification by the purchaser, LIGHNTING S.A. and APLIWARE S.A. will correct, within the warranty period, any defects in equipment of its manufacture either by repair at its factory or by supply of replacement parts to the purchaser.

LIGHNTING S.A. and APLIWARE S.A. must decide to its own satisfaction that the equipment is defective and has not developed malfunctions as a result of misuse, modification, or abnormal conditions of operation. Damages due to over voltage (e.g. lightning strokes) or wrong cabling on any interface are expressly excluded from the warranty. Opening the products also voids the warranty. LIGHNTING S.A. and APLIWARE S.A. assumes no liability for consequential damages, and its liability shall in no case exceed the original purchase price of the equipment.

The warranties set forth above are the sole warranties applicable to LIGHNTING S.A. and APLIWARE S.A. products. THE IMPLIED WARRANTY OF MERCHANTABILITY AND ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, ARE EXCLUDED.

Limitation of Liability

UNDER NO CIRCUMSTANCES, INCLUDING NEGLIGENCE, SHALL LIGHNTING S.A. AND APLIWARE S.A. BE LIABLE FOR LOSS OF USE, INTERRUPTION OF BUSINESS, OR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY KIND (INCLUDING LOST PROFITS) REGARDLESS OF THE FORM OF ACTION WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT PRODUCT LIABILITY OR OTHERWISE, EVEN IF LIGHNTING S.A. AND APLIWARE S.A. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

In no event shall LIGHNTING S.A. and APLIWARE S.A. be liable for costs of procurement of substitute goods. The potential liability of LIGHNTING S.A. and APLIWARE S.A. arising out of this product is in

any case limited to the purchase price paid to LIGHNTING S.A. and APLIWARE S.A. for its products.

Software and Documentation License

The software and documentation included in or with products of LIGHNTING S.A. and APLIWARE S.A. is subject to following licence.

Third-Party Software. A part of the software used within the MultiCom Ethernet series can be freely distributed under the terms of the GNU Public License and BSD copyright. However, some applications remain the property of their owners, and require their permission to redistribute. For a complete listing of the software used within the MultiCom Firewall, and the terms under which it can be distributed, refer to the LIGHTNING Web site at http://www.lightning.ch/ and to the Appendix on Additional Licenses and Copyrights.

Shareware and Freeware Software. Your MultiCom Companion CD contains shareware, freeware and other 3rd Party software not developed by LIGHNTING S.A. and APLIWARE S.A. Such software is neither warranteed or supported by LIGHNTING S.A. and APLIWARE S.A. and is not necessary to use LIGHNTING S.A. and APLIWARE S.A. products. If you wish to use it be sure to check that it meets your company's standards for reliability, security and useability. Please check with the developer of the software for any necessary information about the use or capabilities of such included software.

While all included software on this CD has been virus checked and tested LIGHNTING S.A. and APLIWARE S.A. does not provide any guarantees concerning these products. Be sure to use any virus protection that is required by your company before using the included software. If you go to a website of these software developers be sure to virus check any software that you download from them before using it as well.

LIGHNTING S.A. and APLIWARE S.A. cannot accept responsibility for any disruption, damage and/or loss to your data or computer system that may occur while using these programs. If you are unsure about what you are doing check with your network administrator before installing any software.

License. The software, on any media, including disk, read-only memory, and flash memory and the products related documentation are licensed to you by LIGHNTING S.A. and APLIWARE S.A.. You own the media on which the LIGHNTING S.A. and APLIWARE S.A. software is recorded, but LIGHNTING S.A. and APLIWARE S.A. and/or

LIGHNTING S.A. and APLIWARE S.A.'s Licensor(s) retain title to the LIGHNTING S.A. and APLIWARE S.A. software and related documentation. The license allows you to use the LIGHNTING S.A. and APLIWARE S.A. software on a single LIGHNTING S.A. and APLIWARE S.A. hardware product. In the case of software on disk, you are allowed to make one copy of LIGHNTING S.A. and APLIWARE S.A. software in machine-readable form for backup purposes only. You must reproduce on such copy the LIGHNTING S.A. and APLIWARE S.A. copyright notice and any other proprietary legends that were on the original copy of the disk containing LIGHNTING S.A. and APLIWARE S.A. software. You may also transfer all your license rights in the LIGHNTING S.A. and APLIWARE S.A. software, together with the associated hardware, the backup copy, the related documentation, and a copy of this license to another party, provided the other party reads and agrees to accept the terms and conditions of this license.

Restrictions. The LIGHNTING S.A. and APLIWARE S.A. software contains copyrighted materials, trade secrets, and other proprietary materials and in order to protect them you may not decompile, reverse engineer, disassemble, or otherwise reduce the LIGHNTING S.A. and APLIWARE S.A. software to a human-perceivable form. You may not modify, network, rent, lease, loan, distribute, or create derivative works based upon the LIGHNTING S.A. and APLIWARE S.A. software in whole or in part. You may not electronically transmit the LIGHNTING S.A. and APLIWARE S.A. software from one computer to another or over a network.

Termination. This license is effective until terminated. You may terminate this license at any time by destroying the LIGHNTING S.A. and APLIWARE S.A. software, the related hardware, related documentation and all copies thereof. The license will terminate immediately without notice from LIGHNTING S.A. and APLIWARE S.A. if you fail to comply with any provision of this license. Upon termination you must destroy the LIGHNTING S.A. and APLIWARE S.A. software, the related hardware, related documentation and all copies thereof.

Limited Warranty on Media. LIGHNTING S.A. and APLIWARE S.A. warrants the media on which the software is recorded as its hardware materials, and limits the liability as set for the hardware material.

Disclaimer of warranty on LIGHNTING S.A. and APLIWARE S.A. software. You expressly acknowledge and agree that use of

the LIGHNTING S.A. and APLIWARE S.A. software is at your sole risk. The LIGHNTING S.A. and APLIWARE S.A. software and related documentation are provided "AS IS" and without warranty of any kind and LIGHNTING S.A. and APLIWARE S.A. EXPRESSLY DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. LIGHNTING S.A. AND APLIWARE S.A. DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE LIGHNTING S.A. AND APLIWARE S.A. SOFTWARE WILL MEET YOUR REQUIREMENTS, OR THAT THE OPERATION OF THE LIGHNTING S.A. AND APLIWARE S.A. SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT DEFECTS IN THE LIGHNTING S.A. AND APLIWARE S.A. SOFTWARE WILL BE CORRECTED. FURTHERMORE, LIGHNTING S.A. AND APLIWARE S.A. DOES NOT WARRANT OR MAKE ANY REPRESENTATIONS REGARDING THE USE OR THE RESULTS OF THE USE OF THE LIGHNTING S.A. AND APLIWARE S.A. SOFTWARE OR RELATED DOCUMENTATION IN THE TERMS OF THEIR CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY LIGHNTING S.A. AND APLIWARE S.A. OR A LIGHNTING S.A. AND APLIWARE S.A.-AUTHORIZED REPRESENTATIVE SHALL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF THIS WARRANTY. SHOULD THE LIGHNTING S.A. AND APLIWARE S.A. SOFTWARE PROVE DEFECTIVE, YOU (AND NOT LIGHNTING S.A. AND APLIWARE S.A. OR A LIGHNTING S.A. AND APLIWARE S.A. AUTHORIZED REPRESENTATIVE) ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICING, REPAIR, OR CORRECTION. Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

Limitation of Liability. Conforming to the general limitation of liability.

Controlling Law and Severability. This license shall be governed by and construded in accordance with the laws of Switzerland and Canton de Vaud, as applied to agreements entered into and to be performed entirely between Canton de Vaud residents. If for any reason a court of competent jurisdiction finds any

provision of this license, or portions thereof, to be unenforceable, that provision of the license shall be enforced to the maximum extent permissible so as to effect the intent of the parties, and the remainder of this license shall continue in full force and effect.

Complete agreement. The license constitutes the entire agreement between the parties with respect to the use of the LIGHNTING S.A. and APLIWARE S.A. software and related documentation, and supersedes all prior or contemporaneous understandings or agreements, written or oral, regarding such subject matter. No amendment to or modification of the License will be binding unless in writing and signed by a duly authorized representative of LIGHNTING S.A. and APLIWARE S.A..

Export

Some versions and options of LIGHNTING S.A. and APLIWARE S.A.'s Software and Hardware, including technical data, may be subject to Swiss, E.U., U.S. (including the U.S. Export Administration Act) or other countries export control laws, and their associated regulations, and may be subject to export or import regulations in other countries. Customer agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import Software and Hardware.

Contents

Contents

Preface

Chapter 1

Your New MultiCom Firewall

Congratulations on the purchase of your MultiCom Firewall. Your firewall has been designed to offer security and high performance networking management, all through an easy to use interface.

Whether you are connecting a single computer from home or managing a company network you will find that the MultiCom Firewalls can help. You now have access to many networking possibilities, for instance you can secure your data, share your Internet connection with multiple computers and filter or receive notifications of potential network attacks.

For the latest release notes, documentation, firmware and software check the Lightning website at http://www.lightning.ch/support.

MultiCom Firewall Features

Security

- Dual firewalls, using Stateful Packet Inspection (SPI) Filtering and/ or a NAT based Firewall on each interface to protect against External Intrusions, Denial

of Service (DoS), Port Scanning, Spoofing Attacks and more

- URL Filtering to block or drop web connections based on URL or keywords.
- Intrusion Detection System (IDS) using SPI filtering & syslog
- Real time alerts and statistics using Syslog, SNMPv2, web-based Event Monitor, email and more
- Up to 10 separate user accounts with passwords and access rights
- Secure SSL (HTTPS) & SSHv1-2 (telnet CLI) for remote access & configuration
- DMZ interface support giving extra security for network servers (Ethernet III and Enterprise Ethernet only)

Internet Access

- Connect multiple computers and ethernet devices to the Internet using Internet Sharing using Network Address Translation (NAT)
- Easy Setup & Easy Firewall wizards via the web interface or the multi-platform Configurator software
- DNS Cache for faster Internet response
- Dynamic DNS supporting 9 different services for finding your computer even if the IP address changes
- Multimedia (H.323, IRC, ICQ) and PPTP client pass through support with NAT
- DHCP server (up to 1,000 clients) for automatic IP configuration to clients or DHCP Relay on any Interface
- Ethernet parameter editing for MTU, MAC address, duplex and speed
- Integrated PPPoE client, for single or multiple concentrators (for ISP backup purposes)
- Network traffic round-robin load sharing using NAT
- Virtual IP address support for one or more IP addresses using ARP Proxy and Network Address Translation
- IP Port Redirection with NPAT Network Port & Address Translation
- Static and dynamic routing using RIP (V1 and v2)

Management

- Configurator software for configuring Virtual Private Networks, validating configurations, managing all features and firewall rules. Available for

Windows, Macintosh, and Linux. With secured remote access.

- Monitor software to manage status and restart services like PPP, IPSec, VRRP, DHCP. Available for Windows, Macintosh, and Linux. With secured remote access.
- Configuration scheduling for up to 6 configuration files based on day, hour or minute.
- Telnet, console & ssh Command Line Interface (CLI) with powerful network tools like ping, traceroute name server lookup. Ideal for scriptable configuration changes using 3rd party software like CatTools for time based and centralized management
- Quick Restore Button with LED feedback to load boot config, emergency config (config 1), or the factory default configuration. Additional memory is available on each device to store up to 6 different configurations.
- Centralized time management using the Network Time Protocol
- Transfer configurations to and from the device using the File Transfer Protocol (FTP)
- Built-in Domain Name Server (DNS) to name local computers
- Multilingual with English, French and German built-in
- Upgradable flash memory

Software Add-on Options

- IPSec based Virtual Private Network (VPN) supporting Gateway, client and point-to-point modes. Preshared, Manual and PKI x.509 Keys for central management and 3rd party vendor compatibility. Support for multiple world-class encryption ciphers such as AES (Rijndael), CAST 128, Twofish, Blowfish, 3DES and more. Includes Dead Peer Detection (DPD), NAT Traversal, DHCP over IPSec, Traffic filtering, Domain Name endpoints, Connection testing support.
- SSH Port Forwarding VPN Gateway with public key or user based access, using SSH v1 and v2. With unique authentication for up to 10 users.
- High Availability using the VRRP protocol with authentication
- Network Intrusion Detection System (NIDS) using SNORT for Enterprise devices
- Network Monitoring Service for monitoring local and remote TCP servers.
- Certificate Manager software for generating, managing and deploying PKI x.509 keys, certificates and certification authorities. Available for Windows,

Macintosh, and Linux.

- VPN Client software available

Network Hardware

- 10/100 Mbit/s multi-interface Switch for high-speed communication within your network (Ethernet III & Enterprise Ethernet only)
- 10/100 Mbit/s autosensing LAN interface for your Local network
- DSL annex A integrated modem (Enterprise DSL only)
- 802.11b WiFi with LAN Bridge (Enterprise WiFi only)

Options

Certain functionalities, such as IPSec VPN, SSH Port Forwarding VPN, High Availability or Network Monitoring are not immediately available in the standard firmware releases. These functions are called Options and need to be purchased and activated to be useable.

Activation of Options currently requires the user to install a unique key file (versions before 3.4 required a special firmware) containing the purchased options and then reboot the MultiCom Firewall. Currently the options are available IPSec VPN 2 tunnels, IPSec VPN 20 tunnels and unlimited IPSec VPN tunnel options.

- IPSec VPN 2 Tunnels
- IPSec VPN 20 Tunnels
- IPSec VPN unlimited Tunnels
- SSH Port Forwarding VPN 10 Users
- High Availability (VRRP)
- Network Monitoring

Below are the requirements of this process:

- The option key or firmware is only valid on the machine for which it was purchased.
- For machines using a Lightning Linux older than 3.2, you must either first upgrade to the standard OS 3.2 and then apply the firmware with the option or upgrade to at least OS 3.4 and apply the option key.

Contact your distributor if you are interested in purchasing this option.

IPSec VPN Option

All existing MultiCom Firewalls offer Virtual Private Networks (VPN) using the IPSec protocol when the IPSec option is purchased. This is a powerful Secure Remote Access add-on to the standard MultiCom Firewall functionality. Using IPSec the MultiCom Firewall becomes a security gateway, securing data transfers between other IPSec capable devices or computers running IPSec software.

Simple IPSec configuration can be made using the web based wizard. Advanced IPSec configurations require the use of the Configurator software (included on the MultiCom Companion CDROM) in the Advanced Configuration mode. Refer to the Lightning-Linux Reference Manual for information on configuring this feature.

Optionally, the Certificate Manager can be purchased to manage and deploy PKI Digital Authentication Certificates for more complex IPSec configurations.

For more information or to purchasing this option contact your distributor.

SSH VPN Option

All existing MultiCom Firewalls offer Virtual Private Networks (VPN) using the SSH Port Forwarding protocol when the SSH option is purchased. This is a powerful Secure Remote Access add-on for the standard MultiCom Firewall functionality. Using SSH Port Forwarding the MultiCom Firewall also becomes a security gateway, securing data transfers between remote SSH software on a Macintosh, Windows, Linux, PDA or other computing platform.

All SSH Port Forwarding configurations require the use of the Configurator software (included on the MultiCom Companion CDROM) in the Advanced Configuration mode. Refer to the Lightning-Linux Reference Manual for information on configuring this feature.

For more information or to purchasing this option contact your distributor.

High Availability Option

All existing MultiCom Firewalls support High Availability using the Virtual Router Redundancy Protocol (VRRP) when the VRRP option is purchased. VRRP allows 1 or more additional MultiCom Firewalls to be configured into a

redundant fail-safe backup in case of failure on the Master firewall. This High Availability does not require dynamic routing or router discovery protocols to be installed on local networking devices.

All VRRP configurations require the use of the Configurator software (included on the MultiCom Companion CDROM) in the Advanced Configuration mode. Refer to the Lightning-Linux Reference Manual for information on configuring this feature.

For more information or to purchasing this option contact your distributor.

Network Monitoring Option

All existing MultiCom Firewalls support Network Monitoring when the Network Monitoring Service (NMS) option is purchased. NMS allows the MultiCom Firewall to maintain a list of TCP ports on local and remote networks and regular intervals check if the connection is available and measure the delay time. The results of these status checks are written to the internal log, optionally can be emailed to selected email accounts, and is visible from the web interface and the Monitor software.

All NMS configurations require the use of the Configurator software (included on the MultiCom Companion CDROM) in the Advanced Configuration mode. Refer to the Lightning-Linux Reference Manual for information on configuring this feature.

For more information or to purchasing this option contact your distributor.

About This Manual

Putting together a solution to meet your networking needs is not always an easy task. Whether you are a seasoned professional or a new home-user you will find there are many possibilities you may have not have considered. This manual is designed to get your firewall up and started as soon as possible. To better understand the more advanced features of your firewall please refer to the Lightning-Linux Reference Manual.

While every attempt has been made to explain the features and configuration steps of your new firewall you should have some basic experience in the following areas.

- familiarity with general computer usage

- understanding of basic networking (if not check out the technology overview sections at the end of this manual first.)
- connecting to a network (you still need to have a working connection to either the Internet or a local network: check with your local administrator or Internet Service Provider for assistance in getting that connection up and running.)

Working with the Internet requires knowing many technical acronyms. Please refer to the “Glossary” on page 147 for short descriptions of many of these buzzwords and technologies.

Conventions

The following tables describe the typefaces and symbols used in this manual.

Table 1: Typography

Typography	Meaning
`Computer Output`	is data generally displayed or presented by the computer
`User Input`	is text or commands that you type, contrasted with onscreen computer output
`Button`	is the text on a button, used to describe what button to click
`Menu`	indicates the name of a menu or tab that takes you to specific options
`MENU` > `BUTTON`	describes which buttons to click and the order to click on them for a specific action to occur: for example `FILE` > `PRINT` says to click on the menu named “File” and then the Menu item named “Print”.

Table 2: Symbols

Symbol	Meaning
NOTE -	Notes describe particular features which require attention
CAUTION -	Cautions explains conditions that may cause unwanted results
TIP -	Tips offer useful suggestions

Packaging Contents

- MultiCom Firewall
- Power supply
- Ethernet Networking cables (x1 blue crossed cable, x1 straight cable)
- Console cable (for the Ethernet III and SpeedSurf only)
- MultiCom Companion CD (including User's Manual, Lightning-Linux Reference Manual, configuration software and miscellaneous shareware and freeware)
- Quick Install Guide

If The Product Is Received Damaged

Forward an immediate request to the delivering carrier to perform an inspection and prepare a damage report. Save the container and packing material until contents are verified.

Report the nature and extent of the damage to Customer Support so that action can be initiated to repair or replace damaged items, or instructions issued for returning items.

The responsibility of the manufacturer ends at the delivery to the first carrier. ALL CLAIMS for loss, damage, or nondelivery must be made against the delivering carrier WITHIN 8 DAYS OF RECEIPT of shipment.

To Return The Product

An Return Material Authorization (RMA) Number from Customer Support is required before returning any item(s). Report the fault or deficiency along with the model, type, and serial number of the item(s) to Customer Support. Upon receipt of this information, Customer Support will provide service instructions or shipping information. Clearly mark the RMA number, your address, and shipping address on the original packaging, which has to be used for shipments.

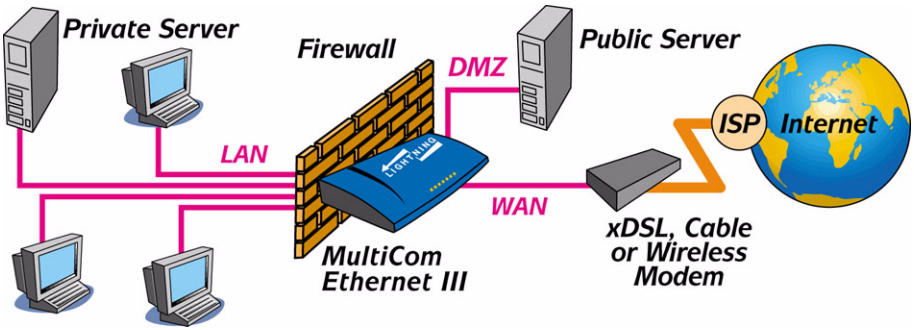
Products returned without an RMA number will be returned to the sender at the sender's expense. Improperly packaged products will not be covered under warranty. For warranty repairs, please include a copy of a dated proof of purchase.

Chapter 2

Introducing The MultiCom Firewalls

MultiCom Firewalls

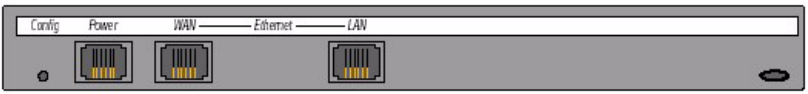
MultiCom Firewalls are available in different hardware configurations to best meet your needs. Each firewall uses Lightning-Linux to provide additional features and options to the hardware. In all cases you can configure your firewall either by using your Internet browser (for Easy Setup, Easy Firewall or Interface configuration) or by using the Configurator software found on your MultiCom Companion CD.



Introducing the Ethernet II

Back Panel

The back panel of your Ethernet II firewall is where all of your cables will connect to.



Config	Push this button and let go when the front LEDs are: ORANGE to load the last saved boot configuration GREEN to load the configuration in memory position 1 RED to load the factory default configuration.
Power	Use the Power interface to connect to the included MultiCom power adapter.
LAN	Use the LAN (Local Area Network) interface to connect to your network devices (workstations, printer servers, network camera) or hub.
WAN	Use the WAN (Wide Area Network) interface to connect to your Broadband modem (xDSL, Cable or Wireless Modem).
Kensington Lock Slot	This connection is to physically secure your Ethernet firewall with a Kensington Lock. It is the oblong whole on the right of the back panel.

Front Panel of the Ethernet II

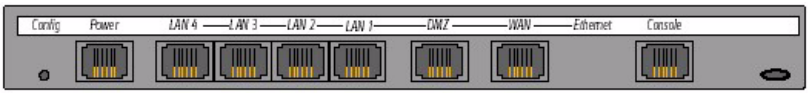
The Front panel of your Ethernet II firewall is where LED lights will inform you of the activity occurring in your firewall.

LAN	Steady GREEN when link is up Blinking ORANGE when traffic is passing Blinking RED when packet collisions occur Steady RED when link is down
WAN	Steady GREEN when link is up Blinking ORANGE when traffic is passing Blinking RED when packet collisions occur Steady RED when link is down
First LED left of Power LED	GREEN when SecureWall is ON ORANGE when filtering is ON and SecureWall is OFF RED when SecureWall and Filtering are OFF
Power	Steady GREEN when power is on

Introducing the Ethernet III

Back Panel

The back panel of your Ethernet III firewall is where all of your cables will connect to.



