WebRamp 700s User's Guide

For Windows and Macintosh

Technical Support

Technical support is available by mail, fax, e-mail, or phone, during the hours 6 AM to 5 PM, Pacific Standard Time (U.S.). Before you contact Technical Support, please check the *WebRamp 700s User's Guide* for more information.

Mail: Technical Support, Ramp Networks, 3100 De La Cruz Boulevard,
Santa Clara, CA 95054, U.S.A.

Fax: 1(408)988-6363, attention Technical Support

E-mail: support@rampnet.com

Phone: 1(408)988-5353

When you request support, be sure to include your WebRamp serial number, your name, company name, street address, e-mail address, and phone number.

Ramp Networks, Inc.
3100 De La Cruz Boulevard
Santa Clara, CA 95054
U.S.A.

Safety Precautions

- Read and follow all warnings and instructions included with this product.
- Do not block the ventilation openings on the WebRamp. Do not expose the WebRamp (even if unplugged) to an environment that exceeds temperature and humidity specifications.
- Do not place cords or cables where they may be walked on or tripped over.
- Be sure to comply with any applicable local safety standards or regulations.
- General-purpose cables are provided with this product. Any cables or other requirements mandated by local authority are your responsibility.
- Never touch telephone wires or terminals unless the line has been disconnected.
- Avoid using telephone equipment or installing the product during an electrical storm.
- Never install telephone jacks, lines, network cables, this product, or power connections in wet locations.

FCC Notice

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

Industry Canada Compliance Notice

This Class B digital apparatus, the WebRamp 700s, complies with Canadian ICES-003.

Cet appareil numérique de la classe B, WebRamp 700s, est conforme à la norme NMB-003 du Canada.

3100 De La Cruz Blvd.
Santa Clara, CA 95054
408•988•5353
Fax 408•988•6363

DECLARATION OF CONFORMITY WITH FCC RULES
FOR ELECTROMAGNETIC COMPATIBILITY

Ramp Networks, Inc.
3100 De La Cruz Boulevard
Santa Clara, CA 95054

Declare under our sole responsibility that the product:

WebRamp 700s

to which this declaration relates complies with Part 15 of the FCC Rules. Operation is subject to the following conditions: 1) this device may not cause harmful interference and 2) this device must accept any interference received, including interference that may cause undesired operation.

Elie Habib
Vice President, Engineering
Ramp Networks, Inc.
January 6, 2000

Ramp Networks Software License Agreement

PLEASE READ THIS LICENSE CAREFULLY BEFORE USING THE SOFTWARE. BY INSTALLING, COPYING, OR OTHERWISE USING THE COMPUTER SOFTWARE, ASSOCIATED MEDIA, PRINTED MATERIALS, AND ONLINE OR ELECTRONIC DOCUMENTATION ("SOFTWARE PRODUCT"), YOU AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE, YOU ARE NOT AUTHORIZED TO USE THE SOFTWARE PRODUCT.

This Ramp Networks License Agreement ("License") is a legal agreement between you (either an individual or a single entity) and Ramp Networks, Inc., for the SOFTWARE PRODUCT accompanying this License.

The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties.

License

The SOFTWARE PRODUCT is licensed, not sold, to you by Ramp Networks. You own the media on which the SOFTWARE PRODUCT is recorded, but Ramp Networks retains title to the SOFTWARE PRODUCT. This License allows you to install and use copies of the SOFTWARE PRODUCT on all computers located at your premises, and to make copies of the SOFTWARE PRODUCT for backup and archival purposes. You may also transfer all your license rights in the SOFTWARE PRODUCT, the backup copy of the SOFTWARE PRODUCT, 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. Ramp Networks reserves all rights not expressly granted to you.

Restrictions

The SOFTWARE PRODUCT contains copyrighted material, trade secrets, and other proprietary information and, in order to protect them, you may not decompile, reverse engineer, disassemble, or otherwise reduce the SOFTWARE PRODUCT to human-perceivable form, except and only to the extent that such activity is expressly permitted by applicable law, notwithstanding this limitation. You may not modify, rent, lease, loan, distribute, or create derivative works based upon the SOFTWARE PRODUCT in whole or in part.

The SOFTWARE PRODUCT is licensed as a single product. Its component parts may not be separated for use on more than one computer.

Support Services

Ramp Networks may provide you with support services related to the SOFTWARE PRODUCT ("Support Services"). Use of Support Services is governed by the Ramp Networks policies and programs described in the user manual, online documentation, and/or in other Ramp Networks-provided materials. Any supplemental software code provided to you as part of the Support Services shall be considered part of the SOFTWARE PRODUCT and subject to the terms and conditions of this License. With respect to technical information you provide to Ramp Networks as part of the Support Services, Ramp Networks may use such information for its business purposes, including for product support and development. Ramp Networks will not use such technical information in a form that personally identifies you.