Config	Push this button and let go when the front LEDs are: ORANGE to load the last saved boot configuration GREEN to load the configuration in memory position 1 RED to load the factory default configuration.
Power	Use the Power interface to connect to the included MultiCom power adapter.
LAN 1-4	Use the 4 LAN (Local Area Network) interfaces to connect to your network devices (workstations, printer servers, network camera).
DMZ	Use the DMZ (Demilitarized Zone) interface to connect public servers (www, ftp...). This port allows customized security for these servers.
WAN	Use the WAN (Wide Area Network) interface to connect to your Broadband modem (xDSL, Cable or Wireless Modem).
Console	Use the console port with the included cable to connect to the serial port of your workstation. This allows you direct access to the CLI (Command Line Interface) an can be used to configure the firewall.
Kensington Lock Slot	This connection is to physically secure your Ethernet firewall with a Kensington Lock. It is the oblong whole on the right of the back panel.

Front Panel of the Ethernet III

The Front panel of your Ethernet III firewall is where LED lights will inform you of the activity occurring in your firewall.

WAN	Steady GREEN when link is up Blinking ORANGE when traffic is passing Blinking RED when packet collisions occur Steady RED when link is down
DMZ	Steady GREEN when link is up Blinking ORANGE when traffic is passing Blinking RED when packet collisions occur Steady RED when link is down
LAN 1-4	Steady GREEN when link is up Blinking ORANGE when traffic is passing Blinking RED when packet collisions occur Steady RED when link is down
Security	GREEN when SecureWall is ON ORANGE when filtering is ON and SecureWall is OFF RED when SecureWall and Filtering are OFF
Power	Steady GREEN when power is on

Introducing the MultiCom SpeedSurf

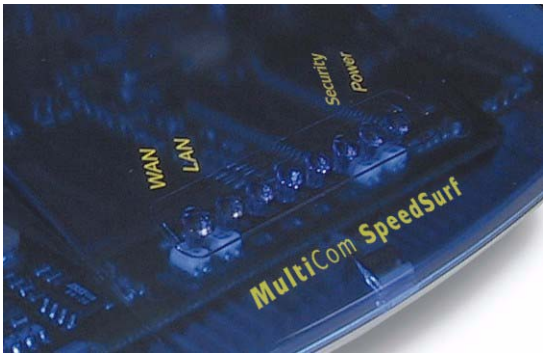
Back Panel

The back panel of your MultiCom SpeedSurf is where all of your cables will connect to.

Config	Push this button and let go when the front LEDs are: ORANGE to load the last saved boot configuration GREEN to load the configuration in memory position 1 RED to load the factory default configuration.
Power	Use the Power interface to connect to the included MultiCom power adapter.
Console	Use the console port with the included cable to connect to the serial port of your workstation. This allows you direct access to the CLI (Command Line Interface) an can be used to configure the firewall.
LAN	Use the LAN (Local Area Network) interface to connect to your network devices (workstations, printer servers, network camera) or hub.
WAN	Use the WAN (Wide Area Network) interface to connect to your Broadband modem (xDSL, Cable or Wireless Modem).
Kensington Lock Slot	This connection is to physically secure your Ethernet firewall with a Kensington Lock. It is the oblong hole on the right of the back panel.

Front Panel of the MultiCom SpeedSurf

The Front panel of your MultiCom SpeedSurf is where LED lights will inform you of the activity occurring in your firewall.

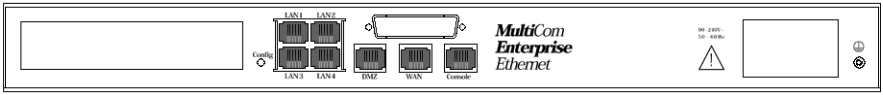


LAN	Steady GREEN when link is up Blinking ORANGE when traffic is passing Blinking RED when packet collisions occur Steady RED when link is down
WAN	Steady GREEN when link is up Blinking ORANGE when traffic is passing Blinking RED when packet collisions occur Steady RED when link is down
Security	GREEN when SecureWall is ON ORANGE when filtering is ON and SecureWall is OFF RED when SecureWall and Filtering are OFF
Power	Steady GREEN when power is on

Introducing the Enterprise Ethernet

Back Panel

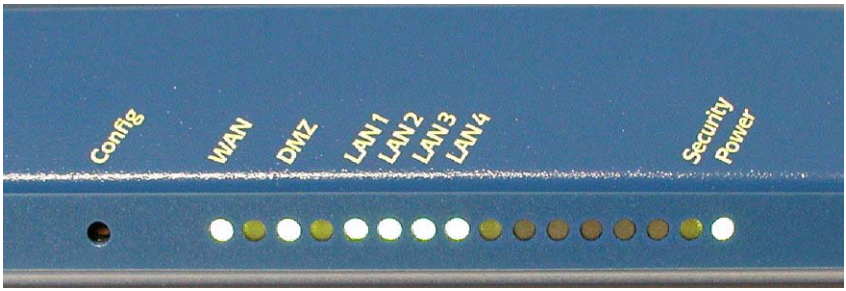
The back panel of your Enterprise Ethernet firewall is where all of your cables will connect to.



Config	Push this button and let go when the front LEDs are: ORANGE to load the last saved boot configuration GREEN to load the configuration in memory position 1 RED to load the factory default configuration.
Power	Use the Power interface to connect to the included MultiCom power adapter.
LAN 1-4	Use the 4 LAN (Local Area Network) interfaces to connect to your network devices (workstations, printer servers, network camera).
DMZ	Use the DMZ (Demilitarized Zone) interface to connect public servers (www, ftp...). This port allows customized security for these servers.
WAN	Use the WAN (Wide Area Network) interface to connect to your Broadband modem (xDSL, Cable or Wireless Modem).
Console	Use the console port with the included cable to connect to the serial port of your workstation. This allows you direct access to the CLI (Command Line Interface) and can be used to configure the firewall.

Front Panel of the Enterprise Ethernet

The Front panel of your Enterprise Ethernet firewall is where LED lights will inform you of the activity occurring in your firewall.



WAN	Steady GREEN when link is up Blinking ORANGE when traffic is passing Blinking RED when packet collisions occur Steady RED when link is down
DMZ	Steady GREEN when link is up Blinking ORANGE when traffic is passing Blinking RED when packet collisions occur Steady RED when link is down
LAN 1-4	Steady GREEN when link is up Blinking ORANGE when traffic is passing Blinking RED when packet collisions occur Steady RED when link is down
Security	GREEN when SecureWall is ON ORANGE when filtering is ON and SecureWall is OFF RED when SecureWall and Filtering are OFF
Power	Steady GREEN when power is on

Network Requirements

- Internet Connection (typically a broadband DSL or cable modem) with a 10Mbps (10–base-T) or 10/100Mbps Autosensing Ethernet connection
- One computer with a 10Mbps, 100Mbps, or 10/100Mbps Autosensing Ethernet interface
- TCP/IP networking protocol for each computer
- (Optionally) a hub or switch to connect more than one computer to your firewall
- (Optionally) Netscape Navigator 4.0 or higher or Microsoft Internet Explorer 4.0 or higher for interaction with the MultiCom Firewalls administrative web server.

NOTE — The Internet Connection can also be an office to office connection such as an ADSL line between two offices and a modem on each side to provide Ethernet connectivity.

Advanced Configuration Software Requirements

For advanced configuration options you may install or run the Configurator Software from your MultiCom Companion CD. Below are the requirements to use this software.

- CD-ROM drive (if installing the Configuration software from CD-ROM)
- Mac OSX, Windows 98, ME, NT4.0, 2000, XP, 2003 or higher, Linux kernel 2.2 or higher, Solaris version 2 or higher
- Pentium CPU, PowerPC CPU or better
- SVGA monitor with at least 800x600 pixel display and 256 colors (more than 256 colors are recommended)
- 64MB of RAM,
- 40 MB of free hard disk space

Safety Precautions

WARNING THERE ARE NO USER SERVICEABLE PARTS INSIDE THIS EQUIPMENT. SERVICE MUST BE PERFORMED BY QUALIFIED SERVICE PERSONNEL. **OPENING CASE VOIDS GUARANTEE**.

VORSICHT KEIN TEIL IM GEHÄUSE KANN VOM BENÜTZER SELBST REPARIERT WERDEN. BITTE WENDEN SIE SICH AN QUALIFIZIERTES WARTUNGSPERSONAL. **DAS ÖFFNEN DES GERÄTES FÜHRT ZUM VERLUST DER GARANTIE.**

ATTENTION CET APPAREIL NE CONTIENT AUCUN ELEMENT QUE L'UTILISATEUR PUISSE REPARER. CONFIEZ LA MAINTENANCE AU PERSONNEL TECHNIQUE QUALIFIE. **L'OUVERTURE DE L'APPAREIL ANNULE LA GARANTIE**.

Chapter 3

Getting Started

This chapter will explain the configuration steps necessary to get your MultiCom Firewall up and running for most local network situations. This includes configuring to connect to your Internet Service Provider through your existing xDSL, cable or wireless modem, and configuring your computers to access the MultiCom Firewall. When you are done you will also have finished setting up the built-in NAT firewall and all of the computers on your local network will be able to access the Internet through your firewall.

Be sure that you have asked your ISP how they expect you to connect to the their services... using DHCP, PPPoE, PPTP, or a static IP Address.

NOTE — The term “Internet” is used to describe the network that you use the MultiCom Firewall to connect to. The MultiCom Firewall that you can also use to connect to other remote computers or servers such as those at another office site. To keep things simple we will refer to the external or WAN network as the “Internet”.

Configuring your MultiCom Firewall can be done in 10 steps as shown below.

1. Connect the MultiCom Firewall
2. Configure your computer to communicate with the MultiCom Firewall

3. Activate any option keys
4. Configure the WAN interface to connect to the Internet, your ISP or your broadband modem
5. Configure the Easy Firewall wizard and optionally redirect specific incoming traffic to computers on your local network that will act as servers on the Internet or need special access
6. Save the Configuration
7. Configure the correct date and time
8. Change the default username and password (be sure to pick a names that you can remember since you cannot retrieve forgotten usernames or passwords)
9. Optionally configure URL Filtering, Stateful Packet Inspection, syslog and email notifications, dynamic and internal DNS.
10. Register your MultiCom Firewall

Advanced configuration such as Syslog/ SNMP messaging, Dynamic DNS, Local Name Server, Interface editing (such as MAC address or link speed), NTP, FTP, customized and standard filters, requires the use of the Configuration Software and is described in the Lightning-Linux Reference Manual. You will also find information there on how to install and use the Configurator software.

Connecting the MultiCom Firewall

Following are the steps to connect your MultiCom Firewall to your existing Ethernet devices. After this physical connection is successful you can begin configuring the MultiCom Firewall.

1. Connect the WAN interface port to your xDSL, cable, wireless modem or router with the included cross-wired cable.
2. Connect the LAN interface port to either your computer ethernet interface (using the blue crossed cable) or to your network hub (using the gray straight cable).
3. Connect the power cable to the MultiCom Firewall.
4. And finally connect the power transformer to the wall outlet.

WARNING - If you are using an Ethernet III you must reverse the LAN cable types. In this case the blue crossed cable is only for connections to a hub and the gray straight cable is only to be connected to your computer.

After this final step your MultiCom Firewall will power on. The boot process will cause flashing lights for about 20 seconds. When the Power, LAN and WAN lights are green then the Firewall is ready for configuration. **If either the LAN or WAN lights remain red then there is a problem with the cable type or the connected Ethernet device is not turned on. Try using a different cable to connect to the modem or computer and verify that the other device is turned on.**

The default boot process loads the "boot" configuration and the WAN interface will begin to search for a DHCP server from your Internet Service Provider. When the WAN and LAN interfaces turn a steady green to show they are connected to a network device or blinking yellow to show that data is passing it will be possible to reach the web server of the firewall. This does not mean that you are connected to your ISP, only that the cable connection between the MultiCom Firewall and the modem, router, computer or hub is good. If you have problems at this point please check the troubleshooting section later in this manual.

The LAN interface by default has an IP Address of 10.0.0.1, with a subnet netmask of 255.0.0.0. This will be the IP Address that you use to communicate and configure your MultiCom Firewall. Other computers using a DHCP client (the default network configuration for most computers) on your LAN network will be assigned an IP address between 10.0.0.17 to 10.0.0.254.

Configuration, diagnostics and status information are available from the MultiCom's web server at http://10.0.0.1/.

NOTE — The most common setup is when your network modem is acting as a bridge between you and your Internet Service Provider. It is possible that your xDSL, cable or wireless modem is acting as a DHCP server for your network and getting an IP address itself from your Internet Service Provider.

If this is the case then your MultiCom Firewall will receive its configuration information directly from your modem. If you are unsure ask whomever installed your xDSL/ Cable line whether your modem is acting as a Bridge or as a DHCP Server.

Configuring Your Computers

To communicate with the MultiCom Firewall you will need to be sure that your computer is configured to access it. There are two general paths for you to follow.

- Set each computer as a DHCP client to receive all necessary information from the MultiCom Firewall each time you boot up your computer on the local network.
- Manually choose IP addresses for each computer on your network between 10.0.0.2-10.255.255.255, with a subnet mask of 255.0.0.0 and enter in the IP address of the MultiCom Firewall (10.0.0.1) as the default gateway and DNS server used to reach the Internet.

The process to enter these settings into your computer varies depending on your operating system. If you do not see your operating system represented in the following sections please refer to your computer's user manual for explanations on configuring your network settings.

Optionally you can make this configuration on only 1 computer to allow access to the MultiCom Firewall. After you have network access to the MultiCom Firewall you can reconfigure the LAN IP parameters to another subnet and also deactivate the DHCP server if there is another being used on your network.

CAUTION - Windows users who were previously connecting to the Internet using an analog or built-in modem or special PPPoE software may need to change their Internet Explorer settings.

Open Internet Explorer, choose Tools and select Internet Options. Under the Connections tab verify that “Never dial a connection” and “use local LAN” is selected. Otherwise every time you want to use the Internet, Windows will try to use the modem.

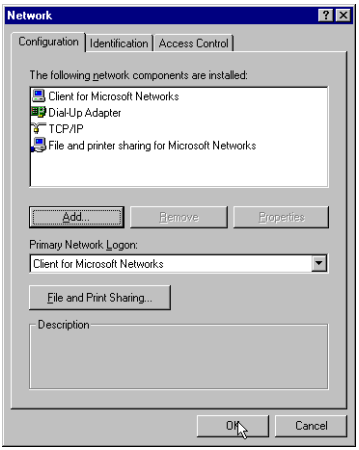
Windows

Windows 9x

To reach the network control on a Windows 95, 98 machine click on `START` > `Parameters` > `Control Panel` > `Network Settings`.

In your networking window you should be in the Configuration panel. Here you will see the network devices (such as your ethernet card/interface) and the protocols installed for each device.

Find the setting the says `TCP/IP -> (the name of your ethernet card)` or just `TCP/IP` and double click on it to open the TCP/IP properties window.



NOTE — if you have scrolled down to the bottom of the list and do not see either TCP/IP or the name of your ethernet card/interface then they are not installed in your computer. Please check the instructions that came with your ethernet card/interface to install that now.

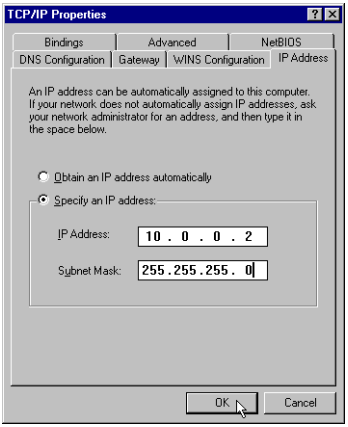
To set your computer as a DHCP Client

1. choose the IP Address tab
2. click on `Obtain IP address automatically`.
3. click on `OK`
4. click on `OK`
5. follow the onscreen instructions (which will probably have you reboot your computer)
6. if you have the option to select a DNS server choose `Obtain DNS`

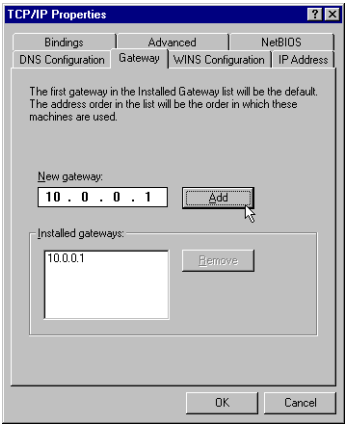
automatically.

To manually set your computer's IP address

1. choose the IP address tab
2. choose specify an IP address
3. enter the IP address (10.0.0.2 for example) and Netmask for your computer (the Netmask should be the same as is configured for the LAN interface of the MultiCom Firewall, by default it is 255.0.0.0)
4. choose the Gateway tab
5. Under New Gateway, enter in the IP address of your MultiCom Firewall's LAN interface (by default this is 10.0.0.1) and click add
6. click on OK to close and save the properties window
7. click on OK to close and apply the network controls for your computer
8. follow the onscreen instructions (which will probably have you reboot your computer)



Windows IP Address Panel



Windows Gateway Panel

Now you are finished configuring your Windows computer to access your MultiCom Firewall. Please continue onto the next section to test your that everything is set up correctly.

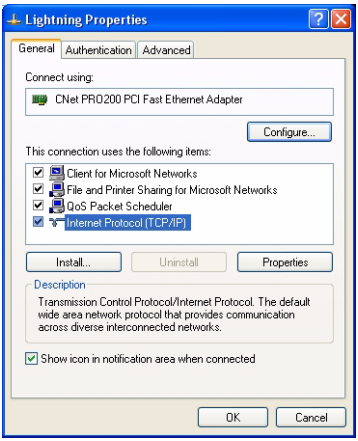
Windows 2000 or XP

To reach the network control on a Windows 2000 or XP machine click on START > Control Panel > Network Connections.

Right click on your network card and select “Properties.”

In your Properties window you should see the protocols and services installed for the selected network device.

Find the setting the says `Internet Protocol (TCP/IP)` and double click on it to open the TCP/IP properties window.



NOTE — if you have scrolled down to the bottom of the list and do not see either TCP/IP or the name of your ethernet card/interface then they are not installed in your computer. Please check the instructions that came with your ethernet card/interface to install that now.

To set your computer as a DHCP Client

1. choose the `General` tab
2. click on `Obtain IP address automatically`.
3. click on `Obtain DNS server address automatically`
4. click on `OK`
5. follow the onscreen instructions (which might ask you to reboot your computer)

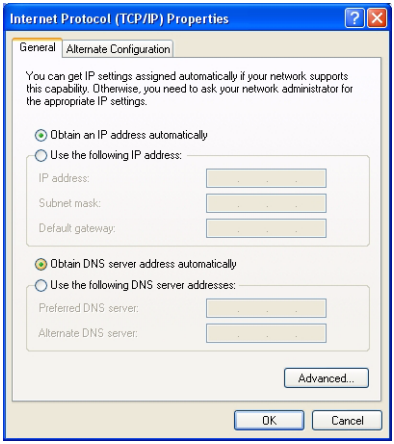
To manually set your computer's IP address

1.choose the `General` tab

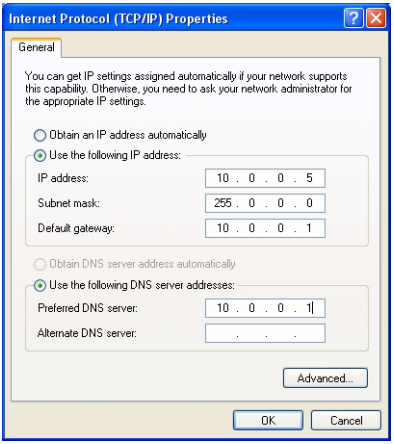
2.click on `Use the following IP address`

3.enter the IP address, Subnet mask, and Default gateway. Be sure that the Subnet Mask and Default gateway match the settings of the MultiCom Firewall’s LAN interface. For the first connection this should be IP address 10.0.0.1, Subnet 255.0.0.0, Default gateway 10.0.0.1

4. click on `Use the following DNS server addresses`
5. Under `Preferred DNS server`, enter in the IP address of your MultiCom Firewall's LAN interface (by default 10.0.0.1) or the Primary DNS server of your ISP
6. Under `Alternate DNS server`, leave it blank or enter the Secondary DNS server of your ISP
7. click on `OK`
8. follow the onscreen instructions (which might ask you to reboot your computer)



Ethernet DHCP Client



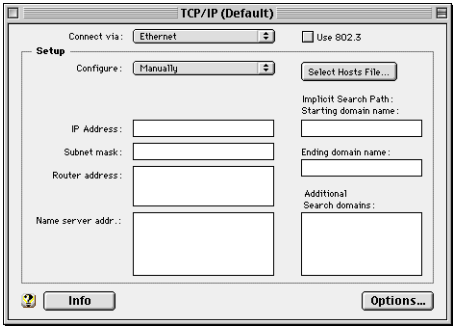
Ethernet Static IP Address

Now you are finished configuring your Windows computer to access your MultiCom Firewall. Please continue onto the next section to verify that everything is set up correctly.

Macintosh

To reach the network control panel on your Macintosh you need to choose on your `Apple Menu` > `Control Panels` > `TCP/IP Panel`. This is where you will find the options to set your Macintosh to use a DHCP server on the network or to use static IP addressing.

These instructions use MacOS9. If you do not see a TCP/IP control panel or are using an earlier version of the MacOS software please check the documentation that came with your Macintosh Operating system for instructions on how to load TCP/IP protocols into your computer.



To set your computer as a DHCP client

1. under `Configure` select "`Using DHCP`"
2. close the TCP/IP panel
3. choose "`Save`" when asked if you want to save your changes

To manually set your computer's IP address

1. under `Configure` select "`Manually`"
2. enter the IP address for your computer in the `IP address` field (10.0.0.2 for example)
3. enter your network mask in the `Network mask` field (by default this should be 255.0.0.0)
4. enter your firewall IP address (the IP address of your MultiCom Firewall's LAN interface, 10.0.0.1 by default) in the `firewall address` field
5. enter the DNS server IP addresses in the `Name server addr` field (by default this is 10.0.0.1)
6. enter your local domain (if you have one) in the `Starting domain name` field
7. close the TCP/IP panel
8. choose "`Save`" when asked if you want to save your changes

Linux

Configuring the network settings for your Linux-based computer will depend on the type of graphical interface and Linux distribution that you have. Be sure you've installed the TCP/IP options when you installed your version of Linux. Otherwise please refer to the documentation that came with your system for the method of configuring your particular networking options.

The following instructions were used on the Debian distribution by editing the configuration file at `/etc/network`

For configuration of the Ethernet interface to use DHCP services

```
iface eth0 inet dhcp
```

To manually set the IP address of the interface card

```
iface eth0 inet static

address 10.0.0.2

netmask 255.0.0.0

broadcast 10.255.255.255

firewall 10.0.0.1
```

Choosing the Internet Connection

Common Configurations

There are 5 common ways to configure your new MultiCom Firewall for use on your network and they are listed below. These assume that your Broadband modem can be (or already is) configured in “bridging” mode, allowing the firewall direct access to your ISP network. The option you choose depends on how your ISP has configured your Internet access. These options are available using the Easy-Setup on the built-in web server or the Configurator software on your MultiCom Companion CD.

1. DHCP: requires the ISP to have a DHCP server.
2. PPPoE: requires a PPPoE username, password, and that the broadband modem is configured into “bridge” mode.
3. PPTP: requires a PPTP username, password and router/server IP addresses of

the Alcatel Modem ANT-1000.

4. Static IP: requires an IP address, subnet mask, default gateway and DNS parameters.
5. Advanced Configuration where you can fully configure the MultiCom Firewall to meet your networking needs.

CAUTION - This information must be exactly the same as received from the ISP or communication to the Internet will not be possible. Please check with your ISP if you have not received the Internet Connection type or the connection's required information. The factory default setting activates DHCP on the WAN interface.

Option 1: Plug and Play with DHCP. This type of Internet connection is typical for use with Cable Broadband modems. Does your our Internet Service Provider uses DHCP to assign you your IP configuration parameters and your computers are configured as DHCP clients? In this case you can simply plug in the MultiCom Firewall immediately between your network and your xDSL, cable or wireless modem to use the default configuration. If your broadband modem is the DHCP server please read below for additional information.

Option 2: PPPoE is used when your Internet Service Provider requires you to only have a username and password to access the Internet. This type of Internet connection is typical for use with DSL Broadband modems. In this cases you enter the necessary information using the Easy Setup window of the built-in web server of your firewall. Click save and you can start surfing the Internet.

Option 3: PPTP with an Alcatel Modem ANT-1000. This process also requires a username and password. Saving a PPTP configuration using Easy-Setup will change the default IP address of the MultiCom Firewall's LAN interface. This change requires you to reboot your computer after using the Easy-Setup wizard.

Option 4: Static IP Configuration. If your ISP gives you a static IP address you can also enter this into the Easy-Setup of the MultiCom Firewall. You will also use this option if you are configuring your MultiCom Firewall for use behind a pre-existing router which will become your default gateway.

Option 5: Advanced Configuration for advanced users. This gives you access to all of the parameters of your MultiCom Firewall. Setting these options requires a good understanding of network terminology and the way your own network is configured. Please refer to the Lightning-Linux Reference Manual for a description of Advanced Configuration options.

Special Configurations

If your modem cannot be configured into “bridge” mode you will have to let the Broadband Modem receive the actual IP parameters from the ISP and share it with the MultiCom Firewall. In this case you have to make a special configuration to use the MultiCom Firewall.

Only choose one of these configurations if you cannot use the Common Configurations above.

1. Broadband Modem receives IP from ISP and is a DHCP server.
2. Broadband Modem receives IP from ISP and has a fixed IP on its LAN interface.
3. Network router is between Modem and Firewall.
4. Network router is between Firewall and Local Network.

> CAUTION - Because you will be creating 2 networks, one between the MultiCom Firewall and the Broadband Modem and one between the MultiCom Firewall and the local network you must be sure that both are using different subnets. For example the default LAN interface uses subnet 10.0.0.0/255.0.0.0 so if this was used in the final configuration the WAN should have a different subnet.

When connecting the MultiCom Firewall to a network that is not directly on the Internet the Firewall will rely on the functionality of the devices between it and the Internet or between it and the Local Network. Some services might be limited or require additional configuration as described below.

- the Network Address Translation (NAT) of the Broadband Modem may not be as powerful as the MultiCom Firewall’s NAT
- if the Broadband modem is using NAT then redirection of incoming traffic to reach internal servers requires NAT rules on BOTH the Broadband Modem and the MultiCom Firewall (including configuration for remote access of the

Firewall itself)

- if the modem/ router is using IP addresses in the 10.0.0.0/255.0.0.0 subnet then you will need to change the IP address and DHCP Server of the Firewall's LAN interface (because it uses this subnet by default.)
- if there is a router between the Firewall and the Modem then the router must be configured correctly to reach the Internet through the Modem or some other route

Option A: Broadband Modem is DHCP Server. The Broadband modem receives all of the IP configuration directly from the ISP and uses its own Network Address Translation to share the connection. In this case you can simply plug in the MultiCom Firewall immediately between your network and your xDSL, cable or wireless modem to use the default configuration. If the Modem uses the 10.0.0.0/255.0.0.0 subnet then you will need to change the LAN interface to a different subnet. For example you could configure the LAN interface to use 192.168.0.1, subnet 255.255.255.0. If you change the IP address of the LAN interface be sure to also change the IP addresses of the LAN's DHCP server, in this case to 192.168.0.17-192.168.0.117.

Option B: Static IP with Modem and Firewall. If the Broadband Modem does not offer a DHCP server then you will need to use the Easy Setup's Static IP configuration to allow the MultiCom Firewall to reach it. Configure the WAN interface of the Firewall to be on the same network as the Modem. For instance if the Modem has an IP address of 192.168.0.1, subnet 255.255.255.0 then configure the Firewall's WAN IP address to be 192.168.0.2, subnet 255.255.255.0. The default gateway will be the IP address of the Modem, in this example it is 192.168.0.1. The DNS parameters should be those of ISP.

Option C: Router between Modem and Firewall. In this case you will need to use the Easy Setup's Static IP configuration to allow the MultiCom Firewall to reach the Router and the router must be configured to reach the Modem and/ or Internet. Configure the WAN interface of the Firewall to be on the same network as the router. For instance if the router has an IP address of 192.168.0.1, subnet 255.255.255.0 then configure the Firewall's WAN IP address to be 192.168.0.2, subnet 255.255.255.0. The default gateway will be the IP address of the router, in this example it is 192.168.0.1. The DNS parameters should be those of ISP.

Option D: Router between Firewall and Local Network. In this case configure the WAN interface using the Easy Setup for Internet Access. Then configure the router to use the LAN interface of the MultiCom Firewall as the default gateway

for all Internet Traffic. Additionally, the MultiCom needs to know that the actual Local Network is behind the router. This requires the use of the Configurator software and is described in the Routing chapter of the Reference Manual.

Configuration Checklist

Before you start the configuration there is some required information needed for your MultiCom Firewall to work correctly. If any of the following terms are unfamiliar to you please check with your Internet Service Provider or the glossary at the end of this book.

Below you can find the default configuration of the LAN side of your MultiCom Firewall. This is the part of the MultiCom Firewall that is connected directly to your local/home network. These settings can be changed by you during the Easy Setup, visiting http://10.0.0.1/setup/lan/ or with the Configurator software.

Table 3: Pre-set configuration of MultiCom Firewall

Configuration Questions	Your Choices
IP Address of the LAN interface	10.0.0.1
Subnet Mask of your network	255.0.0.0
Will you use DHCP on your LAN?	Yes
IP address range for your internal network	10.0.0.17 - 10.0.2.254
User name to configure the MultiCom Firewall	multicom
Password to configure the MultiCom Firewall	(there is no password)
IP Configuration of the WAN interface	DHCP Client
DNS Proxy and Cache	Activated
NAT Firewall	Activated

NOTE — When using the DHCP server of your firewall the necessary IP parameters will be distributed to your LAN by the built-in DHCP server. This saves you from having to manually configure each computer. There can only be one DHCP server on any network.

If your ISP or your Broadband Modem uses DHCP please skip ahead to the next section because you can use the Plug & Play Configuration.

Table 4: Interface Configuration Options

	WAN	LAN	DMZ (Ethernet III only)
DHCP client	DEFAULT	optional	optional
DHCP server	optional	DEFAULT	optional
PPPoE	optional	optional	optional
PPTP	optional	optional	optional
Static/ Manual	optional	optional	optional

If your Internet Service Provider does not provide DHCP configuration the following information will be necessary for you to communicate through your MultiCom Firewall. For PPTP connections this extra information is necessary because you are forming two TCP/IP network links: between your Broadband Modem <--> MultiCom Firewall and between the MultiCom Firewall <--> your network.

If your ISP is using PPPoE or PPTP fill in either the PPPoE/PPTP configuration checklist or the Static configuration checklist depending on how your Internet Service Provider wants you to connect to the Internet.

Table 5: PPPoE/PPTP configuration checklist for WAN interface

Parameters	Information from your Internet Service Provider
the username assigned to you by your Internet Service Provider	
the password assigned to you by your Internet Service Provider	
the domain name of your Internet Service Provider or yours (optional)	
PPTP Only: what is the IP Address of your modem (default 10.0.0.138)	
PPTP Only: what is the subnet mask of your modem (default 255.0.0.0)	

If you are not using DHCP, PPPoE, or PPTP then you will need to configure a Static IP configuration. The table below is all of the information that you will need from your ISP to successfully make a connection to the Internet.

If you have a pre-existing router between the broadband access modem and the MultiCom Firewall you will also need to use the Static IP Configuration option of the Easy-Setup. The Firewall WAN IP address parameters must match the subnet of your router and the router IP address should be the default gateway. Be sure to enter in your ISP's DNS information as well.

Table 6: Static configuration checklist for WAN interface

Parameters	Information from your Internet Service Provider
the IP address assigned to you by your Internet Service Provider	
the IP netmask used by your Internet Service Provider	
the default gateway of your Internet Service Provider	
the domain name of your Internet Service Provider or yours	
the primary IP address of the DNS of your Internet Service Provider	
the secondary DNS IP Address of your Internet Service Provider	

If you do not know this information check with your Internet Service Provider support services or the documentation you received from them when you joined them.

Plug & Play Configuration: DHCP

Here are the requirements necessary to install the MultiCom Firewall without configuration.

1. Is your Internet Service Provider giving you your IP address, DNS server address and default firewall configuration with a DHCP server?
2. Are all of your internal network (LAN) devices configured as DHCP Clients?

If your Internet Service Provider uses DHCP to assign you your IP configuration parameters and your computers are configured as DHCP clients you can simply plug in the MultiCom Firewall immediately between your network and your xDSL, cable or wireless modem. In this case it will automatically be a firewall protecting your internal network (LAN) and enable all of your LAN computers to use the same Internet account.

TIP - Instructions on configuring your computers to use DHCP is in the “Configuring Your Computers” Section on page 42.

If you answered yes to the two above questions then you only need to plug in your cables to the MultiCom Firewall. If a DHCP server is found on the WAN, your MultiCom Firewall will be assigned an IP address by your Internet Service Provider (or possibly your modem, see NOTE below). Additionally, all needed information to communicate with the Internet Service Provider through the modem will be passed to the MultiCom Firewall, which in turn passes it to the DHCP client computers on your network so that they can access the Internet.

If no DHCP server is found the MultiCom Firewall will not be able to connect to the Internet until a different configuration is loaded. If no DHCP service is provided you will need to run the Easy-Setup from the built-in web server of the MultiCom Firewall or use the Configurator software from the Companion CD to properly configure your MultiCom Firewall.

CAUTION - Some Internet Service Providers that use DHCP also require you to register the hardware MAC address of your computer’s Ethernet card. If this was the case you will either have to ask them to change the MAC address to the WAN interface of your MultiCom Firewall (00:90:f4:xx:xx:xx where xx:xx:xx is the 6 digit/ letter serial number of your Firewall) or use the Configurator software to change the MAC address of your MultiCom Firewall. Please see the Reference Manual for more information on this process.

Diagnostics and status information on this connection is available from the MultiCom web server at http://10.0.0.1/status/wan/ and from the DHCP tab of the Configurator software’s Monitor window. DHCP activity can also be logged by activating Syslog using the Advanced Config option.

Using the Easy Setup

The built-in Easy Setup of your MultiCom Firewall’s web interface has been designed to get your Internet connection started as quickly as possible. You will need an Internet web browser installed to use this option. If you do not have one

you can install a web browser from the MultiCom Companion CD that came with your firewall. Just go to the 3rd Party Software section and install Netscape, Internet Explorer, Mozilla or Firefox.

To properly configure your firewall we will be using the information that you have written in the Pre-Configuration Checklist. Please be sure that you have filled in that information now before continuing.

Accessing the Easy Setup Web Server

For the following explanation we assume that you will be directly connected to your firewall. Your computer must be configured as a DHCP client to configure the MultiCom Firewall (optionally a computer with a static IP address between 10.0.0.2-10.255.255.255 and with a subnet mask of 255.0.0.0 can be used.) If you are unsure how to do this see the previous section on Configuring Your Computers.

> CAUTION - if your MultiCom Firewall does not respond you may need to reset it to its default settings. Refer to the Resetting Default Settings section of the Troubleshooting chapter.

Open up a web browser and enter in the IP address of your MultiCom Firewall (the factory default is http://10.0.0.1) You will be asked for the username and password allowed to access the firewall. The default settings for the MultiCom Firewalls is username=" multicom" and no password. Enter this information now and click OK.

The next screen that you will see is the MultiCom Web Server window. Here you select the Easy Setup option.

CAUTION — Remember that you must be using a computer that either is set as a DHCP Client or has a static IP Address (in the 10.x.x.x range, for example 10.0.0.2) and a subnet mask of 255.0.0.0. Otherwise you will not be able to communicate with the MultiCom Firewall in its default settings.

The Easy Setup window (below) allows for fast configuration of your MultiCom Firewall. After reading the warning click the “Next” button to start configuring the WAN interface.

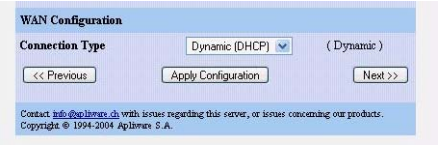
The next choice depends on how your Internet Service Provider connects you to the Internet. You will see the WAN Configuration webpage where you can select the Connection Type that your ISP has asked you to use. The next four sections describe the 4 possibilities for configuring the WAN interface using DHCP, PPPoE, PPTP or a static configuration.

WAN DHCP Easy Setup

If your Internet Service Provider connects you using a DHCP server you will not have to configure any parameters with Easy Setup because this is the default mode of the MultiCom Firewall. During the bootup of your firewall in its default mode it will automatically search for the DHCP server and configure itself with everything needed to reach the Internet Service Provider.

If you use the Easy Setup window to configure DHCP you will have the option to configure the DHCP settings on your LAN interface. This allows you to customize the IP addresses assigned by your firewall or to disable this functionality. Please refer to the Lightning-Linux Reference Manual chapter on DHCP for more information on using this option.

1. Select `Dynamic (DHCP)` in the Connection Type box to see the Easy Setup configuration options.



2. Optionally give a name to your MultiCom Firewall.
3. Click the `Next` button and goto the Section “LAN Easy Setup” on page 63.

WAN PPPoE Easy Setup

If your Internet Service Provider connects you using a PPPoE server you need to click the PPPoE option in the Easy Setup window (see the window above). This window only requires a username and password to access your Internet Service Provider. This information is available from your Internet Service Provider.

The PPPoE setting causes the MultiCom Firewall to automatically and regularly demand its IP configuration from a PPPoE server connected through the WAN interface using the username and password. All needed Internet parameters such as the MultiCom Firewall’s IP address, IP subnet, default gateway, and external DNS servers will be automatically requested directly from the ISP using the PPPoE protocol. Below are the steps necessary to configure a PPPoE connection.

1. Select `PPPoE` in the Connection Type box and click the “Next” button to see the following Easy Setup configuration option page.

2. Enter in the username that your Internet Service Provider gave to you.
3. Enter in the password that your Internet Service Provider gave to you.
4. Optionally enter in your local domain name. (This will become the default suffix used for networking activity.)
5. Select the PPP connection mode that you wish to use: Permanent is an always on connection, Dial on Demand only connects to the Internet when there is network traffic, and Manual requires manually opening or closing the Internet connection from the web interface.
6. Select the PPP connection idle time out if you are using Dial on Demand. When there is no network activity this is the number of seconds before the PPP connection is closed.
7. Optionally enable the TCP Frame Size Adaption as a troubleshooting step if you are having problems connecting to your Internet Service Provider or certain web pages.
8. Click the `Next` button and goto the Section “LAN Easy Setup” on page 63.

Diagnostics and status information on this connection is available from the MultiCom web server at http://10.0.0.1/status/wan/ or from the PPP tab of the Configurator software’s Monitor window. PPPoE activity can also be logged by activating Syslog using the Advanced Config option. See the User’s Manual for more instructions.

WAN PPTP Easy Setup

If your Internet Service Provider connects you using a PPTP server you need to click the PPTP option in the Easy Setup window (see the main window above). This window requires a username and password to access your Internet Service

Provider. Additionally you will need to enter the IP Address and Subnet Mask of your broadband modem. This information is available from your Internet Service Provider.

The PPTP setting causes the MultiCom Firewall to automatically and regularly demand its IP configuration from a PPTP server connected through the WAN interface using a username and password. All needed Internet parameters such as the MultiCom Firewall's IP address, IP subnet, default gateway, and external DNS servers will be automatically requested directly from the ISP using the PPTP protocol.

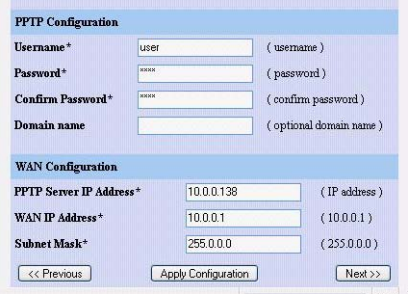
It is important to know the existing IP configuration of the modem offering a PPTP server because the MultiCom Firewall WAN interface mst be on the same subnetwork as the Ethernet interface of the modem. This creates 2 networks, one between the MultiCom Firewall and the broadband modem and one between the MultiCom Firewall and the local network. By default this PPTP Setup Panel configures your WAN interface's network to be 10.0.0.1/255.0.0.0, expects to find the broadband modem at IP address 10.0.0.138, and changes the LAN interface to 192.168.1.1/255.255.255.0. Although this is a very common configuration it may not be the way your broadband modem is configured. Be sure to verify

---

CAUTION - Saving a PPTP configuration using Easy-Setup will change the default IP address of the MultiCom Firewall's LAN interface. This change requires you to reboot your computer after using the Easy-Setup wizard

---

1. Select PPPoE in the Connection Type box and click the "Next" button to see the following Easy Setup configuration option page. This is where you enter in your username and password, modem IP Address, WAN IP Address and Subnet Mask.



2. Enter in the username that your Internet Service Provider gave to you.
3. Enter in the password that your Internet Service Provider gave to you.
4. Optionally enter in your local domain name. (This will become the default suffix used for networking activity.)
5. Enter in the IP Address of the broadband modem that is your PPTP Server.
6. Enter in the IP Address for the WAN interface for the MultiCom Firewall. This address must be on the same subnet as the IP Address of the broadband modem. For instance if your modem 10.0.0.138 then your WAN interface would probably have and IP Address of 10.0.0.1 .
7. Enter in the Subnet Mask of the broadband modem.
8. Click the `Next` button and goto the Section “LAN Easy Setup” on page 63.

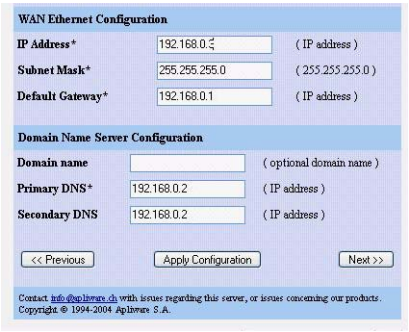
WAN Static IP Easy Setup

In some cases your Internet Service Provider will have you configure all of the necessary information manually. This is common when you are assigned a static IP address that will not change. The needed configuration information is available from your Internet Service Provider. Below are the steps necessary to configure a Static connection.

In a Static IP connection all Internet parameters such as the MultiCom Firewall’s IP address, IP subnet, default gateway, and external DNS servers must be manually configured. If your ISP has told you to manually configure your WAN interface this is where you will enter in the information that they send you.

TIP - If you have a pre-existing router in front of your MultiCom Firewall you will use its IP Address as the default gateway and need to be sure that your WAN interface is on the same subnet as the router.

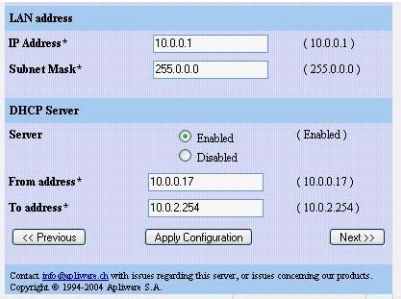
1. Select `Static` in the Connection Type box and click the “Next” button to see the following Easy Setup configuration option page. This is where you manually enter in all of your WAN interface IP parameters. Your ISP should have provided you with all of the information necessary to fill in this form.
2. Enter in the WAN IP Address that your MultiCom Firewall will be known as (provided by your Internet Service Provider.)
3. Enter in the WAN Subnet Mask that will be used between the Internet Service Provider and the MultiCom Firewall.
4. Enter in the Default Gateway address (otherwise known as the IP address of the Internet Service Provider's firewall).
5. Optionally enter in your local domain name. (This will become the default suffix used for networking activity.)
6. Enter in the IP addresses of your Internet Service Provider's Primary and Secondary DNS servers.



7. Click the `Next` button and goto the Section “LAN Easy Setup” on page 63.

LAN Easy Setup

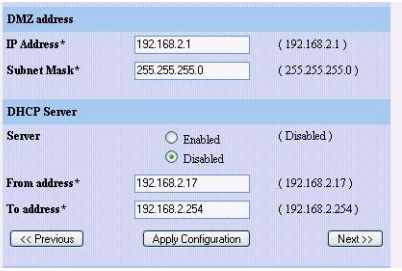
After finishing the WAN configuration as instructed by your ISP you can optionally change the default LAN configuration settings for your local network. You should not normally change these settings unless you know what you are doing and can just click the Next button to continue. For more information about DHCP options refer to the DHCP Chapter of the Reference Manual.