Termination

This License is effective until terminated. You may terminate this License at any time by destroying the SOFTWARE PRODUCT, all of its component parts, and all copies thereof. If you fail to comply with the terms and conditions of this License, this License will terminate immediately without notice from Ramp Networks and without prejudice to any other rights.

Copyright

All title and copyrights in and to the SOFTWARE PRODUCT (including but not limited to any images, photographs, animations, video, audio, music, text, and "applets" incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT are owned by Ramp Networks. The SOFTWARE PRODUCT is protected by copyright laws and international treaty provisions. Therefore, you must treat the SOFTWARE PRODUCT like any other copyrighted material, except that you may install and use copies of the SOFTWARE PRODUCT on all computers located at your premises, and make copies of the SOFTWARE PRODUCT for backup and archival purposes.

Export Law Assurances

You agree and certify that the SOFTWARE PRODUCT will not be exported outside the United States, except as authorized and as permitted by the laws and regulations of the United States. If the SOFTWARE PRODUCT has been rightfully obtained by you outside of the United States, you agree that you will not reexport the SOFTWARE PRODUCT, the Materials, or any other technical data received from Ramp Networks, or the direct product thereof, except as permitted by the laws and regulations of the United States and the laws and regulations of the jurisdiction in which you obtained the SOFTWARE PRODUCT.

Disclaimer of Warranty on Software

You expressly acknowledge and agree that use of the SOFTWARE PRODUCT is at your own risk. The SOFTWARE PRODUCT is provided "AS IS" and without warranty of any kind, and Ramp Networks expressly disclaims any warranty, expressed or implied, including, but not limited to the implied warranties of merchantability and fitness for a particular purpose. Ramp Networks does not warrant that the functions contained in the SOFTWARE PRODUCT will meet your requirements, or that the operation of the software will be uninterrupted or error-free, or that defects in the software will be corrected. Furthermore, Ramp Networks does not warrant or make any representations regarding the use or the results of the use of the SOFTWARE PRODUCT or related documentation in terms of their correctness, accuracy, reliability, or otherwise. No oral or written information or advice given by Ramp Networks or a Ramp Networks authorized representative will create a warranty or in any way increase the scope of this warranty. The entire risk arising out of use or performance of the SOFTWARE PRODUCT remains with you.

Some states do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

Limitation of Liability

Under no circumstance, including negligence, will Ramp Networks be liable for any incidental, special, or consequential damages that result from the use or inability to use the SOFTWARE PRODUCT, even if Ramp Networks or a Ramp Networks authorized representative has been advised of the possibilities of such damages. Some states do not allow the limitation or exclusions of liability for incidental or consequential damages, so the above limitation or exclusion may not apply to you.

In no event shall Ramp Networks's total liability to you for all damages losses, and causes of action (whether in contract, tort [including negligence], or otherwise) exceed the amount paid by you for the Ramp Networks product.

Controlling Law and Severability

This License shall be governed by and construed in accordance with the laws of the United States and the State of California, as applied to agreements entered into and to be performed entirely within California between California residents. If for any reason a court of competent jurisdiction finds any provision of this License, or portion 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 the License shall continue in full force and effect.

Complete Agreement

This License constitutes the entire agreement between the parties with respect to the use of the SOFTWARE PRODUCT 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 this License will be binding unless in writing and signed by a duly authorized representative of Ramp Networks.

Ramp Networks Hardware Warranty

The hardware of your Ramp Networks product ("HARDWARE PRODUCT") is covered by a Limited Warranty. Ramp Networks warrants that the HARDWARE PRODUCT that you have purchased from Ramp Networks or from an authorized reseller is free from defects in materials or workmanship for one year from the date of purchase.

During the Limited Warranty period, Ramp Networks will repair or replace the HARDWARE PRODUCT with the same or a similar model, which may be a remanufactured unit, at Ramp Networks' option, without charge for either parts or labor. Replacement parts assume the remaining warranty of the parts they replace. This Limited Warranty extends only to the original purchaser and is non-transferable.

What is NOT covered by this Limited Warranty:

- Unauthorized modification or misuse.
- Operation outside of the environmental specifications for the HARDWARE PRODUCT.
- Damage due to lightning, "Acts of God," elements of nature, failure or fluctuation of electrical power, fire, theft, add-on items, or attachments.

- Damage from repair or replacement of warranteed parts by anyone other than Ramp Networks or a Ramp Networks authorized service provider.
- Third-party software applications shipped with the HARDWARE PRODUCT.

In order to make a claim under this warranty, you must comply with the following procedure:

- Contact Ramp Networks Technical Support within the warranty period to obtain a Return Materials Authorization ("RMA") number.
- Return the defective HARDWARE PRODUCT and proof of purchase, shipping prepaid, to Ramp Networks with the RMA number prominently displayed on the outside of the package.

If you are located outside of the United States or Canada, please contact your reseller in order to arrange for warranty service.

THE ABOVE WARRANTIES ARE MADE BY RAMP NETWORKS ALONE, AND THEY ARE THE ONLY WARRANTIES MADE BY ANYONE REGARDING THE ENCLOSED HARDWARE PRODUCT. RAMP NETWORKS AND ITS LICENSOR(S) MAKE NO OTHER WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, REGARDING THE ENCLOSED HARDWARE PRODUCT. EXCEPT AS OTHERWISE EXPRESSLY PROVIDED ABOVE, RAMP NETWORKS AND ITS LICENSOR(S) DO NOT WARRANT, GUARANTEE, OR MAKE ANY REPRESENTATION REGARDING THE USE OR THE RESULTS OF THE USE OF THE HARDWARE PRODUCT IN TERMS OF ITS CORRECTNESS, ACCURACY, RELIABILITY, CURRENTNESS, OR OTHERWISE. THE ENTIRE RISK AS TO THE RESULTS AND PERFORMANCE OF THE HARDWARE PRODUCT IS ASSUMED BY YOU. THE EXCLUSION OF IMPLIED WARRANTIES IS NOT PERMITTED BY SOME STATES OR JURISDICTIONS, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. IN THAT CASE, ANY IMPLIED WARRANTIES ARE LIMITED IN DURATION TO NINETY (90) DAYS FROM THE DATE OF DELIVERY OF THE HARDWARE PRODUCT. THERE MAY BE OTHER RIGHTS THAT YOU MAY HAVE WHICH VARY FROM JURISDICTION TO JURISDICTION.

REGARDLESS OF WHETHER OR NOT ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL RAMP NETWORKS, ITS LICENSOR(S) AND THE DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS OF ANY OF THEM BE LIABLE TO YOU FOR ANY CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES (INCLUDING DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, AND THE LIKE) ARISING OUT THE USE OR INABILITY TO USE THE HARDWARE PRODUCT, EVEN IF RAMP NETWORKS OR ITS LICENSOR(S) HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU. THE LIABILITY OF RAMP NETWORKS AND ITS LICENSOR(S) TO YOU FOR ACTUAL DAMAGES FROM ANY CAUSE WHATSOEVER, AND REGARDLESS OF THE FORM OF THE ACTION (WHETHER IN CONTRACT, TORT [INCLUDING NEGLIGENCE], PRODUCT LIABILITY, OR OTHERWISE), WILL BE LIMITED TO $50.

Contents

About This Guide

The *WebRamp 700s User's Guide* provides information about the installation process and the features of the WebRamp 700s. This guide is intended for network administrators and installers, and assumes that you are familiar with Ethernet networks and installing and handling electronically sensitive equipment.

What's in This Guide

The *WebRamp 700s User's Guide* is organized as follows:

Chapter 1, "Before You Begin," describes the features of the WebRamp 700s, the computer and browser requirements needed to set up the WebRamp 700s, and setup considerations for owners of other WebRamp models.

Chapter 2, "Setting Up the WebRamp 700s," describes the hardware of the WebRamp 700s and how to connect it to your network. This chapter also describes how to set up a computer to use for configuring the WebRamp 700s, provides an installation checklist, and steps you through the WebRamp 700s Installation Wizard.

Chapter 3, "Managing the WebRamp 700s," describes how to use a web browser to configure all aspects of the WebRamp 700s. This chapter also contains information about procedures for configuring, rebooting, and resetting the WebRamp 700s, setting factory defaults, uploading new software, accessing the network, using proxies, and limiting access to Intranet resources.

Appendix A, "Technical Specifications," lists the technical specifications for the WebRamp 700s.

Appendix B, “IP Port Numbers,” describes the three ranges of port numbers.

Appendix C, “Installing a Proxy Server,” tells how to set up a proxy server with the WebRamp 700s.

Technical Support

You can reach the Technical Support group at Ramp Networks by phone, e-mail, fax, or mail. The hours are 6 AM to 5 PM, Pacific Standard Time (U.S.).

Here are the ways you can reach Technical Support.

- Web site: www.rampnet.com/support
- Mailing address: Technical Support, Ramp Networks, 3100 De La Cruz Blvd., Santa Clara, CA 95054, U.S.A.
- Fax: 1(408) 988-6363, attention Technical Support
- E-mail: support@rampnet.com
- Phone: 1(888) 726-7638

When you request support, please provide the serial number of your WebRamp 700s, your name, your company name, street address, e-mail address, and phone number.

Chapter

1

Before You Begin

This chapter describes the features of the WebRamp 700s, discusses the computer and browser requirements needed to set up the WebRamp 700s, and talks about setup considerations for owners of other WebRamp models.