1. Enter in the LAN IP Address that your MultiCom Firewall will be known as (provided by your Internet Service Provider.) This cannot be on the same subnet as the WAN interface.
2. Enter in the LAN Subnet Mask that will be used on your local network.
3. Choose to enable or disable the built-in DHCP server for managing your network. By default this is enabled and should not be changed unless you have another DHCP server on your network.
4. If you enabled the DHCP server, choose the first IP address that the MultiCom Firewall should assign on your local network to DHCP clients. This IP Address must be on the same subnet as the LAN IP Address.
5. If you enabled the DHCP server, choose the last IP address that the MultiCom Firewall should assign on your local network to DHCP clients. This IP Address must be on the same subnet as the LAN IP Address. All addresses between the “From address” and the “To address” can be assigned by the MultiCom Firewall to computers on your local network.
6. Click the `Next` button and goto the next Section.

DMZ Easy Setup

If your MultiCom Firewall has a DMZ interface this webpage will appear next. If you do not have a DMZ interface you will immediately go to the Firewall Easy Setup configuration webpage. If you want to leave the DMZ disabled just enter 0.0.0.0 for the IP address and 0.0.0.0 for the subnet mask. You can activate it later.



1. Enter in the DMZ IP Address that your MultiCom Firewall will be known as (provided by your Internet Service Provider.) This cannot be on the same subnet as the WAN or LAN interfaces.
2. Enter in the DMZ Subnet Mask that will be used on your local network.
3. Choose to enable or disable the built-in DHCP server for managing your network. By default this is enabled and should not be changed unless you have another DHCP server on your network.
4. If you enabled the DHCP server, choose the first IP address that the MultiCom Firewall should assign on your DMZ network to DHCP clients. This IP Address must be on the same subnet as the DMZ IP Address.
5. If you enabled the DHCP server, choose the last IP address that the MultiCom Firewall should assign on your DMZ network to DHCP clients. This IP Address must be on the same subnet as the DMZ IP Address. All addresses between the “From address” and the “To address” can be assigned by the MultiCom Firewall to computers on your DMZ network.
6. Click the `Next` button and goto the next Section.

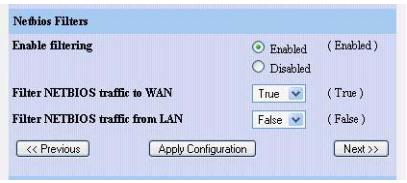
Easy Firewall Setup

Although the SecureWall blocks all incoming traffic arriving at the WAN interface except the traffic which is a response to a data request from the LAN or DMZ networks you may wish to allow customized remote access to your MultiCom Firewall or your local network.

The Easy Firewall Setup is part of the Easy Setup wizard of the Web Interface but it can also be used separately on the MultiCom Firewall by using a web browser to go to http://10.0.0.1/setup/fw/ (where 10.0.0.1 is the IP address of the LAN interface of the Firewall.). Additional options are provided by the next 2 webpages.

Firewall Filters

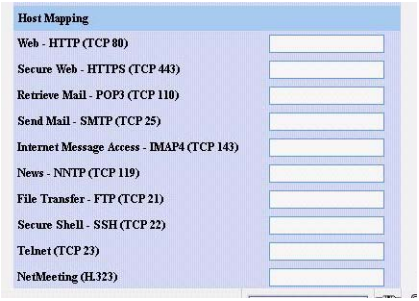
The first part of the Firewall Easy Setup webpages allows you to enable or disable the Stateful Packet Inspection Firewall to work along with the SecureWall firewall. When filtering is enabled all traffic from the DMZ network (if available) to the LAN is blocked. Additionally you can choose to block NetBIOS traffic directed to the WAN interface or coming from the LAN interface.



Additional rules can be customized using the Configurator software and is described in the Lightning-Linux Reference Manual chapter on Filtering. When you are finished click the “Next” button.

Host Mapping

If you make servers on your local network available to users on the Internet (for instance a web or email server) you may enter the IP address on your local network of those servers. Rules will be made to allow access to these servers in the SecureWall and Stateful Filtering Firewall. External users will use the IP address of the WAN interface and be redirected to these internal servers.

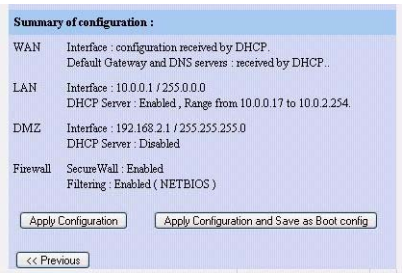


To activate services not in the list, use the Easy Firewall of the Configurator software. When you are finished click the “Next” button.

NOTE - to make secure remote access to your MultiCom Firewall for configuration simply enter in the IP address of the LAN interface (by default 10.0.0.1) in the “SecureWeb - HTTPS (TCP 443)” and or the “Secure Shell - SSH (TCP 22)” server fields.

Saving The Configuration

1. Finally you have a summary of your chosen configuration and the choice of how to save it. You can either choose Apply Configuration to save the configuration to the temporary memory and start using it right away or you can choose Apply Configuration and Save as Boot config. The second option makes your changes permanent, in case you need to reboot your firewall or there is a power outage. The second option is the recommended option.



NOTE — Choosing `Apply Configuration and Save as Boot config` activates and saves the configuration changes you have made so that when the MultiCom Firewall is rebooted your changes will still be there. If you choose `Apply Configuration` then the changes will be activated but the next time you reboot your MultiCom Firewall these changes will also be deleted.

2. When the configuration has been successfully saved using the Apply Configuration button you will see the following screen. Your Easy Setup configuration is now finished.

3. If you saved your configuration using the Apply Configuration and Save as Boot config button you will see the following screen. Your Easy Setup configuration is now finished.

Fine Tuning Your Configuration

The default configuration that you have just set up enables the basic features of your MultiCom Firewall such as Internet Connection Sharing and the SecureWall to protect your network. For more advanced features please refer to the Lightning-Linux Reference Manual for your firmware version.

Activate Option Keys

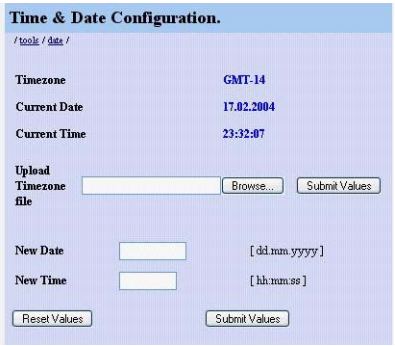
If you have received an Option Key you will need to enter it into the MultiCom Firewall for the new features to be activated. The Option key is a text file that is usually received in an email. You can either save the attached text message to your computer or you can make a new, empty text file and copy and paste the contents of the key into it.

To reach the key activation window on the MultiCom Firewall web interface you will need to use a web browser to goto http://10.0.0.1/tools/options/ (where 10.0.0.1 is the IP address of the LAN interface of the Firewall.)

Finally, click on the browse button to where the Option Key text file has been saved. Finally click the button “Update Options Key”.

Configure Date And Time

To set the correct date and time on the MultiCom Firewall you will need to use a web browser to goto the LAN interface http://10.0.0.1/tools/date/ (where 10.0.0.1 is the IP address of the LAN interface of the Firewall).



Enter in the correct date, the current time and optionally choose a timezone if you plan to use the NTP functionality as described in the Reference Manual. The Timezone files are stored in the zoneinfo directory of your Configurator installation or the MultiCom Companion CD. When you are done click “Submit Values”.

Create New Privileged Administrator

Although the SecureWall firewall is activated by default, blocking access to the Firewall for configuration from the Internet, it is a good idea to change the default username of “multicom”.

To change the Administrator Username and Password on the MultiCom Firewall you will need to use a web browser to goto http://10.0.0.1/advanced/user/create/ (where 10.0.0.1 is the IP address of the LAN interface of the Firewall). Enter in a new Username and Password and select the User Rights “Privileged” with CLI Access enabled. When you are finished click “Submit Values”.

When the new “Privileged” user is created, the default user “multicom” is disabled. This means that only the new user will have the right to configure the MultiCom Firewall. If you forget your username and password, you will have to reset the MultiCom Firewall back into its default configuration and reload the configuration file from a backup copy.

> NOTE - When the first new Privileged user is created the multicom user will be deactivated and you will need to authenticate again using the new username and password that you created.

The Reference Manual has descriptions of all user and permission options.

Quick Interface Configuration

If you want to make a quick change to an interface’s configuration you will need to use a web browser to go to the LAN interface (by default http://10.0.0.1). Select interface from the menu (WAN, LAN, DMZ, DSL, WLAN) and change the configuration on the following pages. When you are finished you will have the option to either

- 'Apply Configuration' to test a new configuration but not save it. Rebooting the Firewall will return the Firewall to its previous configuration.
- 'Apply Configuration and Save as Boot config' to activate and permanently save your configuration

Testing Your Configuration

The process of communication to the Internet works as follows when your MultiCom Firewall and workstation computers are configured properly.

1. Your computer makes a request to reach the Internet or a service from the Internet.
2. This request is sent to the network through your ethernet card/interface.
3. Your ethernet card/interface forwards this information to the MultiCom Firewall
4. Your MultiCom Firewall takes this information and forwards it to your modem or directly to the ISP if the modem is in “bridge” mode
5. your modem, unless already connected will dial your Internet Service Provider, authenticate your user name and password and then send information request to the Internet

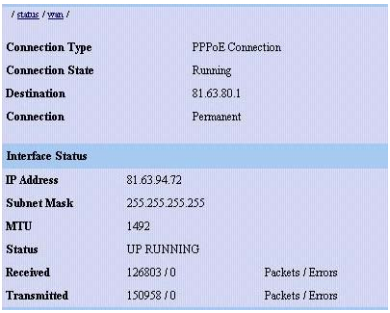
The information that you requested will follow the same route back (in the opposite order) to reach the computer making the request. In most cases you will either get the information that you received, get a response that it was not found, or because of network congestion be told that your request has timed-out and was dropped.

To test that your connections are working correctly you can open your preferred Internet browser (Netscape Navigator or Microsoft's Internet Explorer) and type in a web address.

NOTE — please hit the refresh page on your browser to be sure that you are getting information from the Internet directly instead of from a web page saved to your hard disk. You should also notice the lights on your MultiCom Firewall blinking.

Unless your modem is already connected it will make the phone call now and retrieve the information that your computer requested. If you are able to reach the Internet then everything is working properly. If you have problems first check that everything is plugged in, go over this chapter again, check the Troubleshooting chapter, and finally consider calling the Technical Support of where you purchased your MultiCom Firewall.

Diagnostics and status information on this connection is available from the MultiCom web server at http://10.0.0.1/status/wan/ and from the DHCP or PPP tab of the Configurator software's Monitor window.



/ status / wan /

Connection Type	PPPoE Connection	
Connection State	Running	
Destination	81.63.80.1	
Connection	Permanent	
Interface Status		
IP Address	81.63.94.72	
Subnet Mask	255.255.255.255	
MTU	1492	
Status	UP RUNNING	
Received	126803 / 0	Packets / Errors
Transmitted	150958 / 0	Packets / Errors

Don't forget to register your MultiCom Firewall and consider reading up on the more advanced options available.

> CAUTION — A request to the Internet may be made without your being aware of it. These requests could inadvertently open your network connection and cause you additional phone. Check the Troubleshooting chapter for more information on Internet connections

For more detailed testing suggestions for your configuration and firewall check the Lightning-Linux Reference Manual.

Testing Security

Here are some web sites that offer free security scanning of your Internet connection. There are many such sites available on the Internet.

http://www.dslreports.com/scan

http://www.hackerwhacker.com/

http://scan.sygatetech.com/

http://security1.norton.com/us/intro.asp

http://www.mcafeeasap.com/intl/EN/content/managed_services/vulnerability.asp

Testing Connection Speed

Here are some web sites that offer free bandwidth tests of your Internet connection. There are many such sites available on the Internet.

http://www.zdnet.co.uk/misc/band-test/speedtest50.html

http://www.testmyspeed.com/internationalspeedtests.htm

http://www.dslreports.com/stest

http://www.gibroadband.com/pages/speedtest.asp

http://bandwidthplace.com/speedtest/

http://www.itzalist.com/com/dsl-speed-test.html

Registering Your Firewall

Registering your firewall allows you to keep up to date with the latest developments for your product. Additionally registration takes away the burden of keeping proofs of purchase (for upgrades or repairs) as our database will take care of that for you. Now is a good time to do it while you have your receipts and serial number readily available.

For online registration go to http://www.lightning.ch/register.html

Chapter 4

Maintenance

While basic security is enabled as soon as you plug your MultiCom Firewall firewall between your modem and your network, a well running network requires regular maintenance. A poorly maintained network may suffer from network performance loss or worse such as network failure (especially when you need it most.)

Any number of factors can affect the way your network runs — new software installations, misconfigurations of hardware, and even electromagnetic interference can all cause serious changes in the way data travels through your network.

Just as with any emergency, preparation will minimize the effect on your business and peace-of mind. Your MultiCom Firewall has been equipped with numerous tools to assist in your maintenance needs.

- Checking System Status
  —Using the Configurator software
  —Using the built-in web server
  —Using shell commands to directly log into the firewall
- Configuration
  —Backup the Configuration

—Restoring the Configuration

- Keep up to date

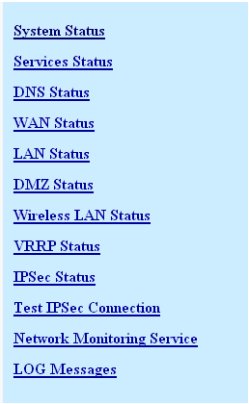
—update the firmware

—read about current networking exploits

Web Server Status Reports

By using a web browser you can get status information of ARP and routing tables, interfaces, memory and CPU loads, uptime and more. You just type in the IP address of the firewalls LAN or WAN interface (by default http://10.0.0.1), enter any necessary user names and passwords (by default user=“multicom” and there is no password). You can print this information out using your web browser's print functions.

Starting in Lightning-Linux 3.4 the web server provides direct status information of the Firewall, services, interfaces, and logged events. Simply select the STATUS link in the menu. This page is shown below.



Tools	Function
System Status	Shows system firmware version, device type, serial number, installed options, system uptime and CPU load
Services Status	Shows the status of the ARP Proxy, DNS Proxy, DynDNS, FTP, NTP, RIP, SNMP and Syslog services.

Tools	Function
DNS Status	Shows the current Domain Name Servers
ADSL Status	Shows ADSL connection diagnostics and PPP configuration on the ADSL interface
WAN Status	Shows WAN interface diagnostics such as MAC address, ethernet speed, and IP parameters. If the interface is a DHCP client you will have a button to renew the DHCP lease. If it is a PPPoE Manual/ Dial on Demand connection you will have the option to Connect or Disconnect.
LAN Status	Shows LAN interface diagnostics such as MAC address, ethernet speed, and IP parameters. It will also show if a DHCP server is active on the interface and offer the option to see existing DHCP Leases.
DMZ Status	Shows DMZ interface diagnostics such as MAC address, ethernet speed, and IP parameters. It will also show if a DHCP server is active on the interface and offer the option to see existing DHCP Leases.
Wireless LAN Status	Shows the Wireless Interface diagnostics. This is the window where the user can see the WLAN status and state of each hardware interface, the current configuration of the selected interface, the broadcast level.
VRRP Status	If the High Availability option has been installed this table shows the status of VRRP on each interface.
IPSec Status	Shows a table of existing IPSec connections and statistics about each connection when the IPSec Option is installed.
Test IPSec Connection	Allows the testing of each active IPSec connection when the IPSec Option is installed.
Network Monitoring Service	Shows a table of TCP networking services that are being monitored by the MultiCom Firewall when the Network Monitoring Option is installed.
LOG Messages	Event log of activities occurring on the MultiCom Firewall such as loading new configurations, activation or deactivation of IP services, errors. This is the same event log as can be seen in the Monitor software.

All of the web servers status screens are shown in the Web Server Screens Appendix in the Reference Manual.

Below are some of the direct web links to commonly used diagnostic information in older firmware versions. The following examples use the firewall's default IP address of 10.0.0.1. If your firewall is using a different IP address use that in place of the 10.0.0.1.

Table 7: Common web server diagnostics pages for firmware 3.0-3.3

MultiCom Serial number	http://10.0.0.1/config/system/hardware/
Software version	http://10.0.0.1/config/system/software/
LAN status	http://10.0.0.1/config/interface/ethernet[LAN]/status/
LAN DHCP server leases	http://10.0.0.1/config/interface/ethernet[LAN]/ip/dhcp/server/status/leases/
WAN status	http://10.0.0.1/config/interface/ethernet[WAN]/status/
WAN DHCP client status	http://10.0.0.1/config/interface/ethernet[WAN]/ip/dhcp/client/status/
PPPoE status	http://10.0.0.1/config/interface/ppp[PPPoE]/status/
PPPoE IP status	http://10.0.0.1/config/interface/ppp[PPPoE]/ipcp/status/
PPPoE Link status	http://10.0.0.1/config/interface/ppp[PPPoE]/lcp/status/
Available PPPoE servers	http://10.0.0.1/config/interface/ppp[PPPoE]/pppoe/server_list/
PPTP Status	http://10.0.0.1/config/interface/ppp[PPTP]/status/
PPTP Link status	http://10.0.0.1/config/interface/ppp[PPTP]/lcp/status/
ARP entries	http://10.0.0.1/config/arp/status/arp_entry/
DNS servers used	http://10.0.0.1/config/ip/dns/status/nameserver/

Using the above links will help you to find where a problem may be. For example, if you have checked the WAN status or the PPPoE status and they both have IP addresses assigned to them they are functioning normally and your problem is probably somewhere else.

Monitor Status Reports

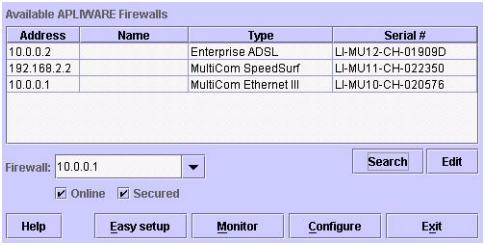
The Configurator software for your MultiCom Firewall includes detailed monitoring windows. These diagnostic utilities give you the current state of your firewall whether it is on a local or remote network.

CAUTION - when accessing remote MultiCom Firewalls on the Internet it is recommended to always use the Configurator in "Secured" mode to protect the information exchanges.

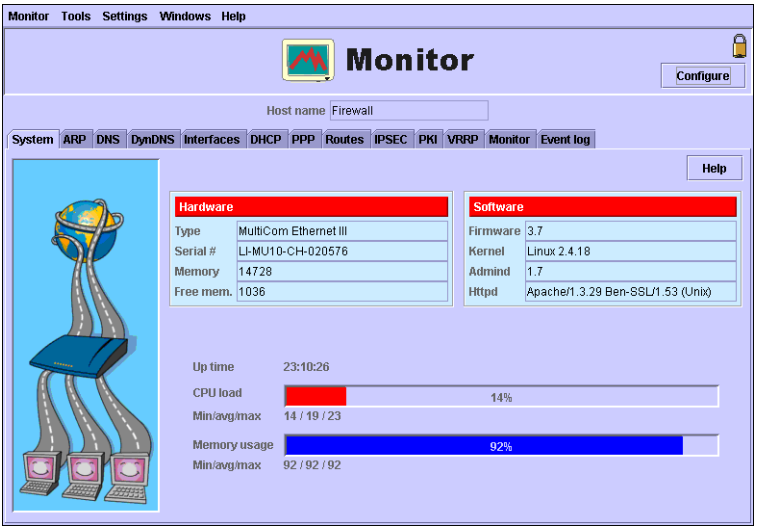
With the monitoring options you will be able to get information on the System status, ARP tables, DNS, each interface, DHCP services, installed routes and more.

Optionally you could also have a syslog server set to listen for info level announcements from the MultiCom Firewall and watch for alerts, warnings, notices and other information.

1. To reach the monitoring screens of the Configurator you will need to first start the Configurator from CD, hard disk or a remote drive. (see the section on Starting Easy Setup or Installing the Configuration Software if you need assistance in starting the Configurator).



2. Click search to search for the MultiCom Firewall on your local network or just enter the IP address of the firewall you wish to monitor
3. Be sure "Online" and "Secured" buttons are checked and click on the Monitor button
4. You should now have arrived at the screen titled Monitor. Depending on what sort of diagnostics you are looking for, go to the appropriate screen.



You should now have arrived at the screen titled Monitor. Depending on what sort of diagnostics you are looking for, go to the appropriate screen.

Panels	Available Information
System	General information about the hardware, firmware and work load of your MultiCom Firewall.
ARP	The currently active ARP table in the firewall
DNS	The currently active DNS servers for the firewall
Dynamic DNS	The current status of a Dynamic DNS configuration if one exists
Interfaces	Status of each interface port (LAN/WAN), identifying information, and data traffic reports
DHCP	Client Window— shows all of the configuration data received from a DHCP server Server Window — shows currently assigned IP addresses and their lease times.
PPP	Describes current status of PPPoE interfaces if they are active
Routes	The currently active routes in your firewall
Bridges	Displays information about the LAN-WLAN bridge of your MultiCom Firewall when the Bridge is activated.

Panels	Available Information
IPSec	Status of selected IPSec connections and summary of all IPSec connections (when IPSec options are installed)
PKI	Status of PKI Keys, Certificates and Certificate Revocation Lists installed on the Firewall (when IPSec optionsa are installed)
VRRP	Status of High Availability on each interface (when the High Availability option is installed)
Monitor	Status and delay of each listed service host (when Network Monitoring options are installed)
Event Log	Events being generated by the MultiCom Firewall

Telnet/ Console Status Reports

By logging into the Firewall's telnet, SSH telnet or console interface (check your User's Manual to see if your firewall has a console interface) you can run the "info" commands to get a text status information of particular parts of the MultiCom Firewall and its software.

This used with telnet scripting utilities (such as the Expect software for Linux and Windows, or CatTools for Windows at http://www.kiwisyslog.com) for reports and automated management of the MultiCom Firewalls.

Table 8: Common telnet/ console diagnostics

Description	Commands	Sample output
last error causing reboot	/: backtrace	only available in 3.5+
MultiCom Serial number	/: info system hardware serial_number	serial_number = LI-MU7-CH-0200D2
Software version	/: info system software firmware	firmware = 3.6
LAN status	/: info interface ethernet LAN status status	status = UP RUNNING
LAN IP Address	/: info interface ethernet LAN status ip_address	ip_address = 10.0.0.1
	/: info interface ethernet LAN ip netmask	netmask = 255.0.0.0
LAN DHCP Mode	/: info interface ethernet LAN ip dhcp mode	mode = server

Description	Commands	Sample output
LAN DHCP server leases	/: info interface ethernet LAN ip dhcp server status leases	indexes: 0 1 2 3
	/: info interface ethernet LAN ip dhcp server status leases 0 ip	ip = 10.0.0.17
	/: info interface ethernet LAN ip dhcp server status leases 0 hw_address	hw_address = 00:c0:f0:4c:a7:90
	/: info interface ethernet LAN ip dhcp server status leases 0 starts	starts = 4 2001/06/28 13:24:06
	/: info interface ethernet LAN ip dhcp server status leases 0 ends	ends = 4 2001/06/28 14:24:06
	/: info interface ethernet LAN ip dhcp server status leases 0 hostname	hostname = "NT-workstation"
WAN status	/: info interface ethernet WAN status status	status = UP RUNNING
WAN DHCP client status	/: info interface ethernet WAN ip dhcp client status state	state = Assigned
PPPoE status	/: info interface ppp PPPoE status status	status = UP RUNNING
PPPoE IP address	/: info interface ppp PPPoE status ip_address	ip_address = 212.147.17.76
PPPoE IPCP info	/: info interface ppp PPPoE ipcp status state	state = UP state = DOWN
PPPoE Link status	/: info interface ppp PPPoE lcp status info	info = "" info = CHAP authentication failed info = Timeout sending Config-Requests info = Endpoint not connected
PPPoE DNS assigned servers	/: info interface ppp PPPoE ipcp status primary	primary = 212.147.10.10
	/: info interface ppp PPPoE ipcp status secondary	secondary = 212.147.0.1

Description	Commands	Sample output
Available PPPoE servers	/: info interface ppp PPPoE pppoe server_list	indexes: 0 1 2
	/: info interface ppp PPPoE pppoe server_list 0 access_concentrator_name	access_concentrator_name = ipc-lsp690-r-lc-01
	/: info interface ppp PPPoE pppoe server_list 0 service_name	service_name = Any
ARP entries	/: info arp status arp_entry	indexes: 0 1 2
	/: info arp status arp_entry 0 hw_address	hw_address = 00:C0:F0:57:4A:6D
	/: info arp status arp_entry 1 hw_address	hw_address = 00:C0:F0:4C:A7:90
DNS servers used	/: info ip dns status nameserver 0 ip	ip = 192.168.1.115
	/: info ip dns status nameserver 1 ip	ip = 192.168.1.116

The console interface is useful if you may have blocked your Ethernet interface access or think there may be a problem with your Ethernet network (your computer's Ethernet interface, a hub/ switch, cabling). Simply configure your workstations serial port according to the Console Configuration in the Hardware Specification chapter and plug in the serial cable to your MultiCom Firewall and workstation's 9pin serial port. This gives direct access to the firewall.

Table 9: Common telnet/ console commands

Description	Commands
ENABLE IPSEC	set security ipsec enabled=true saveconfig current
DISABLE IPSEC	set security ipsec enabled=false saveconfig current
SEE IPSEC CONNECTIONS	ipsec
STOP AN IPSEC CONNECTION	ipsec terminate <connection name>
START AN IPSEC CONNECTION	ipsec initiate <connection name>
ENABLE SECUREWALL	set interface ethernet WAN ip nat securewall=true saveconfig current
DISABLE SECUREWALL	set interface ethernet WAN ip nat securewall=false saveconfig current
ENABLE FILTERING	set ip filtering enabled=true saveconfig current
DISABLE FILTERING	set ip filtering enabled=false saveconfig current
ENABLE FILTERING OBJECTS	set ip filtering_objects enabled=true saveconfig current
DISABLE FILTERING OBJECTS	set ip filtering_objects enabled=false saveconfig current
ENABLE DNS PROXY	set ip dns proxy enabled=true saveconfig current
DISABLE DNS PROXY	set ip dns proxy enabled=false saveconfig current
ENABLE RIP	set routing ip rip enabled=true saveconfig current
DISABLE RIP	set routing ip rip enabled=false saveconfig current
ENABLE FTP	set ip ftp server enabled=true saveconfig current
DISABLE FTP	set ip ftp server enabled=false saveconfig current
ADD SYSLOG SERVER	add ip syslog server 0 set ip syslog server 0 address=10.0.0.2 level=debug saveconfig current
ENABLE SYSLOG DEBUG OUTPUT	eventdebug start

Description	Commands
DISABLE SYSLOG DEBUG OUTPUT	eventdebug stop
ENABLE SSH	set security access ssh enabled=true saveconfig current
DISABLE SSH	set security access ssh enabled=true saveconfig current
REBOOT	reboot
ENABLE TELNET	set security access telnet enabled=true saveconfig current
DISABLE TELNET	set security access telnet enabled=false saveconfig current
RENEW DHCLP CLIENT ON WAN	dhcpclient WAN renew

Error Messages

In addition to the Web server, Monitor and Telnet/ Console Status reports, the MultiCom Firewall has 3 other methods for informing you what is happening and if something is wrong.

- LED light messages
- Syslog messages
- SNMP messages

LED Light Messages

The LED lights on the front of your MultiCom Firewall are designed to give you a quick update on the current status of your firewall. Some of the things you can find out from your Interface LED lights (labeled LAN, WAN or DMZ) are

- If an ethernet interface is properly connected (a solid green light)
- If an interface is not connected (a solid red light)
- If data is traversing the interface (when the active port blinks orange, data is traveling through that interface)
- If there are collisions occurring on the firewall (the light blinks red)

Starting with Lightning-Linux 3.3 the Security LED is also functional and will show:

- If SecureWall is activated (a solid green light)
- If SecureWall is deactivated but SPI Filtering is activated (a solid orange light)
- If both SecureWall and Filtering are deactivated (a solid red light)

Syslog Messages

Syslog messages can be configured to be sent from the firewall to a syslog server. Please refer to the SNMP & Syslog chapter of the Reference Manual if you wish to use this functionality.

Some common, Syslog messages are:

- Telnet, ssh, and web logins, logouts and failures
- Failed and successful attempts to save a configuration file to the firewall
- IPSec activity
- Network Monitoring activity
- Network Monitoring activity
- Email activity
- DHCP activity
- PPPoE activity
- PPTP activity
- Stateful Packet Inspection (SPI) activity
- SecureWall dropped packets
- Startup of firewall

SNMP Messages

The MultiCom firewall can be configured to respond to SNMP requests from SNMP client software. Please refer to the SNMP & Syslog chapter of the Reference Manual if you wish to use this functionality.

Some common SNMP requests will show:

- Hostname and Linux firmware version
- Uptime
- Customizable location and contact information
- detailed information on each Ethernet interface

- detailed IP/UDP/ICMP packet statistics
- connection state for ports on the MultiCom Firewall and IP address of who is using that port (for instance for telnet or SSH CLI access)
- statistics on SNMP data requests
- route and ARP data stored on the MultiCom Firewall

Configurator messages

If you choose to use the Configurator Software, it also has a log window that lists successful activity and errors of the Configurator software. These error messages will explain if anything has gone wrong while using the Configurator software and will help identify what is causing the problem. The information in this window can be cut and paste for printing or emailing to Technical Support.

To see the Log window click on the Tools Menu and select the Show Log command.

The error messages from the Configurator allow you to cut and paste the text in most operating systems. Check with your operating system for it's method of cutting and pasting text into different windows.

Web Server Toolbox

The MultiCom Firewall offers a live toolbox for common maintenance activities. You just type in the IP address of the firewalls LAN or WAN interface (by default http://10.0.0.1), enter any necessary user names and passwords (by default user="multicom" and there is no password), and click on the Toolbox menu item. The following tools are available:

Tools	Function
Language Selection	Choose which language to see the web interface in or choose AUTO to select the language based on the language the web browser is configured to use.
Configure Time and Date	Enter the new date and time for the MultiCom Firewall
Update the Firmware	Tells the MultiCom Firewall where the upgrade firmware is and to start the upgrade process.
Reboot the Firewall	Reboots the MultiCom Firewall using the configuration in the “boot” memory position
Restore the Factory Defaults	This will delete all passwords, security parameters, option keys and configuration files and reboot with the factory default configuration
Load Options Key	Loads purchased option keys to activate additional features like Virtual Private Networks using IPSec or SSH Port Forwarding.

Web Server Advanced Tools

The MultiCom Firewall offers an configuration window for advanced maintenance activities. You just type in the IP address of the firewalls LAN or WAN interface (by default http://10.0.0.1), enter any necessary user names and passwords (by default user=“multicom” and there is no password), and click on the Advanced menu item. The following tools are available:

Tools	Function
Configuration Tools	Edit a live configuration, upload a new configuration from a text file, or save the current configuration to a text file.
Firewall Configuration Status	Advanced statistics about IP Services, Interfaces, Security, ARP, Routing, and the current system hardware and software.

Tools	Function
User Configuration	Create, edit or delete users and permissions on the MultiCom Firewall. Additionally you can login as a different user from this window. See the Reference Manual chapter on Concepts for explanations on the different users and rights.
Manage IPSec Connections	Enable, disable or remove IPSec connections. Requires an IPSec option to be installed.
Security	Edit a live security configuration, upload a new security configuration from a text file, or save the current security configuration to a text file. The security configuration contains the keys for creating IPSec tunnels. Additionally configure IPSec PKI keys and certificates here.
URL Filtering List	Enable or disable URL Filtering and directly edit the URL keyword list. Additional options are available when using the Configurator software.

Backup Your Configuration

It is important to maintain a backup of your configuration file in case of emergencies. This can easily be done with the built-in web server.

1. Start web browser software and go to http://10.0.0.1/advanced/config/ where 10.0.0.1 is the IP Address of the MultiCom Firewall's LAN interface.
2. Click on "Save current configuration" (if a question appears asking what to do with the file select "Save this file to disk".)
3. Enter in the name you want to save the configuration backup under and the directory location.
4. Click Ok

The file saved is a text file that you can save to a floppy or attach to an email.

Restoring A Configuration

When you need to restore a saved configuration file to your MultiCom Firewall firewall you will use the built in web server or the included Configurator software.

1. Start web browser software and go to http://10.0.0.1/advanced/config/upload/ where 10.0.0.1 is the IP Address of the MultiCom Firewall.
2. Enter the directory and name where the saved configuration file resides. Optionally use the Browse... button to search for the file on your hard disk.
3. Click Submit Values

NOTE - During the application of a new configuration or while an MultiCom Firewall is loading a new configuration during bootup the routing table is blocked. This allows all of the rules to be loaded before traffic can move through the firewall.

Updating Your Firmware

Because your MultiCom Firewall has been equipped with flash memory it is possible for you to update it with a newer operating system (also known as firmware) than was available when you purchased it.

NOTE — Contact your distributor or check the Lightning web site for notifications on the latest firmware. Additional charges may apply.

Upgrading the firmware on your MultiCom Firewall requires you to access the web server on the firewall. Your configuration files will remain untouched however the factory default configuration may change (this configuration is accessed when rebooting the Firewall while holding down the config button.)

Your MultiCom Firewall will reboot and be offline for up to 5 minutes during the upgrade process. Be sure that your network can afford to be without Internet access for at least 5 minutes and that there are no important data transfers occurring during this time.

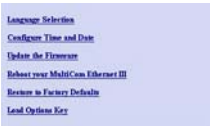
CAUTION - Please note, that if the power is interrupted during the upgrade process your MultiCom Firewall could become unusable and require repairs from your local distributor. Continue at your own risk.

To install the latest firmware follow the steps below. Please check the Support website for the latest version of the MultiCom Firmware Upgrade instructions.

Table 10: Steps to Upgrade MultiCom Firmware

1. Download the latest firmware to your computer

2. Access the MultiCom Firewall web server. Simply type in the IP Address of the MultiCom Firewall into an Internet browser which is connected to the same network as the MultiCom (usually this is the LAN interface).
3. Type in your username and password (by default the username is "multicom" and there is no password.)
4. Select `Toolbox` (or MultiCom Tools in firmware versions before 3.4)
5. Select `Update the Firmware`



6. Type in the location of the new firmware file or click `Browse` to find the file on your hard disk. If you use `Browse` you may need to choose “All Files (*.*) in the Type: box if you cannot see the firmware.

7. Select `Update Firmware` after you have selected the firmware file to update with.

8. The Web server will verify that the firmware is indeed valid before writing it to the device. If it is valid you will see the button `Write New Firmware`, press this button. Otherwise you are asked to reload the firmware.

   If the web server gives you an error or does nothing then try using a different web browser or check with your distributor for another copy of the firmware.

NOTE - this step is skipped in firmware versions 3.1 and higher. If the firmware is good you will jump to step 9 and write the new firmware. If the firmware is bad your router will reboot with the previous firmware.

9. The MultiCom Firewall now begins the process of erasing the old firmware and writing the new firmware. Wait for the MultiCom Firewall to reboot with the new firmware upgrade. The lights on the front of the device will change colors during the upgrade process and will stop blinking after the MultiCom Firewall has rebooted.

WARNING - While the firmware upgrade is being written do not interrupt the power to the MultiCom Firewall!

10. You are finished. Verify that your new version of Lightning-Linux firmware is currently installed in your MultiCom Firewall. In your web browser go to http://10.0.0.1/config/system/software/ where 10.0.0.1 is the IP Address of your MultiCom Firewall.

LED Status During Upgrade

Starting with Lightning-Linux 3.1 the leds on the front of your MultiCom Firewall indicate the status of the firmware upgrade according to the table below.

Table 11: LED Status during upgrade

Status	Description
Checking the validity of the firmware	All of the leds are lit green except the power led which is blinking green and black.
Erasing existing flash memory	All of the leds are lit green except the power led which is blinking orange and black.
Writing the new firmware into the flash memory	All of the leds are lit green except the power led which is blinking orange and green.
Error while erasing the existing flash memory	All of the leds are blinking red and orange.
Error while writing the new firmware to flash memory	All of the leds are blinking red and black.

Troubleshooting Firmware Upgrade

If power is interrupted during the flash upgrade process the existing firmware could become corrupted. Normally this will be evident because the lights are frozen every time you reboot the MultiCom Firewall and it will not respond to normal networking activity. To recover from this please contact your local distributor. If after a reboot you have the same firmware version that was previously installed then there was a problem with the firmware upgrade. Try reinstalling it again, rebooting the MultiCom Firewall into the default configuration and then try reinstalling again, download or contact your distributor for another copy of the firmware.

Remember that you will need to upgrade the Configurator software to the same version of the firmware that you just installed.

Chapter 5

Troubleshooting

When you are running a network (whether one computer connected directly to the Internet or many) it is possible that problems can come up. Maybe the network is giving you slow responses, some devices or computers are not reachable, you are reaching the wrong computer or your filters do not seem to be working. This chapter will help you fix some common networking issues.

To correctly fix the problem the source of it must be found. In networking this is especially true because the problem may not necessarily point you toward the answer (for instance a bad DNS server would stop you from reaching web addresses but not if you only used the IP address.)

There are two questions you must always check...

1. Were the instructions followed correctly
2. Has anything recently changed before the problem occurred? (for instance are you using new network drivers, new workstation on the network...)

If these two questions do not help you find the problem then it is time to do some troubleshooting with the firewall itself.

Basic Things To Check

Always check that your cabling and basic connections are functioning correctly for the ports you are using. If there is a problem moving your data back and forth at this level then higher level troubleshooting will be ineffective.

- Are the cables correct (crossed cable versus straight cable.)
- Are the interface lights (LAN, WAN, DMZ) on the firewall green when the cables are plugged into your ethernet card/interface or xDSL, cable or wireless modems?
- Are the lights on the hub or ethernet interface of the device green where the firewall cable is plugged in.

These answers must be yes before you do any more in-depth troubleshooting. If there are problems here and you are using a hub, be sure to verify that you are not using the uplink port. Otherwise try verifying the ethernet device is functioning correctly and try switching the ethernet cable to one that you know is good.

If all of the physical connections are good (as tested above) the next steps is to verify that you can:

1. from your computer, communicate with the LAN interface of the MultiCom Firewall
2. from the MultiCom Firewall, communicate with your ISP
3. from your computer, communicate with the Internet

TIP - A simple troubleshooting step is to reboot the MultiCom Firewall and try again. If all else fails, reset the Firewall into the default mode as described in the “Resetting the Default Configuration” Section on page 105. Then reconfigure it using the Easy-Setup.

After checking these basic issues please continue to the Common Network Problems on the next page which describe some common problems that may occur on your Local Network.

Finally, look at the sections below that corresponds to the type of connection that your ISP uses - DHCP, PPPoE, PPTP. These sections will explain common problems on the Remote Network that connects you to your ISP and the Internet. If you are still having problems consider calling technical support.

Common Local Network Problems

Please look over these common reasons for networking problems. Additionally, please check the section below relating specifically to your type of connection (DHCP, PPPoE, PPTP, Static IP addresses.)

Once you know that your cabling is okay it is time to ask some more detailed questions.

- Is the modem working? (check the diagnostics that came with the modem, maybe you can check LED displays or communicate directly with the modem)
- Is TCP/IP installed on your computer? (if you can ping 127.0.0.1 in a telnet window/ DOS window TCP is installed)
- Is the firewall reachable? (using the ping command for instance in a telnet window/ DOS window and try PING 10.0.0.1 where 10.0.0.1 is the IP Address of your MultiCom Firewall's LAN interface.) Sometimes a Filter or recent configuration change can block access to the Firewall.
- Did you try using an IP address (such as http://193.247.134.2) to reach a web site. If it does then your DNS is not reachable and you should check with your Internet Service Provider.
- Is there another DHCP server on your Local Network in addition to the one on the MultiCom Firewall? If so you can only have one so you must disable one of them.
- Were you using an analogue modem before connecting the Broadband modem? Maybe you forgot to change the Internet Options of Windows. Be sure that under the Control Panels>Internet Connections>Connections the "Never dial a connection" is activated or your computer will keep trying to use the modem.
- If you are using more than one Ethernet card on your computer be sure that you do not have more than one default route.
- Are there other devices on your network using the same IP Address as the MultiCom Firewall's LAN interface (10.0.0.1) the IP Addresses being given by the Firewall's DHCP server?
- If you are using a Static IP on your Local Network make sure that each of your workstations are configured to be on the same subnet as the MultiCom Firewall and use the Firewall as their default Gateway.

DHCP Troubleshooting

DHCP To The Internet

With DHCP configured for your WAN interface your MultiCom Firewall sends out discovery packets looking for a DHCP server to give it an IP configuration. If a DHCP server is not found then the WAN interface is not enabled (i.e. you cannot reach the Internet.)

Some common connection problems are...

- DHCP is not being used by your Internet Service Provider
- your cabling is incorrect
- your modem is not configured as a bridge
- you changed the time on the MultiCom Firewall but did not reboot
- your WAN and LAN interfaces are using the same IP address range

To check the status of your WAN interface using DHCP visit the WAN DHCP client status web page using the web server diagnostic pages (found at “Web Server Status Reports” on page 74.) Also be sure to check the IP configuration received by your workstations and that the firewall IP address received is the IP address of your MultiCom Firewall (the default setting is 10.0.0.1).

Table 12: WAN DHCP client status states

State of the interface	Possible problem
Disabled	DHCP is not enabled for this interface.
Expired	The existing IP configuration has expired without it being renewed. Check that firewall was rebooted after changing the time.
Trying to get address	The firewall is in the process of trying to get an IP configuration from the Internet Service Provider.
Failed	The attempt to contact a DHCP server failed, check all troubleshooting steps.
Assigned	The DHCP interface is functioning correctly.
Rebind	Normal DHCP activity, check back soon to see if the state is Assigned or Failed.
Renew	Normal DHCP activity, check back soon to see if the state is Assigned or Failed.

DHCP is not being used by your Internet

Service Provider

Verify that your Internet Service Provider uses DHCP to configure your connection to them. Other possible connections may be PPPoE or a static IP configuration.

State: Trying to get address or State: failed or State: Assigned or State: Expired

Your cabling is incorrect

Be sure that the WAN interface light on your MultiCom Firewall is green. If it is not you either have the wrong cable, a faulty cable or the broadband modem is not plugged in. Try switching cables and verify that the modem is indeed turned on.

Your modem is not configured as a bridge

Your broadband modem must be configured as a bridge for you to connect directly to your Internet Service Provider. Verify with the instruction manual of your modem that it is indeed configured as a bridge. If the two above steps are not showing a problem this may be your problem.

You changed the time on your firewall but did not reboot.

The default date of your MultiCom Firewall is January 1970. DHCP works on a lease system where IP configurations are good for a specified amount of time. When the original lease runs out your MultiCom Firewall will attempt to renew its IP configuration information but will erroneously report that the IP configuration has expired (since the current date is now more then 30 years in the future.) The easiest fix for this is to reboot the MultiCom Firewall and it will make a fresh request using the new time.

Your WAN and LAN interfaces are using the same IP address range

This will normally only happen office to office connections since the default IP range of 10.0.x.x for your LAN network is never used on the Internet. Check that the WAN network is not assigning address in the 10.0.x.x range

and if it is change either the LAN or the WAN network so that one of them uses a different range of IP addresses. For example, reconfigure your LAN address range to be from 192.168.0.2-192.168.0.100.

DHCP On Your Local Network

Using DHCP on to manage your own network's IP addresses makes administration convenient. The most common problem is that a device is unable to receive an IP configuration from the DHCP server (normally your MultiCom Firewall. Below are some reasons this might happen.

- your workstations are not configured as DHCP clients
- there are not enough IP addresses for your computers
- there is another DHCP server on your network
- there is another device on your network with the same IP address as your firewall
- you changed the time on the MultiCom Firewall but did not reboot

Be sure to check the LAN DHCP server leases page to see what IP addresses have been assigned and their status. These require using the web server diagnostic pages found at "Web Server Status Reports" on page 74.

Your workstations are not configured as DHCP clients

Check that each workstation is configured as a DHCP client. For some operating systems setting this configuration requires you to reboot your workstation. Please refer to the section on Configuring your Computers or to the manuals that came with your computer for instructions on configuring this setting.

There are not enough IP addresses for your computers

The default setting of the MultiCom Firewalls allows for up to 1,000 DHCP clients. If you either need more than this or have customized your settings please refer to the Lightning-Linux manual for more information.

There is another DHCP server on your

network

If you are sure that your workstations are configured as DHCP clients and they are receiving IP configuration information check the LAN DHCP server leases page to see if those computer names or IP addresses show up there. If they do not then you may have another DHCP server on your network giving out configurations. Check with your Computer Administrator to see if this is the case.

Only one DHCP server is allowed on your local network. If there is another one in place you need to decide to use the built-in one of the MultiCom Firewall or your other server.

There is another device on your network with the same IP address as your firewall

Your MultiCom Firewall has a default IP address of 10.0.0.1 on the LAN interface. You cannot have another ethernet device on your network with this same IP address. Consider changing the other devices IP address or change the IP address of your MultiCom Firewall.