About the WebRamp 700s

The WebRamp 700s is an Internet security device that provides a security firewall between your local area network (LAN) and the Internet. The WebRamp 700s acts as a secure barrier to prevent access to your network from unauthorized Internet users. You can use the WebRamp 700s to prevent theft, destruction, or modification of data, to log events that may affect the security of your system, and to filter incoming data for objectionable content from web sites and newsgroups. You can also use it to block access to Internet resources to the users on your network.

The WebRamp 700s includes a four-port hub, which enables you to connect up to four computers and create a secure network. If you need to expand your network, you can connect a hub to the WebRamp 700s.

Because you install the WebRamp 700s between the LAN and your router or cable or DSL modem, it acts as a secure gateway for all data passing between the Internet and the LAN.

NOTE – The WebRamp 700s does not support Internet connections with analog modems.

WebRamp 700s Features

The following sections describe the features of the WebRamp 700s.

Firewall Security

- **Stateful inspection.** The WebRamp 700s uses stateful packet inspection to determine if a data packet is allowed through the firewall to the private LAN. By default, all incoming data that is in response to sessions initiated by users within the private LAN is allowed and all other incoming traffic is blocked.
- **Network Address Translation.** Network Address Translation (or NAT) translates multiple IP addresses on the private LAN to one public address that is sent out to the Internet. This adds a level of security, because the address of a computer connected to the private LAN is never transmitted on the Internet. NAT also allows the WebRamp 700s to be used with xDSL or cable modems, where only one IP address is provided by the ISP.
- One-to-One NAT. One-to-one NAT maps external addresses to one internal address, which is hidden by NAT. This allows machines using internal addresses to be accessed from the Internet.
- **Java, ActiveX, cookie, proxy blocking.** Many web sites contain Java and ActiveX applets and cookies, which can make them vulnerable to hackers. The WebRamp 700s examines HTTP traffic and blocks the download of the Java and ActiveX portions of a Web page. It also blocks cookies. You can customize this feature by allowing Java, ActiveX, and cookies from trusted sites. When a proxy server is located on the WAN, LAN users can point to this proxy server to circumvent content filtering. The WebRamp 700s prevents this by letting you block access to proxy servers.
- **Hacker attack prevention.** The WebRamp 700s is configured to automatically detect and thwart Denial of Service (DoS) attacks such as Ping of Death, Syn Flood, Land Attack, IP Spoofing, and so on.
- **Alerts.** The WebRamp 700s maintains a log of events that may be security concerns. You can use a web browser and the Web Management Interface to view the log, or have it sent as an e-mail message to any e-mail address.
- **Network access rules.** Network access rules are management tools that allow you to define rules that extend the firewall functions of the WebRamp 700s.

- **Public LAN servers.** You can configure the WebRamp 700s to allow access from the Internet to specific machines on the LAN. For example, you might allow access to a company's inventory database so suppliers can track inventory levels.
- **MD5 encrypted management sessions.** The WebRamp 700s uses MD5 encryption to ensure the privacy of all management and remote access user names and passwords.

Content Filtering

- **Internet content filtering.** You can set up Internet content filtering (filter list) to block or monitor access to specific sites. You can provide users with a password to bypass the filter for unrestricted Internet access.
- **Filter list subscription (optional).** A filter list subscription is available that automatically updates the filter list on a weekly basis. This ensures that access restrictions are in place for all new and relocated sites.

  See the Ramp Networks Online Store information on content filter list subscriptions and feature upgrades.

  Web site: **www.rampnet.com/order/index.html**

  Phone: 1(888) 726-7638

  Fax: 1-408-988-6363

  E-mail: sales@rampnet.com
- **Customizable list.** The WebRamp 700s supports customization of the filter list. You can add sites to the list or allow access to blocked sites.
- **Configurable deny message.** When a user attempts to access a blocked site, a message appears on the user's screen. You can modify this message to suit your needs or direct users to your Acceptable Use Policy statement.
- **Block all web sites except.** You can configure the WebRamp 700s to allow web access only to sites on a custom list, which you create. With careful screening, this can be close to 100% effective at blocking objectionable material.
- **Authorized users may bypass the filter.** The WebRamp 700s allows you to set up accounts that allow certain users to bypass the content filters. For example, a school administrator could give teachers an account that allows them to visit any site on the Internet, regardless of whether or not it's included in the filter list.

- **Block URLs by keywords.** You can configure the WebRamp 700s to block web sites that contain certain keywords. For example, if you enter the keyword “XXX”, the URL http://www.new-site.com/xxx.html is blocked, even if it is not included in the filter list.
- **Log and block access or log only.** You can configure the WebRamp 700s to log attempts and block access to all sites on the filter list, custom list, and keyword list, or to simply log the attempt and then allow access to the site. This lets you choose the proper restriction method for your network without losing the ability to monitor appropriate usage.
- **Restrict web features.** In addition to blocking access, you can also configure the WebRamp 700s to refuse to accept ActiveX, Java, and cookies from sites accessed from the LAN.
- **Consent.** This feature allows you to fine-tune which machines are always filtered and which are filtered only when protection is requested by the user.
- **Time of day.** You can limit content filtering to specific time periods and days of the week.