You changed the time on your firewall but did not reboot.

The default date of your MultiCom Firewall is January 1970. DHCP works on a lease system where IP configurations are good for a specified amount of time. When the original lease runs out your MultiCom Firewall will attempt to renew its IP configuration information but will erroneously report that the IP configuration has expired (since the current date is now more then 30 years in the future.) The easiest fix for this is to reboot the MultiCom Firewall and it will make a fresh request using the new time.

PPPoE Troubleshooting

If you are using a PPPoE connection there are a few specific troubleshooting steps for you to try. These require using the web server diagnostic pages found at “Web Server Status Reports” on page 74. Common problems that can block your Internet connection include...

- incorrect password

- PPPoE server (ISP) not available
- some web sites are not available

Incorrect Password

If you have typed in an incorrect username or password you will not be able to open a PPPoE Internet connection with your Internet Service Provider.

To check if this is the case visit the PPPoE Link status page on your firewall. You will see the error message “CHAP authentication failed”. This means that a connection to the ISP is possible but that the username and password you have entered is incorrect.

Verify your username and password is correct and/ or contact your Internet Service Provider.

PPPoE Server (ISP) Not Available

If your cabling is incorrect, the modem is not functioning/ configured properly or the xDSL line is not functioning you will not be able to reach your ISP’s PPPoE server to correctly use their services.

To check that this connection is available or not visit the PPPoE Link status page on your firewall. If you see the error message “Endpoint not connected” that means there is no available connection to the ISP.

Check that your cables are connected properly (all interface lights are green on your modem and MultiCom Firewall), and that the modem is configured to act as a bridge. Finally if these are OK, contact your Internet Service Provider to verify the line is connected properly.

Some Web Sites Are Not Available

In some cases certain web sites will not be available when using PPPoE connections. Using PPPoE over the Internet requires that data packets of a certain size move over the Ethernet connection. Usually this process is done by the remote web server using a discovery process to discover the best size of data packets to use. Sometimes Internet routers between you and the web page you are trying to reach do not support this process and the data is dropped by these routers.

When this problem is happening, normally small packets will move back and forth fine but large data packets (often occurring during file transfer, web page reception, and media streaming) will not reach your computer. This problem will be evident in the following ways

Table 13: PPPoE Frame Size Symptoms

Web Page/ HTTP	your browser will seem to connect but no data or web page comes back
FTP	you can login into a web server but cannot use dir (ls) of directories with a lot of files and cannot transfer large files
Telnet	you can log into a telnet server but any action which sends your computer a lot of text will hang the connection
Email (POP3)	you can often log into the remote email server and even receive small messages of a few lines but larger emails or long lists of emails will not transfer to your computer
Real Player or Microsoft Media Player	when using TCP or HTTP options to make a connection the connection will start but then stops saying the network is busy or it is rebuffering (however using UDP works fine)
Ping	usually pinging the remote host will work fine but this requires that you have ping software on your computer to test with

The easiest fix for this problem is to enable the TCP Frame Size Adaption option under your PPPoE configuration. To do this go back through the Easy Setup you used to configure your firewall and select “enable” by the question asking if you want to use TCP Frame Size Adaption. This sends the correct size of packet to use automatically to remote web servers using TCP.

You can try communicating with your Internet Service provider but the problem may be out of their control as the router causing the problem can be half way around the world.

More information about this can be found in RFC2923 “TCP Problems with Path MTU Discovery”

Other Sources Of DSL Information

DSL Reports at http://www.dslreports.com/

PPTP Troubleshooting

If you are using a PPTP connection there are a few specific troubleshooting steps for you to try. These require using the web server diagnostic pages found at “Web Server Status Reports” on page 74. Common problems that can block your Internet connection include...

- incorrect password
- PPTP server (ISP) not available
- incorrect IP configuration of WAN or LAN

Incorrect Password

If you have typed in an incorrect username or password you will not be able to open a PPTP Internet connection with your Internet Service Provider.

To check if this is the case visit the PPP Link (LCP) status page on your firewall. You will see the error message “CHAP authentication failed”. This means that a connection to the ISP is possible but that the username and password you have entered is incorrect.

Verify your username and password is correct and/ or contact your Internet Service Provider.

PPTP Server Not Available

If your cabling is incorrect, the modem is not functioning/ configured properly, the xDSL line is not functioning, or the IP Address of the WAN interface is not in the same subnet as the Broadband Modem you will not be able to reach your Broadband Modem’s PPTP server to correctly receive the IP configuration to communicate with the ISP.

To check that this connection is available or not visit the PPTP status page on your firewall. If you see the error message

- “Connection refused” means the IP address that was given for the PPTP Server is refusing to allow an PPTP connection.

- “Connection timed out” means there is no response from the remote IP Address when a request is made to open a PPTP tunnel.

Check that your cables are connected properly (all interface lights are green on your modem and MultiCom Firewall), and that the modem is configured to act as a bridge. Finally if these are OK, contact your Internet Service Provider to verify the line is connected properly.

Incorrect IP configuration of WAN or LAN

If the IP Address of the WAN interface is not in the same subnet as the Broadband Modem you will not be able to reach your Broadband Modem's PPTP server to correctly receive the IP configuration to communicate with the ISP.

To check that this connection is available or not visit the PPTP status page on your firewall. If you see the error message

- "No route to host" means the WAN Interface is configured for a different subnet than the IP address that was given for the PPTP Server.

Resetting The Default Configuration

If you think that a configuration is preventing you from accessing the firewall you may want to restore the default configuration of the firewall and start with a fresh configuration file. When you want to restore the default configuration for your MultiCom Firewall you need only to follow these steps.

For firmware 3.6+

1. Leave the MultiCom Firewall powered on
2. Hold down the config button in the back, using a ballpoint pen if available, until the front LED lights change to RED. This will load the factory default configuration.
3. Optionally holding the config button down until the LEDs are ORANGE will load the last saved boot config or holding the config button down until the LEDs are GREEN will load the configuration in memory position 1.

NOTE - Resetting the default configuration this way does not erase your user accounts. To load the default configuration with the default "multicom" user account you will need to follow the instructions for **For firmware 3.0-3.4.1** below.

For firmware 3.5+

1. Leave the MultiCom Firewall powered on
2. Hold down the config button in the back, using a ballpoint pen if available, for 6 or more seconds will load the default configuration. (holding the config button down for 3 seconds will load the boot config.)

For firmware 3.0-3.4.1

1. Power off the MultiCom Firewall.
2. While holding down the config button in the back (using a ballpoint pen if available), turn on the MultiCom Firewall.
3. Wait for the firewall to finish booting up; this is when the LAN and WAN light remain either a steady green or red and the rest of the LEDs have stopped blinking.

The factory default configuration is then loaded up into the current memory location of the MultiCom Firewall. Configurations that were stored in the firewall prior to the reset are still saved in the memory of the firewall.

CAUTION - This configuration is temporary and unless you save it to the Boot Memory location on the firewall, your original configuration will return after a reboot.

To completely reset the firewall you will need to save this default configuration to the Boot Config memory location so that every time the firewall reboots it will load the default configuration.

This may be useful if you have configured your firewall in such a way that it is inaccessible (accidentally typing in the wrong IP address or if you have moved

the firewall to a different network).

Chapter 6

Frequently Asked Questions

Below are a collection of frequently asked questions (FAQ). For a more up to date FAQ list on the MultiCom Firewall or the IPSec functionality be sure to check the LIGHTNING web site at http://www.lightning.ch.

Frequently Asked Questions

What will a power outage do?

Without power no data will be able to go through the firewall. If you have saved your config to the memory of the firewall (such as the config boot location) then it will still be there when you boot up again. If your changes were only made in the config current location then your changes are erased and you will need to load them from a backup copy.

However, after 2 day without power your MultiCom Firewall will forget what the date is and reset itself back to January 1970. You would need to rest the date to the current time.

Can I back up my configuration?

Yes, you can save your configuration to a text file. Refer to the section on saving your configuration

My changed configuration disappeared after a reboot, what happened?

If you only save a configuration to the Current Config memory location in your firewall it is only temporary and will be erased after a reboot. This is useful for tests and quick changes. Be sure to always backup your config changes to a text file and/or keep a copy in one of the permanent memory locations in the firewall.

After making changes to the configuration I cannot reach the firewall any more.

Since you communicate with the firewall via an Ethernet connection it is possible to accidentally filter all traffic or route it incorrectly and hence block your own access to the firewall. In that case you will need to reboot the firewall into the default configuration and either edit your saved configuration or make a new one.

What is the default configuration of the firewall?

The while the default setting may be changed by your distributor or Internet To see the default configuration installed in the Ethernet firewall see the Concepts Chapter of the Lightning-Linux Reference Manual.

Why do some network services seem very slow after I have applied filtering?

Be sure to have read the chapter on filtering data and that you understand how your software communicates with remote servers. In particular port 113 is often used to verify if a communication link is valid and if all external packets are being dropped instead of rejected (allowing a message to be sent back to the remote server) the software keeps waiting for a response, eventually timing out.

How do I know what ports are being used?

The best place is to check with the manufacturer of the software that you are using. Consider using network monitoring software such as network monitor for Windows NT Server or the free software Ethereal at http://www.ethereal.com/ to track usage over a general amount of time and identify ports and addresses that are commonly being used.

Another option is to set the filters on your Ethernet firewall to log all types of TCP and/or UDP data. Your Syslog server will receive messages reporting all network traffic and you can then study the output for common usage types.

Can I use the firewall as a bridge?

The Ethernet firewall is not designed to be used as a bridge at this time.

What is the order that data goes through the firewall?

1. Data comes into an interface as Input and is subject to Input NAT rules for the particular interface
2. Data is subject to filtering rules* (in the Filtering Forward Panel)
3. Data is subject to routing rules
4. Data goes out an Interface as Output and is subject to Output NAT rules for the particular interface

*data going directly to the firewall (telnet for example) use the Filtering Input panel and data leaving directly from the firewall (syslog message for example) uses the Filtering Output panel

How can I filter any thing but a certain address?

In the filtering source window you have the option of adding a ! before the IP address or Port number. For instance if you selected !10.0.0.1 you are selecting every IP address but 10.0.0.1. The same reaction occurs for ports such as !1000–2000 means all ports except those between 1000 and 2000.

If I log a packet will it continue through the filtering rules or will it be dropped?

Logging a packet in the filtering rules table does not stop it from going through other rules which in turn could drop, accept or use any other available action on them.

What is a connection and how does it affect my filtering rules?

Because data packets are necessarily small they may not contain all of the information that was requested in a data transaction (such as downloading a web page). When the first packet is allowed through you are actually saying that traffic related to this connection should be allowed through until its completion.

What is the IP address of my firewall?

Devices do not have IP addresses, only their interfaces. In that sense there are two IP addresses that will reach you firewall, the one on the LAN side and the one on the WAN side. If you have a DMZ, Wireless, DSL or multi-PPPoE configurations, your MultiCom can be reached by IP addresses assigned to those interfaces.

Do routing rules take place before or after IP addresses have been translated by NAT?

Routing takes place after IP network address translation, unless Output NAT

rules are being used. Any Output NAT rules change the data after routing.

What happens if I turn off the SecureWall Firewall?

When the SecureWall Firewall is enabled for an interface all incoming data-packets must have a matching NAT rule to allow them into the network, either through the internal Connection Tracking table (which keeps track of all outgoing requests to the Internet for data) or a fixed rule for services like Virtual IP or Port Mapping to an internal computer or server. When the SecureWall Firewall is turned off then data can come through with or without matching a NAT rule and it is up to the Stateful Packet Inspection Firewall to turn away data packets that you do not want.

If I use NAT to map a range of ports or IP addresses how does it choose?

Choosing ranges of port numbers or IP addresses tells NAT to randomly choose a number in this range to use for its mapping. This is also known as Round-Robin load-sharing.

Is it possible to assign more than 1 IP address to the WAN interface?

You can use NAT to have the Ethernet firewall accept data packets for an IP address other than the one assigned to the WAN interface. ARP requests to the WAN interface are only replied to when the requested IP address is the one assigned to the WAN interface or if the ARP Proxy is configured to respond to a chosen IP address. Otherwise no ARP replies will occur for the other IP addresses using NAT. Check the Virtual IP section of the Reference Manual.

If I am using NAT to redirect WAN data to an internal server can I also redirect LAN requests?

Yes, you can redirect LAN and WAN data to the same server when you enter in a NAT rule in the NAT Global panel and activate NAT on the LAN interface. This is a common use when redirecting HTTP (web) traffic to a publicly known IP address for users on the LAN... allowing them to use the same IP address as the external or WAN users. Activating NAT on the LAN interface will however make all traffic seem to originate from the LAN interface itself and so possibly cause problems with any statistics logs you are keeping. In this case it might be better to use the DNS server on the LAN instead of activating NAT.

Can I reset the connection for my WAN port on the Ethernet firewall

For a static configuration you simply use the Web Interface to access and

change the WAN settings. For a DHCP client setting on an interface you need to telnet into the Ethernet firewall and enter `dhcpclient WAN renew`. And for a PPPoE configuration you open the Monitor window of the Configurator software, goto the PPP window and select the PPPoE interface you are using, and then click the RESET button on the screen. Of course you could always simply reboot the device to reset all services.

Software, Shareware and Freeware

The following software is either included on your MultiCom Companion CD or is mentioned here as a possible solution for your tests and troubleshooting. LIGHTNING Instrumentation assumes no responsibility for the use, maintenance or damage these software products may cause. Please refer to the software's authors for support and any other information you may need.

Please check the author's web sites for the latest information on these software packages.

General Utilities

Adobe Acorbat (document reader) at http://www.adobe.com

Firefox (web browser) at http://www.mozilla.org/products/firefox/

Internet Explorer (web browser) at http://www.microsoft.com/ie

MP Commander 2 at http://www.lightning.ch

Netscape (web browser) at http://www.netscape.com

Opera (web browser) at http://www.opera.com

Windows

Active SNMP at http://www.cscare.com/activesnmp/

Adaware (spyware removal) at http://www.lavasoftusa.com/

Cain & Abel (Network security tests) at http://www.oxid.it/cain.html

Ethereal (network protocol analyzer) at http://www.ethereal.com

Expander (file compression) at http://www.aladdinsys.com/

Expect (telnet, ftp automation) at http://expect.nist.gov/

Eyeball Chat (video conferencing) at http://www.eyeball.com/

FileZilla (FTP and SFTP file transfer) at http://filezilla.sourceforge.net/

NetMeeting (video conferencing) at http://www.microsoft.com/netmeeting/

NetStumbler (wireless network discovery tool) at http://www.netstumbler.com/

NetView Scanner at http://www.rawlogic.com

Kiwi CatTools (automated device configuration management) http://www.kiwisyslog.com/

Kiwi Syslog Daemon (syslog message viewer and archiver) at http://www.kiwisyslog.com/

NetStat Live at http://www.analogx.com/contents/download/network.htm

Nmap for Windows (port scanning) at http://sourceforge.net/projects/nmapwin

NetTime (time synchronisation client) at http://nettime.sourceforge.net/

OpenSSH (SSH/SCP/SFTP server/ client) at http://sshwindows.sourceforge.net/

PuTTY (ssh telnet) at http://www.chiark.greenend.org.uk/~sgtatham/putty/

RealVNC (visual remote control) at http://www.realvnc.com/

RSS News Ticker (RSS News feeds) at http://www.rssnewsticker.com/

Sam Spade (network query tool) at http://www.samspade.org

The Green Bow (IPSec VPN client) at http://www.thegreenbow.fr/vpn.html

WAMP (webserver/ database for windows) at http://www.wampserver.com/

What's UP (network management software) at http://www.ipswitch.com

Winzip (file compression) at http://www.winzip.com/

Macintosh OS Classic

AGNetTools at http://www.aggroup.com/products/agnettools

Better Telnet 2.0 (FAT)at http://www.cstone.net/~rbraun/mac/telnet/

Expander at http://www.aladdinsys.com/

Fetch FTP at http://fetchsoftworks.com

Interarchie (FTP client) at http://www.stairways.com/

IPNetMonitor at http://www.sustworks.com/site/prod_ipmonitor.html

Mac NetLogger 0.96b8 at http://www.laffeycomputer.com/

MacSSH (ssh telnet) at http://pro.wanadoo.fr/chombier/

MacTelnet 3.0 at http://www.mactelnet.com

NCSA Telnet 2.6 at http://www.ncsa.uiuc.edu/SDG/Software/MacTelnet/Docs

OTTool at http://www.neon.com/

PortSniffer 68K at http://www.zdnet.com

PortSniffer PPC 2.0 at http://www.zdnet.com

SLog 2.5a1 at http://www.macdownload.com

Socket Sifter at http://www.ekimsw.com/socketsifter/

Transmit 1.5 (FAT) at http://www.panic.com/transmit/

TrashScan 1.0.3 at http://www.zdnet.com

VNC (visual remote control) at http://www.uk.research.att.com/vnc/

What Route at http://crash.ihug.co.nz/~bryanc/readme.html

Macintosh OSX

Aqua Ethereal (x11 based version of Ethereal) at http://www.wordtech-software.com/aquaethereal.html

AquaPacket (tcpdump, traffic sniffing) at http://www.wordtech-software.com/aquapacket.html

Chicken of the VNC (remote control) at http://sourceforge.net/projects/cotvnc/

Dans Guardian (web content filtering) at http://www.lopata.net/staticpages/index.php?page=DGCHome

Fugu (SFTP, SCP and SSH Frontend) at http://rsug.itd.umich.edu/software/fugu/

IPSecuritas (IPSec client) at http://www.lobotomo.com/

iStumbler (finding wireless networks and devices) at http://www.istumbler.net/

JellyfiSSH (SSH telnet client) at http://www.arenasoftware.com/grepsoft/

OSXVNC (remote control) at http://www.redstonesoftware.com/vnc.html

Privoxy (web proxy and content filtering) at http://www.privoxy.org/

PureFTPd Manager (file transfer management) at http://jeanmatthieu.free.fr/

Remote Desktop Client (connect to Windows) at http://www.microsoft.com/mac/otherproducts/otherproducts.aspx?pid=remotedesktopclient

VPN Tracker (IPSec client) at http://www.equinux.com/us/products/vpntracker/

XNMAP (network auditing) at http://homepage.mac.com/natritmeyer/

Linux

Cheops at http://www.marko.net/cheops/

Ethereal at http://www.ethereal.com/

Expander at http://www.aladdinsys.com/

Expect at http://expect.nist.gov/

IP Traffic at http://cebu.mozcom.com/riker/iptraf/

Knoppix at http://www.knoppix.net/

Nessus at http://www.nessus.org/

Netstatpl at http://freshmeat.net

Net-tools at http://freshmeat.net

NMAP at http://www.insecure.org/nmap/

RealVNC (visual remote control) at http://www.realvnc.com/

Sniffit at http://reptile.rug.ac.be/~coder/sniffit/sniffit.html

Tcpdump at http://www.tcpdump.org/

Tkined (Scotty) at http://wwwsnmp.cs.utwente.nl/~schoenw/scotty

Appendix A

Hardware Specifications

Please refer to the section describing your particular MultiCom Firewall. If you are unsure what model you have refer to the title on the cover of the firewall or to the box that your firewall arrived in.

Additionally, the pin assignments for MultiCom products is at the end of this section.