Logs

- **Log categories.** You can choose which information to show in the WebRamp 700s event log. You can schedule when you want to view the log or if you want to receive it by e-mail.
- **Alerts sent via e-mail.** When the WebRamp receives an Alert event (such as an attempted attack), it immediately sends a message to the e-mail account or e-mail pager that you specify.
- **Predefined reports.** The WebRamp 700s can perform a rolling analysis of the event log to show the top 25 most accessed web sites, the top 25 users of bandwidth by IP address, and the top 25 services that consume bandwidth.
- **Syslog.** In addition to the standard screen log, the WebRamp 700s can write detailed event log information to an external Syslog server. Syslog is an industry standard protocol used for capturing log information for devices on a network.

Easy to Install

- Installation Wizard. The WebRamp 700s Installation Wizard is an easy-to-use, step-by-step installation tool that lets you quickly configure the WebRamp 700s.

- **Web management interface.** You can install the WebRamp 700s from a Windows computer, Macintosh computer, or Unix workstation using any web browser that supports Java.
- **Connects between an existing Internet router and LAN.** You install the WebRamp 700s between your router's Ethernet port and the LAN, offering the perfect security complement to an Internet access router. This placement ensures that the WebRamp 700s analyzes all traffic to and from the Internet. When you add the WebRamp 700s to your network, you don't need to reconfigure your existing Internet router.
- **Automatic web proxy forwarding.** The WebRamp 700s can automatically forward all web proxy requests to the proxy server.
- **Online help.** Documentation is built into the WebRamp 700s for easy access from the Web Management Interface during installation and use.
- **No reconfiguration of computer applications.** Since the WebRamp 700s is transparent to user applications, you do not need to configure a proxy address for each client application used on the network.
- **Compact design.** The WebRamp 700s is about the size of a videocassette, making it easy to fit into an already crowded office or wiring closet. The solid-state design of the WebRamp 700s eliminates the need for a cooling fan.

Easy to Administer

- **Logs e-mailed at scheduled times.** Instead of connecting to the WebRamp 700s on a daily basis to read the activity log, the WebRamp 700s can send you the log file via e-mail at the times you specify.
- **Status screen.** You can view the configuration and operational status of the WebRamp 700s from a single web browser window. Important reminders, such as changing the default password, are highlighted in red.
- **WebRamp 700s configuration saved to local computer.** The Web Management Interface of the WebRamp 700s makes it easy to save the configuration file to a local computer or workstation. You can also upload configuration files to the WebRamp 700s using the web browser.
- **Flash upgrades.** As new features and maintenance releases become available, you can upgrade the WebRamp 700s firmware using a web browser. Ramp Networks maintains current versions of "flash images" for the WebRamp 700s on its web site.

- **Automatic notification of new software.** The WebRamp 700s checks to see if new firmware is available for download from Ramp's FTP site on a weekly basis. If there is a new firmware release, you receive an e-mail informing you of the new version's availability and new features.

Intranet Support

The WebRamp 700s allows Intranet firewalling by letting you restrict access to certain resources on the LAN. For example, you can limit access to a company's accounting department or other sensitive resources to other users on the same network. Or, schools can use this feature to restrict access to the administration office computers by users in a student computer lab.

Remote Access From the Internet

Users can access Intranet resources on the private LAN by successfully logging into the WebRamp 700s from the Internet. To log in, users must have a valid user name and password specified on their computers. The name and password are sent to the WebRamp 700s by the remote user using a web browser through an MD5-based encrypted security mechanism. Once logged in, remote users can access all IP resources on the LAN. The connection closes if user inactivity on the connection exceeds the configured time-out period.

NOTE – For remote users to access Intranet resources remotely from the Internet, the WebRamp 700s must be in Standard mode, and all the LAN IP addresses must be valid and static.

DHCP Server and Client

The DHCP server provides centralized management of TCP/IP client configurations, including IP address, gateway address, DNS address, and more. At startup, each network client receives its TCP/IP settings automatically from the DHCP Server.

DHCP Client allows the WebRamp 700s to acquire TCP/IP settings (such as IP address, gateway address, DNS address, and so on) from the ISP. This is ideal when only one TCP/IP address is provided by the ISP and this address may change from time to time, as is the case with some xDSL or cable modem Internet accounts.

You can choose to use the DHCP Server on the WAN or on your router instead of using the WebRamp 700s DHCP Client.

WebRamp Owners

If you are already using a WebRamp on your LAN, you should note the following features and characteristics of the WebRamp 700s. They will have an impact on your existing WebRamp setup.

- You install the WebRamp 700s between the LAN and the other WebRamp. This means that the WebRamp 700s is on the LAN side, and your other WebRamp will be on the WAN side, outside the firewall.
- The WebRamp 700s provides a DHCP server. If you are currently using the DHCP server of your other WebRamp, or any other router's, and want to use the DHCP server of the WebRamp 700s instead (which will be on the LAN side), you need to disable the DHCP server on your existing WebRamp.

NOTE – There can be only one enabled DHCP server on the network. If you want to use the DHCP server of the WebRamp 700s, disable the other DHCP server before installing the WebRamp 700s.

- The WebRamp 700s does not support bridging or IPX connections. If you have a bridging or IPX connection to another office and you want to use the WebRamp 700s, you must reconfigure this connection to use IP routing.
- WebRamps have certain reserved IP addresses. The WebRamp 700s uses the IP address of 192.168.1.251. Other WebRamp models use the IP address of 192.168.1.1 The addresses 192.168.1.252, 192.168.1.253, and 192.168.1.254 are reserved for users dialing in from remote locations.
- If you used another WebRamp model to set up a local server on your LAN, you must enter the same setting information in the WebRamp 700s. For more information, see "Rules" in Chapter 3.
- Visible computers are not supported on the LAN side of the 700s. It's possible to set up a visible computer with another WebRamp model on the WAN side, but it can pose a security risk since it will not be protected by the WebRamp 700s.
- The Internet Applications feature is not supported on the LAN side of the WebRamp 700s. It's possible to set up a computer with another WebRamp model to use Internet applications on the WAN side, but it can pose a security risk since it will not be protected by the WebRamp 700s.

Understanding the Three Modes of the WebRamp

You can use the WebRamp 700s in one of three modes:

- **Standard.** Choose this mode if your network uses IP addresses provided by the ISP. You can also use this mode if you want to use the NAT feature on the router on your network instead of the NAT on the WebRamp 700s. If you are using a WebRamp M3, 300e, or 410i and a single IP address for your LAN's Internet connection, use this mode.
- **NAT Enabled.** Network Address Translation (NAT) connects the LAN to the Internet using a single IP address. Use this mode if your network includes a WAN router and you want to use private TCP/IP addresses on your LAN with two or more valid IP addresses in a subnet provided by an ISP. You should also use this mode if you are using an xDSL or cable modem and your ISP provides static instead of dynamic IP addresses.
- **NAT With DHCP client.** Use this mode if the ISP provides a dynamic IP address from a remote DHCP server on the WAN. For example, when you use a cable modem or xDSL modem for the Internet connection.

What the WebRamp 700s Includes

The following items are included in the WebRamp 700s package:

- One WebRamp 700s
- One 5 VDC power supply
- One 10BaseT crossover cable (the cable is red and labeled "Crossover")
- One 10BaseT standard cable
- *WebRamp 700s User's Guide* (this book)
- *WebRamp 700s CD*

The *WebRamp 700s CD* includes all of the documents and software you need to set up and use your WebRamp 700s. You can run the CD on any Windows computer, Macintosh computer, or Unix workstation that has a CD drive. The CD includes:

- *WebRamp 700s User's Guide.* In addition to the printed version included in the WebRamp 700s package, this book is provided on the CD in pdf format.
- Netscape Communicator. This web browser is included in case you need one.

- Adobe Acrobat Reader. This application is included in case you need it to view the pdf version of the *WebRamp 700s User's Guide*, which is on the CD.
- Setup Tool. You can use the Setup Tool to find an unconfigured WebRamp 700s on your LAN or to find the WebRamp 700s on your LAN if you forgot its IP address.
- WebRamp 700s firmware, version 4.1. The firmware is provided in case you need to reinstall it.

What You Need

In addition to the WebRamp 700s, the computer that you choose to configure the WebRamp must meet certain requirements. This section discusses what you need to set up the WebRamp 700s using either a Windows computer or a Macintosh computer.

The installation process also requires a browser. This section also discusses the browser requirements.

Windows Requirements

A Windows system must meet the following requirements:

- a Windows 95, Windows 98, or Windows NT 4.0 computer that has an Ethernet network card installed
- TCP/IP network protocol installed for each computer
- 16 MB of RAM (32 MB recommended)

Macintosh Requirements

A Macintosh computer must meet the following requirements:

- a 68030 Macintosh computer (PowerPC recommended) running system software version 7.5.3 or later that has an Ethernet network card installed
- Open Transport 1.1.2 (or higher) or MacTCP 2.0.6 installed for each computer
- 16 MB of RAM (32 MB recommended)

Browser Requirements

The web browser you use must be Java-enabled and support HTTP uploads in order to fully manage the WebRamp 700s. If you use a browser that does not support HTTP uploads, certain features, such as updating the software and uploading pre-configured settings, will not work. Netscape Navigator (version 3.0 and above) and Microsoft Internet Explorer (version 4.0 and above) meet the requirements. For your convenience, Netscape Navigator (for Windows and Macintosh) is included on the WebRamp 700s CD.