The MultiCom Firewall line of products is as follows:

- MultiCom Ethernet II
- MultiCom Ethernet III
- MultiCom SpeedSurf
- MultiCom Enterprise Ethernet

Ethernet II

Physical Specifications

Table 14: Physical Specifications Ethernet II

Dimensions:	26 x 18 x 3.5 cm
Weight:	0.6 kg
Ethernet:	1 x 10BaseT RJ45 MDI 10 Mbits/s (WAN) 1 x 100BaseTX RJ45 MDI 10/100 Mbits/s autosensing (LAN) supporting full and half duplex modes
LED Display:	WAN, LAN, Power
Power:	12V DC, 1.2 A
Temperature:	5° to 40° C
Humidity:	10% to 85% non-condensing
Noise:	Noiseless
Approvals:	CE
Standards:	IEEE 802.3 (10Base T) CSMA/CD IEEE 802.3u (100BaseTX) CSMA/CD
MTBF Value:	100,000 hours

Maximum cable segment length of 100 m (327.86 ft) for 10BaseT or 100BaseTX

Cabling 10BaseT - STP Category 3 or better

Cabling 100BaseTX - STP Category 5 or better

Declaration of Conformity

Conforms to EN45014 of the ISO/IEC

Manufacturer	LIGHTNING Instrumentation S.A.
Address	Avenue des Boveresses 50 CH-1010 Lausanne, Switzerland

declares that the product:

Name of Product	MultiCom Ethernet II
Reference Number	MultiCom Ethernet II

conforms to the following standards:

Safety (73/23/EEC)

EN 60950

EMC (89/336 EEC)

EN 300386-2

- Emission

EN 55022 class B

FCC Part 15 subpart B class B

- Immunity

EN 61000-6-2

EN 6100-4-2 Electrostatic discharge

EN 6100-4-3 Electromagnetic fields

EN 6100-4-4 Fast electric transcients

EN 6100-4-5 Surge

EN 6100-4-6 Conducted disturbance

EN 6100-4-11 Voltage dips, short interruptions

following the provisions of the EC directive **RTTE 99/5 EEC**

Lausanne, Switzerland

November 2000

Ethernet III

Physical Specifications

Table 15: Physical Specifications Ethernet III

Dimensions:	26 x 18 x 3.5 cm
Weight:	0.6 kg
Ethernet:	1 x 10BaseT RJ45 MDI 10 Mbits/s (WAN) 4 x 100BaseTX RJ45 MDI-X 10/100 Mbits/s autosensing switched ports (LAN) 1 x 100BaseTX RJ45 MDI 10/100 Mbits/s autosensing (DMZ) supporting full and half duplex modes
LED Display:	WAN, LANx4, DMZ, Security, Power
Power:	12V DC, 1.2 A
Temperature:	5° to 40° C
Humidity:	10% to 85% non-condensing
Noise:	Noiseless
Approvals:	CE
Console:	RS-232 (RX/TX only with special cable)
Standards:	IEEE 802.3 (10Base T) CSMA/CD IEEE 802.3u (100BaseTX) CSMA/CD
MTBF Value:	100,000 hours

Table 16: Console Configuration

Protocol:	Asynchronous RS-232 (RX/TX only)
Baud Rate:	9600 bits/s
Number of Data Bits:	8
Number of Stop Bits:	1
Parity Bit:	No parity
Handshake:	None
Line Drivers:	RS-232

Maximum cable segment length of 100 m (327.86 ft) for 10BaseT or 100BaseTX

Cabling 10BaseT - STP Category 3 or better

Cabling 100BaseTX - STP Category 5 or better

Declaration of Conformity

Conforms to EN45014 of the ISO/IEC

Manufacturer	LIGHTNING Instrumentation S.A.
Address	Avenue des Boveresses 50 CH-1010 Lausanne, Switzerland

declares under sole responsibility that the product:

Name of Product	MultiCom Ethernet III
Reference Number	MultiCom Ethernet III

to which this declaration relates, are in conformity with the following standards:

Safety (73/23/EEC)

EN 60950

EMC (89/336 EEC)

EN 300386-2

- Emission

EN 55022 class B

FCC Part 15 subpart B class B

- Immunity

EN 61000-6-2

EN 6100-4-2 Electrostatic discharge

EN 6100-4-3 Electromagnetic fields

EN 6100-4-4 Fast electric transcients

EN 6100-4-5 Surge

EN 6100-4-6 Conducted disturbance

EN 6100-4-11 Voltage dips, short interruptions

following the provisions of the EC directive **RTTE 99/5 EEC**

Lausanne, Switzerland

June 2001

MultiCom SpeedSurf

Physical Specifications

Table 17: Physical Specifications MultiCom SpeedSurf

Dimensions:	13.6 x 8.5 x 3.0 cm
Weight:	0.12 kg
Ethernet:	1 x 10BaseT RJ45 MDI 10 Mbits/s (WAN) 1 x 100BaseTX RJ45 MDI 10/100 Mbits/s autosensing (LAN) supporting full and half duplex modes
LED Display:	WAN, LAN, Security, Power
Power:	4.5V DC, 1.5 A
Temperature:	5° to 40° C
Humidity:	10% to 85% non-condensing
Noise:	Noiseless
Approvals:	
Console:	RS-232 (RX/TX only with special cable)
Standards:	IEEE 802.3 (10Base T) CSMA/CD IEEE 802.3u (100BaseTX) CSMA/CD
Security:	Kensington Lock Slot
MTBF Value:	100,000 hours

Table 18: Console Configuration

Protocol:	Asynchronous RS-232 (RX/TX only)
Baud Rate:	9600 bits/s
Number of Data Bits:	8
Number of Stop Bits:	1
Parity Bit:	No parity
Handshake:	None
Line Drivers:	RS-232

Maximum cable segment length of 100 m (327.86 ft) for 10BaseT or 100BaseTX

Cabling 10BaseT - STP Category 3 or better

Cabling 100BaseTX - STP Category 5 or better

Declaration of Conformity

Conforms to EN45014 of the ISO/IEC

Manufacturer	LIGHTNING Instrumentation S.A.
Address	Avenue des Boveresses 50 CH-1010 Lausanne, Switzerland

declares that the product:

Name of Product	MultiCom SpeedSurf
Reference Number	MultiCom SpeedSurf

conforms to the following standards:

Safety (73/23/EEC)

EN 60950

EMC (89/336 EEC)

EN 300386-2

- Emission

EN 55022 class B

FCC Part 15 subpart B class B

- Immunity

EN 61000-6-2

EN 6100-4-2 Electrostatic discharge

EN 6100-4-3 Electromagnetic fields

EN 6100-4-4 Fast electric transcients

EN 6100-4-5 Surge

EN 6100-4-6 Conducted disturbance

EN 6100-4-11 Voltage dips, short interruptions

following the provisions of the EC directive **RTTE 99/5 EEC**

Lausanne, Switzerland

September 2001

Enterprise Ethernet

Physical Specifications

Table 19: Physical Specifications Enterprise Ethernet

Dimensions:	44.1 x 4.4 x 23.5 cm (without optional external mounts)
Weight:	2.8 kg
Ethernet:	4 x 100BaseTX RJ45 MDI-X 10/100 Mbits/s autosensing switched ports (LAN) 2 x 100BaseTX RJ45 MDI 10/100 Mbits/s autosensing (WAN & DMZ) supporting full and half duplex modes
LED Display:	WAN, LANx4, DMZ, Security, Power
Power:	100-240V AC, ~50-60HZ, 0.5 A
Temperature:	5° to 40° C
Humidity:	10% to 85% non-condensing
Noise:	Noiseless
Approvals:	CE
Console:	RS-232 (RX/TX only with special cable)
Standards:	IEEE 802.3 (10Base T) CSMA/CD IEEE 802.3u (100BaseTX) CSMA/CD

Table 20: Console Configuration

Protocol:	Asynchronous RS-232 (RX/TX only)
Baud Rate:	9600 bits/s
Number of Data Bits:	8
Number of Stop Bits:	1
Parity Bit:	No parity
Handshake:	None
Line Drivers:	RS-232

Maximum cable segment length of 100 m (327.86 ft) for 10BaseT or 100BaseTX

Cabling 10BaseT - STP Category 3 or better

Cabling 100BaseTX - STP Category 5 or better

Declaration of Conformity

Conforms to EN45014 of the ISO/IEC

Manufacturer	LIGHTNING Instrumentation S.A.
Address	Avenue des Boveresses 50 CH-1010 Lausanne, Switzerland

declares under sole responsibility that the product:

Name of Product	MultiCom Enterprise Ethernet
Reference Number	MultiCom Enterprise Ethernet

to which this declaration relates, are in conformity with the following standards:

Safety (73/23/EEC)

EN 60950

EMC (89/336 EEC)

EN 300386-2

- Emission

EN 55022 class B

FCC Part 15 subpart B class B

- Immunity

EN 61000-6-2

EN 6100-4-2 Electrostatic discharge

EN 6100-4-3 Electromagnetic fields

EN 6100-4-4 Fast electric transcients

EN 6100-4-5 Surge

EN 6100-4-6 Conducted disturbance

EN 6100-4-11 Voltage dips, short interruptions

following the provisions of the EC directive **RTTE 99/5 EEC**

Lausanne, Switzerland

November 2001

Pin Assignments

Table 21: MultiCom Firewall Interfaces

Pin #	WAN Interface of *Ethernet II, III, SpeedSurf* - 10 Mbits/s, MDI	LAN Interface of *Ethernet II, SpeedSurf* - 10/100 Mbits/s, MDI	LAN Switched Hub of *Ethernet III & Enterprise Ethernet* - 10/100 Mbits/s, MDI-X	DMZ Interface of *Ethernet III*, DMZ/WAN of *Enterprise Ethernet* - 10/100 Mbits/s, MDI
1	Ethernet TX+	Ethernet TX+	Ethernet RX+	Ethernet TX+
2	Ethernet TX-	Ethernet TX-	Ethernet RX-	Ethernet TX-
3	Ethernet RX+	Ethernet RX+	Ethernet TX+	Ethernet RX+
4				
5				
6	Ethernet RX-	Ethernet RX-	Ethernet TX-	Ethernet RX-
7				
8				

Table 22: DB9 Console Interface

Pin#	Description
2	Console RX
3	Console TX
5	Console GND

Table 23: RJ45 to Console Cable

RJ45Pin#	Description	DB9 Pin#
4	Console GND	5
5	Console RX	2
6	Console TX	3

Table 24: RJ45 Straight Cable

RJ45Pin#	Description	RJ45 Pin#
1	Blue/White	1
2	Blue	2
3	Orange/White	3
6	Orange	6

Table 25: RJ45 Crossed Cable

RJ45Pin#	Description	RJ45 Pin#
1	Blue/White	3
2	Blue	6
3	Orange/White	1
6	Orange	2

Appendix B

Additional Licenses and Copyrights

Embedded Third-Party Software. A part of the software used within the MultiCom Firewalls can be freely distributed under the terms of the GNU Public License and BSD copyright. However, some applications remain the property of their owners, and require their permission to redistribute. For a complete listing of the software used within the MultiCom Firewalls, and the terms under which it can be distributed, refer to the LIGHTNING Web site at http://www.lightning.ch/ and http://www.lightning.ch/opensource.

Licensing

Apache License

Apache License

The MultiCom Firewalls include software developed by the Apache Group for use in the Apache HTTP server project (http://www.apache.org/).

BSD Copyright

BSD Copyright:

This product includes software developed by the University of California, Berkeley and its contributors:

Copyright (c) 1980-1998 Regents of the University of California. All rights reserved.

/*

* Copyright (c) 1980-1998 Regents of the University of California.

* All rights reserved.

*

* Redistribution and use in source and binary forms, with or without

* modification, are permitted provided that the following conditions

* are met:

* 1. Redistributions of source code must retain the above copyright

* notice, this list of conditions and the following disclaimer.

* 2. Redistributions in binary form must reproduce the above copyright

* notice, this list of conditions and the following disclaimer in the

* documentation and/or other materials provided with the distribution.

* 3. All advertising materials mentioning features or use of this software

* must dInternet Providerlay the following acknowledgement:

* This product includes software developed by the University of

* California, Berkeley and its contributors.

* 4. Neither the name of the University nor the names of its contributors

* may be used to endorse or promote products derived from this software

* without specific prior written permission.

*

* THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS" AND

* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE

* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE

* ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE

* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL

* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS

* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)

* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT

* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY

* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF

* SUCH DAMAGE.

*/

GNU General Public License

GNU General Public License

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and

modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively

when run, you must cause it, when started running for such
interactive use in the most ordinary way, to print or dInternet Providerlay an
announcement including an appropriate copyright notice and a
notice that there is no warranty (or else, saying that you provide
a warranty) and that users may redistribute the program under
these conditions, and telling the user how to view a copy of this
License. (Exception: if the Program itself is interactive but
does not normally print such an announcement, your work based on
the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If
identifiable sections of that work are not derived from the Program,
and can be reasonably considered independent and separate works in
themselves, then this License, and its terms, do not apply to those
sections when you distribute them as separate works. But when you
distribute the same sections as part of a whole which is a work based
on the Program, the distribution of the whole must be on the terms of
this License, whose permissions for other licensees extend to the
entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest
your rights to work written entirely by you; rather, the intent is to
exercise the right to control the distribution of derivative or
collective works based on the Program.

In addition, mere aggregation of another work not based on the Program
with the Program (or with a work based on the Program) on a volume of
a storage or distribution medium does not bring the other work under
the scope of this License.

3. You may copy and distribute the Program (or a work based on it,
under Section 2) in object code or executable form under the terms of
Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable
source code, which must be distributed under the terms of Sections
1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three
years, to give any third party, for a charge no more than your
cost of physically performing source distribution, a complete
machine-readable copy of the corresponding source code, to be
distributed under the terms of Sections 1 and 2 above on a medium
customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer
to distribute corresponding source code. (This alternative is

allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent

infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions

either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

OpenSSL License

OpenSSL License

```
/* ====================================================================
 * Copyright (c) 1998-2000 The OpenSSL Project.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
```

```
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must dInternet Providerlay the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com).  This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*

*/
```

Original SSLeay License

Original SSLeay License

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to. The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code. The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 *   notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *   notice, this list of conditions and the following disclaimer in the
 *   documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 *   must dInternet Providerlay the following acknowledgement:
 *   "This product includes cryptographic software written by
 *   Eric Young (eay@cryptsoft.com)"
 *   The word 'cryptographic' can be left out if the rouines from the library
 *   being used are not cryptographic related :-).
 * 4. If you include any Windows specific code (or a derivative thereof) from
 *   the apps directory (application code) you must include an acknowledgement:
 *   "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
 *
 * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE

```
* ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed.  i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]

*/
```

TCPD License

TCPD LICENSE

```
/*
 * Copyright (c) 1998 Kazunori Fujiwara <fujiwara@rcac.tdi.co.jp>
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 *    must dInternet Providerlay the following acknowledgement:
 *      This product includes software developed by Kazunori Fujiwara,
 *      Polish Linux Distribution Team and its contributors.
 * 4. Neither the name of the author nor the names of its contributors
 *    may be used to endorse or promote products derived from this software
 *    without specific prior written permission.
 *
 * THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
```

```
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.

 */
```

Login License

LOGIN LICENSE

```
/*
 * Copyright 1989 - 1994, Julianne Frances Haugh
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. Neither the name of Julianne F. Haugh nor the names of its contributors
 *    may be used to endorse or promote products derived from this software
 *    without specific prior written permission.
 *
 * THIS SOFTWARE IS PROVIDED BY JULIE HAUGH AND CONTRIBUTORS ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL JULIE HAUGH OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.

 */
```

Cryptix General License

Cryptix General License

Copyright (c) 1995, 1996, 1997, 1998, 1999, 2000 The Cryptix Foundation

Limited. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE CRYPTIX FOUNDATION LIMITED AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE CRYPTIX FOUNDATION LIMITED OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

PureTls License

This package is a SSLv3/TLS implementation written by Eric Rescorla <ekr\@rtfm.com> and licensed by Claymore Systems, Inc.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

This product includes software developed by Claymore Systems, Inc.

4. Neither the name of Claymore Systems, Inc. nor the name of Eric Rescorla may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyrights

BSD Copyright

BSD Copyright:

This product includes software developed by the University of California, Berkeley and its contributors:
Copyright (c) 1980-1998 Regents of the University of California. All rights reserved.

```
/*
 * Copyright (c) 1980-1998 Regents of the University of California.
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 *    must dInternet Providerlay the following acknowledgement:
 *     This product includes software developed by the University of
 *     California, Berkeley and its contributors.
```

```
* 4. Neither the name of the University nor the names of its contributors
*    may be used to endorse or promote products derived from this software
*    without specific prior written permission.
*
* THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED.  IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.

*/
```

Glossary

This is the glossary of terms relating to the usage of your MultiCom Firewall. Other terms relating to Internet Security can be found in RFC2828.

100Base-T

A networking standard (IEEE 802.3u) that allows for data transfer rates of up to 100 megabits per second between 2 or more devices. It is also referred to as Fast Ethernet. This standard frequently uses the same cable connectors (RJ45) as does its slower counterpart 10Base-T.

10Base-T

A networking standard that allows for data transfer rates of up to 10 megabits per second between 2 or more devices. It is also referred to as twisted pair ethernet because it uses twisted pairs of cable. The standard cable for the 10Base-T standard uses an RJ45 connector.

Action

The activity to occur when a specified data packet matches a filtering table entry. When configuring filtering you describe a type of data packet to watch for and then the “action” that is to occur to it when found.

The actions available are

drop	discarding the data packet as if it had never received it
accept	allow the data packet to pass
reject	like drop but sending out an ICMP message to the source that the data arrived but was rejected
forward	redirects a data packet to a local port
log	make a syslog report on the detection of the data packet
return	return to a previous set of rules (only available from the filter user library).

AH

Authentication Header can be part of an IP packet header that can ensure the integrity of the data and the IP header itself. It does not encrypt the data however.

See RFC2402.

ARP

The Address Resolution Protocol is used by TCP/IP to convert an IP address into a DLC or MAC address of a network interface. Whenever network traffic is made the first step is for the computer to make an ARP request to find the correct network interface to send the packet to.

See RFC826.

ARP Proxy

The Proxy of the Address Resolution Protocol is used by a network interface to pretend that it is in fact one or more different interfaces. After responding to an ARP request for the IP address that is being proxied, the remote device will send the IP packet to the ARP Proxy for further processing. This process can allow multiple IP addresses to receive traffic as if they were directly connected to the Internet when in fact they are hidden behind a network firewall.

Authentication

The process of identifying oneself over a network. This is commonly done by entering a user name and secret password to receive access to a network or networked device. A very common form of authentication is when you identify yourself to your Internet Service Provider to have access to the Internet.

Bandwidth

Describes how much data you can reach per second. An analogy could be the width of a pipe and how much water can come through per second. There are many factors that affect this speed so if you are unsure what speed you should be able to reach the Internet you should check with your Internet Service Provider.

Bridge

A device that connects to networks at a low level of connectivity. They will not modify, analyze or route packets that move over them. Many xDSL, Cable or wireless modems will be configured to act as a bridge allowing the Internet Service Provider to directly assign addresses to the customers computers.

Broadcast

When the same message or data packet is sent to a group of machines. This information may have many purposes such as simply announcing that a new device is on the network, saying that a device is still connected to the network, to providing a way for the backup power supply to send a message to everyone that it will be turning itself off due to a power outage.

The number of machines that a broadcast reaches depends on the type of the broadcast — network broadcast (where subnet and host parts of an IP address are set to 255 as in 128.190.255.255), subnet broadcast (where only the host part of the IP address is set to 255 as in 128.190.1.255, or a cable broadcast where all hosts on the local physical network are targeted to receive a message with the IP address of 255.255.255.255.

Burst

An optional filtering identifier that works in tandem with the “limit” parameter. Burst specifies the maximum burst of data packets allowed in the traffic flow before the associated limit parameter takes affect. The value is X where X equals the number of packets to match the associated rule before the limiting takes effect. By default this number is 5.

It is an extra identifier to help account for irregular network traffic (network overloads or faulty equipment) that might otherwise get blocked by the limit command.

Cable

The enclosure that holds your network wiring which has connectors such as RJ45 on both sides. The use of the cable can change depending on the layout of the wires at the end points. For example a straight through cable has the same wires

in the same connector locations at both ends of the cable. A crossed wire cable however has, as its name suggests, a pair of crossed wires ending in a different order at one end than on the other end.

Be sure you are using the right cable for your desired connection.

Cable Modems

These modems connect you to high speed Internet-access using cable TV lines. Since you are connecting to your TV line you will use coaxial cables between the modem and your cable TV interface. The modem should have an ethernet interface on it to communicate with your internal network. Speeds are possible up to 2 Mbps depending on your service provider.

CATV

The high speed Internet-access technology uses cable TV lines to connect the user's home to the Internet.

Client

Part of a client-server architecture. The client is the software which presents information to the user and often allows for interaction with that data as well. This information is retrieved from a server which will actually do the work of preparing the information for the client.

An example of this is an email program where the program on your computer is the client and the computer that you connect to (to retrieve your email) is the server.

Compression

The action of transforming data into files of smaller sizes. While in a small size the data can be transmitted faster over network media and then uncompressed on the other side.

Connection State

A TCP identifier found in the header of a TCP data packet. Below are the 4 IP packet states that filtering rules can be set to watch for.

New - A packet which creates a new connection.

Established - A packet which belongs to an existing connection (i.e. which is a reply to an accepted request, or an outgoing packet on a connection which has seen replies.)

Related - A packet which is related to, but NOT part of, an existing connection, such as an ICMP error or some ftp data connections.

Invalid - A packet which could not be identified for some reason such as running out of memory, ICMP errors which do not correspond to known connections.

Crossed Cable

An RJ45 ethernet cable that allows you to connect to network devices together without needing a hub in between them. For instance you might use this cable if you chose to connect your router directly to your computer or laptop. MultiCom crossed cables are blue or have a blue tape around them.

This cable is useful when you need to do direct testing and configurations of a network device and do not have a hub nearby.

Denial of Service

Also known as DoS, is a type of network attack where the attacker floods a known firewall or server with packets, thereby degrading network performance and possibly crashing the software that is receiving those packets.

Destination

The IP address of the firewall or host to which the data packet should be sent.

DHCP

Dynamic Host Configuration Protocol simplifies network administration by assigning IP addresses and other configurations from a central DHCP server. This information is given out to DHCP Clients that request it, usually for a preset period of time before a new request must be made.

See RFC1531

DHCP Client

A computer or device configured to receive its IP address, subnet mask, broadcast address, firewall address, domain name and DNS servers necessary to operate on the network. The client also receives a lease time after which it must ask the DHCP server if it can still have this information or if there is a new configuration that should be used instead.

DHCP Server

A computer configured with IP addresses to manage as well as other data necessary for a networked device to operate on the network. It responds to requests by DHCP clients who ask for this information. Many networks use this as a convenient way to manage many computers from one place.

DNS

Domain Name Servers are the phone books of the Internet. Just as people have trouble memorizing everyone's phone number they wish to call the same problem exists with the Internet. Having the DNS numbers of your Internet Service Provider allows you to move about the Internet with names like www.lightning.ch instead of 206.201.2.233. This number will take the form of x.x.x.x where x's are numbers between 0 and 255.

See RFC1035.

Domain

A virtual group of computers and devices that share a common administrative purpose. For instance, the domain mynetwork.com will cover everyone's computer in the “mynetwork” company. These computers may be in the same LAN or be located around the world in different offices.

Aside from administratively keeping a group of computers together, using a domain tells your router that there is network that can be reached internally, and that it may not need to connect to the Internet to reach a computer or web address ending in that name.

Download

To copy data (such as a file) from a remote source to a local destination. Usually referred to as the action of the recipient when taking the data. When you copy a file from the Internet to your computer you are downloading the data to your computer.

Duplex

Duplex identifies the possibility that the Ethernet interface can both send and receive data. Full-duplex means the interface can both send and receive at the same time while half-duplex means that the data can only go in one direction at a time.

EPROM

See Flash Memory

ESP

Encapsulated Security Payload is an IP packet that is transporting encrypted data. This is the type of Packet that the MultiCom Firewalls use to transfer IPSec protected data.

See RFC2406

Ethernet

A networking specification that identifies how the data is to travel. This term is sometimes used interchangeably with “LAN” to identify the local network.

Filter

The process of matching IP packet header information of incoming packets to a list of rules and corresponding actions. Either a matching entry is found and the specified action implemented or the packet is rejected because it did not match any of the table entries.

This table is stored on the router and the IP packets are checked by going sequentially down the table entries. When two entries identify the same type of packet (for instance, having two entries for all web data) the first one found in the table will be used.

Filter Forward

The filtering table used to list rules affecting IP packets that pass through the firewall from one network to another.

Filter Input

The filtering table used to list rules affecting IP packets that only arrive at one of the firewall’s interfaces and is not meant to be passed any further. For example accessing the built in webserver or a ping to the firewall itself.

Filter Forward

The filtering table used to list rules affecting IP packets that originate from the firewall. For example responses to pings of the firewall’s interfaces and responses to remote configuration requests by telnet or the webserver.

Filter User

The filtering table used to group lists of rules that are only used when packets are sent to the s.

Firewall

A hardware device or software program used to prevent unauthorized access to your computer or network. These walls are usually used at points where the network is vulnerable to the general public or hacker attempts to gain access. These firewalls examine all data packets that pass through it and search them for characteristics that match pre-defined access rules.

There is a built-in firewall capability in the MultiCom Firewall. When it is enabled all incoming data is denied unless there is a mapping rule in the NAT table for the interface it is active on. For instance, if the Firewall was enabled for the WAN interface, no data would be allowed through it unless it matched a rule in the NAT table for that interface.)