Chapter

2

Setting Up the WebRamp 700s

This chapter describes the hardware features of the WebRamp 700s and how to set it up on your existing network. This chapter also tells you how to set up a computer to use to set up the WebRamp 700s, provides an installation checklist, and steps you through the WebRamp 700s Installation Wizard.

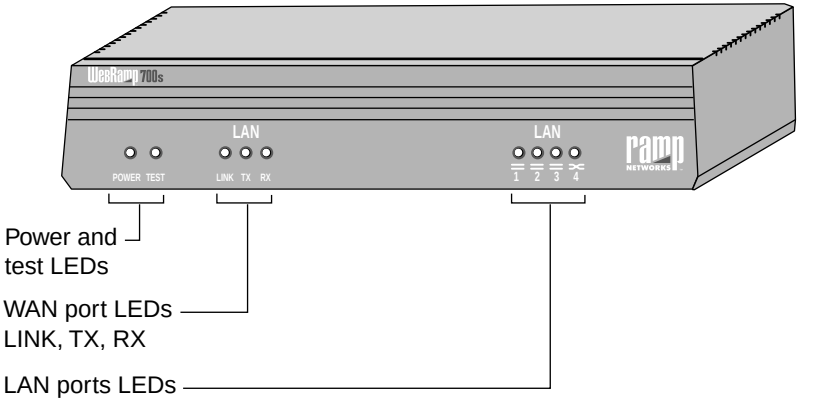
Hardware Description

This section describes the physical characteristics of the WebRamp 700s.

Front View

Figure 2-1 shows the front view of the WebRamp 700s.

Figure 2-1 Front view



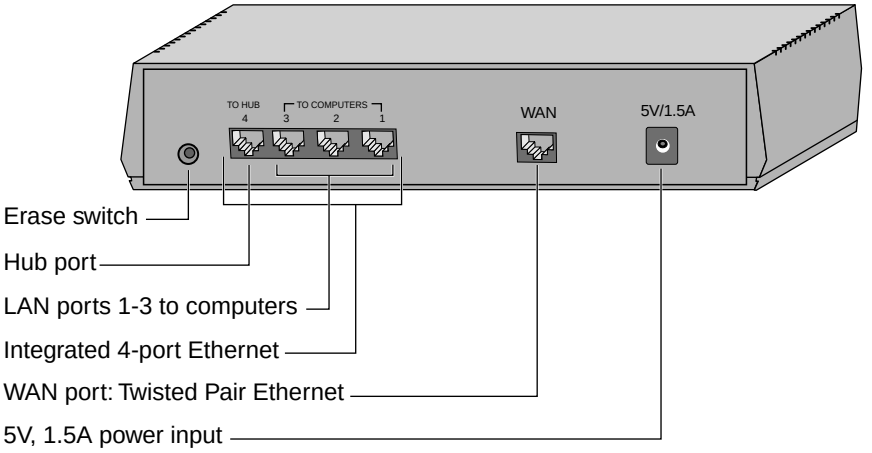
The front panel of the WebRamp 700s contains the following:

- **Cooling vents.** The WebRamp 700s is convection cooled; no internal fan is needed.
- **Power LED.** Lights up when you connect the WebRamp 700s to a power source.
- **Test LED.** The WebRamp performs a series of diagnostics checks when it first starts up. While these diagnostics are running (about 90 seconds), this LED is amber. When the diagnostics are complete, the LED is dark. If the **Test** LED remains lit after 90 seconds, the software is damaged and must be reinstalled.
- **WAN LEDs**
  - **LINK.** Lights up when a twisted-pair connection is made to another Ethernet device on the port. The device must support the standard Link Integrity test.
  - **TX.** Lights up when the WebRamp 700s transmits a packet through the twisted-pair port to the network.
  - **RX.** Lights up when the WebRamp 700s receives a packet through the twisted-pair port.
- **LAN LEDs.** Each LAN port LED lights up when connected to another Ethernet device and also flickers during any transmit or receive activity on that port. LAN ports 1, 2, and 3 are straight-through connections and LAN port 4 is a hub connection. (To connect port 4 to an additional computer instead of a hub, use a crossover cable.)

Back View

Figure 2-2 shows the back view of the WebRamp 700s.

Figure 2-2 Back view



The back panel of the WebRamp 700s contains the following:

- **Erase switch.** This switch erases the WebRamp's firmware.When pressed, all connections through the WebRamp 700s are dropped and all unsaved log information is lost. The firmware is cleared and you must then upload new firmware.

  Follow the steps below to erase all settings and reset the WebRamp 700s to its factory default state:

NOTE – This switch is functional only when power to the unit is off.