Typically this capability is enabled along with a single rule in the WAN outgoing interface that masquerades all data as if it had originated from the WAN port itself. What this does is limit communication to only be allowed in response to a request from the internal LAN.

Firmware

The basic software and data that is written to the read-only memory (ROM) of your router. This data is written to the Flash memory which is protected from power outages and reboots of the device. If your firewall has damaged firmware it will not know how to manage any activity.

Higher version numbers often contain additional functionality. Please check the Lightning Instrumentation website at http://www.lightning.ch/support for information on the most recent version available.

Flag

A TCP identifier found in the header of a TCP data packet.

Common types include.

URG	Urgent Pointer field significant
ACK	Acknowledgment field significant
PSH	Push Function, indicating that this segment contains data that must be pushed through to the receiving user
RST	Reset the connection
SYN	Synchronize sequence numbers (packets used to request a TCP connection)
FIN	No more data from sender announcement

Flash Memory

This is a type of memory that has similarities to both RAM and ROM. Its similarity to RAM is that it can be modified on-line. It acts like ROM in respect that it retains its contents even if the MultiCom is turned off.

In your MultiCom, it is used to store both the firmware and the configuration. Unlike a ROM memory, it is possible to install a new release of the firmware and store it in the Flash memory of your MultiCom.

Fragment

When a data is too large to fit into one packet it can be divided into multiple packets (also fragments). Typically the header information such as source port, destination port, ICMP type is only stored in the start of the packet (i.e. the first packet).

This is a problem since a rule filtering a source port (for instance port 80) will always fail when a fragment data packet is inspected because the source port was not in the header (except for the first data packet which had all of the required information.)

Freeware

This is software that is given away free by the author. The author still retains the copyright however so you cannot resell or alter the software without first obtaining permission from the author.

FTP

File Transfer Protocol creates a virtual connection over TCP/IP which allows file sharing. For example an FTP client (your computer) asks an FTP server (a remote computer with files you want) for permission to transfer files. You will often need a login ID and password to access the FTP server though many servers have a guest account under the login ID “anonymous” and password of the users email address.

See RFC959.

Firewall

The networking hardware device that links two different networks. Usually this device (such as a router) will be identified with an IP address. To reach the other network your computer must know the IP address of the firewall so it can send the information through it to the remote network.

G.DMT

Discrete Multitone Technology is a DSL line modulation standard. Sometimes referred to as “full rate” ADSL.

G.Lite

Also referred to as “DSL Lite”, “Universal DSL”, or “splitterless ADSL”, is a SDSL Line Modulation Standard. It requires no filters or splitters and supports speeds up to 1.5 Mbps download and 512Kbps upload.

Hacker

While a hacker means an amateur programmer it increasingly is recognized as meaning a person trying to get unauthorized access to your computer or network with the purpose of causing damage, stealing or manipulating information.

Host Name

A name that is used to identify and IP address in a way more user-friendly than a set of numbers alone. While host names are easier to remember they rely upon some method to translate the name into an IP address (such as using DNS.) Because of this it may be easier to use just the IP address when troubleshooting connectivity problems.

Hub

A physical device that contains multiple ethernet ports which allows devices on different network segments (or cables) to communicate. Data packets that reach the hub are copied to all of the other ports it is connected to.

Please note that not all hubs can communicate at the same speed. Some hubs work only at 10Base-T speeds or 100Base-T speeds while some can support mixed speeds together. Be sure the hub matches your needs and existing hardware.

ICMP

Internet Control Message Protocol messages are typically messages relating to network errors, congestion, timeouts of data packets and echoes (used by the ping command) by a device on the network. These messages are sent in the IP header and are often sent by a firewall on the path the data packet was traveling.

See RFC792, and RFC1256 for more information on router advertisement and solicitation.

IKE

Internet Key Exchange (formerly called the ISAKMP/Oakley key exchange) negotiates the parameters needed to build a secured connection with IPSec. This occurs using TCP or UDP port 500. After a successful key exchange encrypted data can travel between the two points.

See RFC2407, RFC2408, RFC2409.

Interface

This is the physical port on the back of your ethernet device. There are many possible interfaces depending on your model of MultiCom Firewall, the LAN (also known as the local area network), the WAN (also known as wide area

network), the DMZ (demilitarized zone). It is through these physical connections that the Internet device is connected to your network and/ or your xDSL, cable or wireless modem.

Internet

The global, decentralized network connecting computers. Many of these computers are connected 24 hours a day to provide services such as web sites, retail stores, databases of information, email services and more. Individuals can access the Internet through an Internet Service Provider (Internet Service Provider).

Internet Service Provider

Internet Service Providers are the companies that manage your Internet connection. Frequently they will have a local phone number for you to call with your modem which will give you access to the whole Internet, email and other services they may offer.

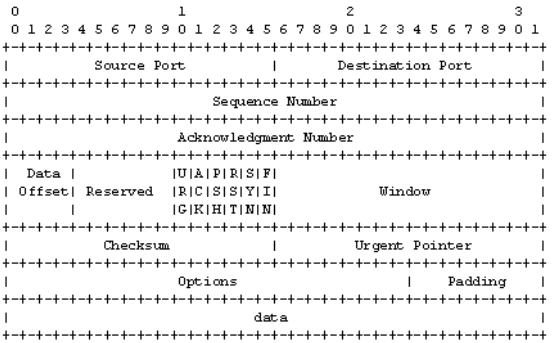
IP Address

A 32–bit number broken up into 4 octets and used to identify a computer on a TCP/IP network. This address takes the form of x.x.x.x where each x is an octet (a number from 0–255). It is these addresses that identifies computers and web sites on the Internet as well.

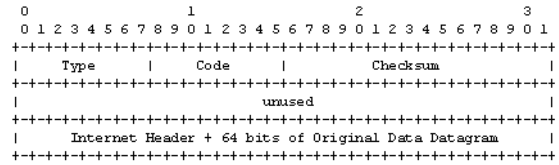
IP Header

The section of a data packet that is reserved for identifying information. Such information could be the source IP address, the destination IP address, and other information describing the type of data that the data packet carries. For examples of different headers please see below.

TCP Header



ICMP Header



IP Protocol

A format that specifies how data is transmitted between two or more devices or software. It is important to have devices using the same protocol such as assuring that your network printer and network computer both use TCP/IP.

Some common protocols are TCP, UDP and ICMP.

See RFC791 and RFC2411

IPSec

IPSec is a suite protocols designed by the Internet Engineering Task Force (IETF) to protect IP communication. Working on the network level, IPSec provides authentication, encryption, and integrity services for data packets and streams. This can be done either between 2 machines (transport mode) or 2 networks (tunnel mode)

IPSec can use three protocols to provide these services: Authentication Header (AH), Encapsulating Security Payload (ESP), Internet Key Exchange (IKE).

See RFC2401.

Kernel

This is the kernel or operating system corresponding to the release of the Linux Operating System. Lightning-Linux is the operating system that runs the MultiCom Firewall. Because it is a customized version of Linux, each version of Lightning Linux will have its corresponding Linux kernel that was integrated into the current version. This is visible in the first screen of the Monitor software.

LAN

Local Area Network is the interconnection of computers and network devices in a relatively small group. This group can be the computers in your home or the computers in your office building as compared to a remote network (WAN) that you may connect to through the phone company or satellite uplinks. LAN are typically differentiated by the media/ cabling connecting the devices, the protocols being run over the media and the layout or topology of the media.

Lease

The amount of time that a DHCP client can keep the configuration information that it was given by a DHCP server. When this time has expired the DHCP client must again ask for configuration information.

Limit

A definition to specify the maximum average number of matches to allow during the defined time frame. This parameter can take the form of X/s, X/m, X/h, or X/d where X is the number of packets and s=seconds, m=minute, h=hour, and d=hour. Traffic less than the limit activates the corresponding action. Traffic flow greater than this rate causes the corresponding filtering action to be skipped for all exceeding data packets UNLESS you specify burst sizes.

This is a filtering option where other types of tags can be used to identify types of data along with a limited throughput and actions such as dropping or rejecting can be specified.

LLC

Logical Link Control is one of 2 different methods for encapsulating data over a DSL connection. Sometimes it is also known as LLC/SNAP (Logical Link Control/ Sub-Network Access Protocol.) The other method is VC-Mux.

Login

A part of authenticating so that the computer or network will know who you are. This is often used with a secret password to identify users correctly.

MAC Address

Media Access Control addresses are unique addresses assigned to each ethernet interface such as found on an ethernet card in a networked computer. It is made up of 12 hexadecimal digits in the form such as 12:34:56:78:9A:BC, 123456789ABC, or 123456–789ABC. The first 6 digits is the identifying code of the manufacturer of the device.

Metric

The number of routers between one IP address and another. This field allows you to keep track of and manage routes according to the distance between any two computers. Note: this is a manually entered field and will not be computed for you.

MIB

Management Information Base is a database in the shape of a tree of objects. Each object is in fact a parameter which has specific settings or grouping of other subheadings. For instance under an object heading of ethernet interface may be information for the IP address of that interface, the netmask, or if DHCP is on or off.

The MIB in your router is where you will be making changes to the way your router works. You can enter your changes with the Configurator software or with line commands via a telnet connection directly to your router.

Modem

The acronym fro modulator-demodulator device that converts digital data from your computer to analog data that can be transmitted over your telephone line. This analog data is in turn converted back into digital data at the other end of the phone line.

MTU

The maximum transmission unit (MTU) is the largest size packet (or frame) that can be sent through a connected network. Ethernet networks can use up to 1500 MTU while interfaces configured to use PPPoE can have a maximum MTU of 1492.

NAT

Network Address Translation is done on a device resting between 2 or more networks (for instance between the WAN and the LAN). IP packets arriving or leaving can have their source or destination changed to a different IP address.

For example, incoming NAT allows you to store a publicly registered IP addresses at the router and link it (or them) to other IP addresses in the LAN. Outgoing NAT changes the source address of packets leaving the device (from the LAN to the Internet) so that the responses to the packets can find there way back. This allows more than one computer to share a single IP address on the Internet.

The added benefit of NAT is that it keeps a list of who asked for what information to the Internet and when data is trying to enter your own network it is compared against the list to be sure that someone has asked for it. If no one has the data is rejected and a report is sent to the Syslog server.

See RFC1631

NetBIOS

Network Basic Input Output System is a set of basic network functions that can be used on a LAN. Most frequently these ports are used by computers running Microsoft Windows software.

The data is used to identify names of shared objects and other computers but due to their frequency this data traffic may inadvertently open dial up connections. In this case it may be useful to disable the spreading of this data past the MultiCom Firewall.

Netmask

Also known as subnet mask, is a 32–bit number that separates the network and host portions of an IP address. The form looks like an appendage to a device's IP address such as 1.2.3.4/24 (meaning a 24–bit sized netmask for device 1.2.3.4) or as an IP address x.x.x.x such as 255.255.255.0 (also a 24–bit sized netmask). It is frequently used to divide a larger network into smaller, virtual networks.

Network

A group of computers connected together to share data. This group can be the computers in your home or the computers in your office building as compared to a remote network (WAN) that you may connect to through the phone company or satellite uplinks.

Networks are typically differentiated by the media/ cabling connecting the devices, the protocols being run over the media and the layout or topology of the media.

Octet

An 8-bit number. This number is often in binary as 00001111 or decimal 15. The range of numbers an octet can be is from 00000000–11111111 in binary or 0 – 255 in decimal form.

Packet

Also known as a datagram or frame is the envelope that data travels within over your network. Each of these envelopes can have different identifying information on them such as the source IP address, the destination IP address, error checking information, sequence numbers and more. Additionally packets can be of different sizes as well. Data that is too large to be fit into one packet of data will be broken down into a series of packets before being sent across the network.

PAT

Port Address Translation allows you to redirect internal or external data traveling via ports to specific locations. For instance you want everyone using Internet newsgroups (port 113) to be redirected to your internal news-server. All external web requests (typically on port 80) could also be directed to your web server inside your company. This redirection can also be to different ports. To redirect IP addresses you would use NAT.

See the technology overview section on PAT for a more detailed explanation on what it can do for you.

Ping

The Packet Internet Groper is a software utility used to verify if a remote device is accessible over a network. After the remote device is identified by either its IP address or its domain name the program or utility will send a small data packet to that device and wait to hear a reply. This reply uses the ICMP Echo function and will also usually include a time stamp identifying how long the packet exchange took.

Port

While people are getting more familiar with the IP addresses used on the Internet few people realize that for each different address there are over 65,000 channels over which the data can travel. Fortunately most communication takes place over preset channels (such as channel 80 for reaching for a web page.)

Some software makes use of random channels so if you want to filter data by the port address it is important that you know which ports are being used by which software on your network.

Port Scan

A network attack where the attacker tries to gain information about software running on servers or workstations. The attacker attempts to make access with every available TCP port on a computer and by analyzing the result the attacker can then focus their attack on the specific software.

PPP

The Point-to-Point Protocol provides a standard method for transporting IP data packets over point-to-point links (such as a link from a home computer to the Internet via an Internet Service Provider). This simple link between two network devices allows data packet transport between the two devices in full-duplex simultaneous bidirectional operation.

See RFC1661.

PPPoE

The Point-to-Point Protocol over Ethernet (PPPoE) encapsulates IP data packets over point-to-point links (such as a link from a home computer to the Internet via an Internet Service Provider). This link is authenticated with a username and password and then PPP communication can take place between two network devices (your router and your Internet Service Provider firewall).

See RFC2516.

PPTP

The Point-to-Point Tunneling protocol uses a version of GRE (Generic Routing Encapsulation) to transport PPP packets. A username, password and IP address of the PPTP server is required to receive IP address parameters. This is frequently used by Microsoft Windows as a way of creating Virtual Private Networks. See the chapter on PPP in the reference manual for more information.

Proxy DNS

A device which pretends to be a DNS server but actually forwards all DNS requests to a remote server is called a Proxy DNS. For instance, clients on a local network will make DNS requests to a Proxy DNS device which in turn forwards those requests to the appropriate external DNS server. Frequently there is a cache that keeps a list of frequently requested names so that the responses from the local network can be replied to quickly.

Reboot

Rebooting is when your router is powered off and then turned back on again. This happens either when your remove the power connection to the device or your local power supply is interrupted (a blackout for example.) After reboot the device will check to be sure all of the hardware is working correctly and then load in the “Boot Config”. Any changes that were made to the “Current Config” will have been erased after the reboot.

RFC

Request For Comments are documents that define standards on the Internet. They are a good resource when you need detailed information on a particular aspect of your network. Fortunately there are many databases of these documents such as at http://www.normos.org, http://www.faqs.org/rfcs/, http://www.cis.ohio-state.edu/hypertext/information/rfc.html, http://www.freesoft.org/CIE/RFC/

RIP

The Routing Information Protocol (RIP) allows groups of firewalls to dynamically update their routing tables according to the state of the firewalls or routers they interact with. By dynamically updating available routes a network can compensate when one router fails by sending data through another route. More information on this protocol is described in the chapter on Routing in the Reference manual.

RJ45

Registered Jack 45 is a commonly used eight-wire connector or cable that connects computers, routers, printers onto a ethernet based LAN.

Router

A device that connects networks and directs the traffic of data packets across them. The router uses the IP address of a data packet to decide where it should go (whether to send it out towards a remote network or to leave the data packet on the local side.) Because the router limits what data can leave the network it reduces unnecessary traffic over networks.

By keeping a table of IP addresses and the remote location that they should be forwarded to, the router is able to distribute data in the most efficient manner. The routing table can either be maintained statically (where the routes are manually entered) or dynamically (when routing devices pass information automatically between themselves.)

Shareware

Software that is freely distributable to friends or colleagues but which the author asks a small fee (also called registering the software) if you decide to regularly use the program. In some cases additional features are available when you register the program. Some shareware have built in time limits after which you must register or the program will not operate.

Shell

Or console is the text based window giving you direct access to your router. This window is accessible when using a telnet client to reach the telnet server built into the router. From this window you can enter commands that change your the configuration of your router or that return data on the status or history of activity within your router.

Source

The IP address of the firewall or host that composes the data packet.

Spoofing

A network attack when the attacker tries to send packets into a network by changing the source IP address to be that of a known network. Often this is done by saying the packet is from the LAN network but it arrives on the WAN and asks for permission to get in. A properly configured firewall will protect against this sort of access.

Spyware

A piece of software or Internet browser plug-in that makes unrequested contacts to the Internet to share information. For example, software that contacts the manufacturers web site each time the program is used, possibly even sending data about the computer it is running on. Although this is not necessarily a network attack it is a program that communicates to other programs without the user being aware of it. Possibly sensitive data could be communicated remotely as well.

Straight Cable

An RJ45 ethernet cable that connects network devices together through a hub. This will not allow you to connect network devices directly to each other, for that situation you would use a crossed wire cable.

Subnet

Dividing an TCP/IP network into smaller, equally sized logical networks. By using what used to be the host part of an IP address a network can seem to be many smaller networks lessening network traffic caused by broadcasts for instance.

See RFC950

Syslog Message

These messages are generated by the MultiCom Firewall for the following reasons: system events, custom filtering rules, DHCP trace activity, PPP trace activity. For more information see the chapter on Syslog messages in the Reference Manual.

Syslog Server

A software that collects and stores system events (syslog) messages. Syslog messages are sent to this server and stored for later reviewing. Some Syslog servers provide additional utilities such as sending pages or emails to administrators.

System Administrator

Or network manager is the individual or group of people responsible for supporting your office or company network. They maintain security, configurations, and upgrades for your computers so the network works for everyone. Sometimes certain functions of If you do not know certain configurations for your network they will probably know the answer. In some firms making changes to your computer or connecting devices to it first requires the permission of the System Administrator.

T1.413

An ANSI industry standard for full-rate DSL Line Modulation.

TCP

The Transmission Control Protocol actually establishes a connection between two hosts as though they were directly connected. By checking for errors and keeping track of which order the data packets should be in TCP provides for reliable data transmissions and interactions. If a data packet is lost or damaged during transit it is TCP that asks for that data packet to be retransmitted.

See RFC793.

TCP Option

A very technical variable in the TCP header. Filtering for these markers should be for advanced users only. RFC1323 describes the last two options in more detail.

Common types include:

end of list	when the end of the options would not otherwise coincide with the end of the TCP header
no operation	may be used between options, for example, to align the beginning of a subsequent option on a word boundary
maximum segment size	communicates the maximum receive segment size at the TCP which sends this segment
window scale factor	an option that allows the TCP packets to identify data windows larger than 65K bytes
timestamp	an option that allows time stamping from a virtual clock to allow accurate measurements of round-trip time between sending a segment and receiving an acknowledgement for it

TCP/IP

Transmission Control Protocol/ Internet Protocol is actually two separate protocols used to transmit data over a network. The Internet Protocol is used to move data packets (also known as datagrams) around the network or Internet but in a one way method.

The Transmission Control Protocol actually establishes a connection between two hosts as though they were directly connected. By checking for errors and keeping track of which order the data packets should be in TCP provides for reliable data transmissions and interactions. If a data packet is lost or damaged during transit it is TCP that asks for that data packet to be retransmitted.

See RFC793.

Telnet

Is a program that runs on your computer and allows you to connect to a telnet server on your network in a text based window. You will often need a login ID and password to access the telnet server but once you are logged in you can use commands as though you were typing them directly into the telnet server (even if the server or device is around the world, though that may make communication a little slower.)

Your router contains a telnet server to allow you remote control access to run commands or get reports. The telnet program is sometimes referred to as a terminal emulator.

See RFC854.

Threshold

Setting a level of throughput or activity is called setting the threshold. This number identifies a frequency or size of data that, when exceeded, cause an action to occur.

Trigger

The activity that causes an action to occur. By setting filtering rules and their corresponding actions you are setting a trigger. When the specified data packet is found by the router the action is triggered.

Trojan horse

A type of network attack that relies on a software program getting inside of the secured network, for example as an email attachment. This program can either open communication to a remote host or allow incoming communication by acting as a server itself, listening on a relatively unknown tcp or udp port.

UDP

User Datagram Protocol is similar to TCP/IP but unlike TCP it does not provide error recovery methods if the message was not received correctly. Because it is essentially a one way method of sending data it is primarily used to broadcast messages over a network.

See RFC768.

Uplink Port

Many hubs will have one uplink port where you can attach a cable to another hub to share interfaces. If this is the only port available on your hub you can indeed use it but you will need to connect a crossed cable to use it.

Upload

To copy data (such as a file) from a local source to a remote destination. Usually referred to as the action of the recipient when putting or sending data to another device or computer. When you copy a configuration file from your computer to your router you are uploading the data to your router.

URL

The Uniform Resource Locator is the global format to access documents and resources on the Internet. A URL uses three parts to reach a specified resource or file. The first part of the address describes the protocol to be used (such as http or ftp), the second part identifies the IP address or domain name of where the desired resource is located (www.mycompany.com). Finally the name of the resource or file is added. A complete url to reach a web page may look like this http://www.mycompany.com/storefront.html.

Users

User accounts on the MultiCom Firewall allows up to 10 different users to be configured with usernames, passwords and administrative privileges. These Users will be allowed access to the MultiCom Firewall for configuration and data access purposes (from http, https, telnet, ssh, and ftp.) These accounts are not related to PPPoE or PPTP accounts.

VC

Virtual Circuit Multiplexing is one of 2 different methods for encapsulating data over a DSL connection. The other method is LLC.

WAN

Wide Area Network is the interconnection of LAN's over phone lines, satellite links or other communication services. The WAN of a global company encompasses all of their LANs but more specifically the devices that connect them such as routers and switches as compared to a LAN which focuses on the network right up to the workstation. The largest WAN is the Internet.

Web Server

A computer or device that serves web pages. The web server is typically reached through a browser by either its IP address (http://10.0.0.1 is the default address of your routers web server) or domain name such as http://www.somecomputer.com. The pages of the web server may be read only or interactive.

xDSL

Digital Subscriber Lines such as ADSL, SDSL, HDSL are collectively referred to as xDSL. It is a high-speed networking technology allowing connection to the Internet from your home or office. Data rates for downloading information will be from 1.5 to 9 Mbps and uploading information from 16 to 640 Kbps depending on your service provider.

xDSL Modem

These modems are required to connect you to high speed Internet-access using Digital Subscriber lines. Since you are connecting through your phone line you will probably use a phone cable between the modem and your telephone wall interface. The modem should have an ethernet interface on it to communicate with your internal network. Data rates for downloading information will be from 1.5 to 9 Mbps and uploading information from 16 to 640 Kbps depending on your service provider.

Index

M

O

P

R

S

T

U

W