1. Turn off the power to the WebRamp 700s and disconnect it from the network.
2. Push and hold down the **Erase** switch while you power up the WebRamp 700s. Once the test LED starts to flash, release the **Erase** switch.
3. Upload and install new firmware to the WebRamp 700s, and then reconfigure it using the Installation Wizard. See "Setting Up the WebRamp 700s," for more information.

- **LAN ports:** Ports 1, 2, and 3 attach to computers. Port 4 can be connected to an additional computer or to a hub.
- **WAN port.** Connects to the cable modem, DSL modem, or Internet router (ISDN, Frame Relay, TI, and so on).
- **Power input (5VDC/1.5A).** Connects the external power supply to the WebRamp 700s.

WARNING – Always use the power supply designed for the WebRamp 700s in the power input. Do not use any power supplies from other WebRamp products with the WebRamp 700s.

Connecting the Hardware

This section assumes you're connecting the WebRamp 700s to a cable or DSL modem connected to a computer in a home office or small office, or that you're connecting it to an internal, protected network.

Here are some guidelines to help you set up your WebRamp 700s.

- You can connect four computers directly to the WebRamp 700s. To expand the number of connections to the WebRamp 700s, you can use an Ethernet hub.
- Use straight-through Ethernet cables when connecting computers directly to ports 1–3 of the WebRamp 700s. Use a crossover cable to connect a computer directly to port 4.
- Use a straight-through Ethernet cable when connecting port 4 of the WebRamp 700s to a hub or switch.

NOTE – Never connect two ports on the WebRamp 700s to the same physical wire. For example, never connect the LAN and WAN ports to the same hub. Doing this will bypass all firewall functions.

- Use a straight-through Ethernet cable when connecting the WAN interface to the Internet modem or router. If you're connecting to a hub, use a straight-through Ethernet cable.

NOTE – The connection can require either a straight-through or crossover Ethernet cable, depending on the type of modem or hub you're using. The WAN link LED will turn green when you use the correct cable.

Figure 2-3 shows a connection between the WebRamp 700s and a cable or DSL modem.

Figure 2-3 Connecting a cable or DSL modem and an Ethernet hub

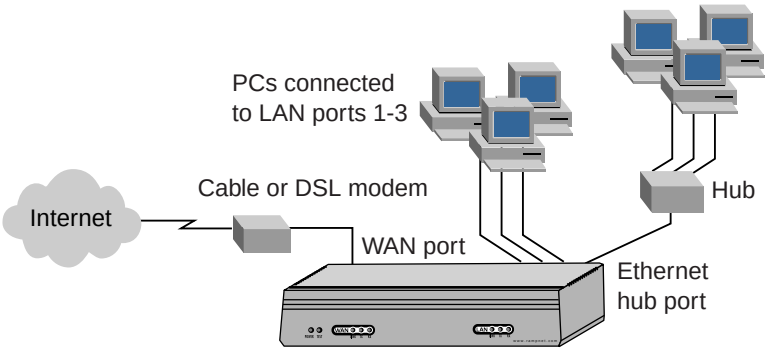
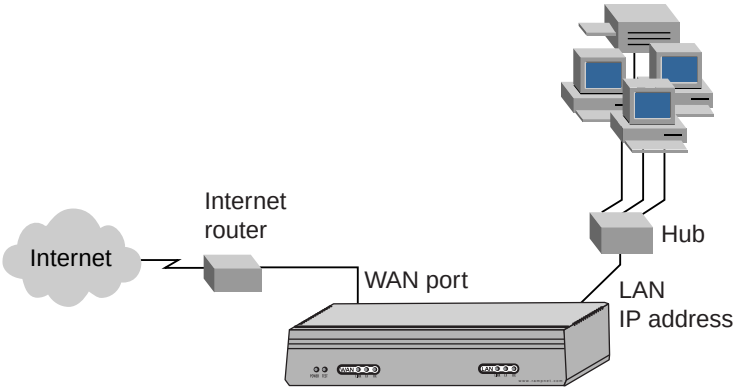


Figure 2-4 shows a connection between the WebRamp 700s and a router.

Figure 2-4 Connecting to the network



The following steps describe how to connect the WebRamp 700s to a cable or DSL modem or to a network that includes an Internet router (for example, one of the WebRamp 300 series):

1. Disconnect the Ethernet cable connecting the computer to the cable modem, DSL modem, or router from the computer end of the connection.
2. Connect the WAN port.

- **Cable or DSL modem.** Connect the Ethernet cable coming from the modem to the **WAN** port on the back of the WebRamp 700s. The **WAN Link** LED on the WebRamp 700s will turn green. If the LED doesn't turn green and you're using a straight-through Ethernet cable, try using the red crossover cable.
- **Router.** Using the red crossover cable, connect the WAN port on the back of the WebRamp 700s to the Ethernet port on the Internet router. If you're connecting to a hub, use a straight-through Ethernet cable.

NOTE – If the Internet router on your network is one of the WebRamp 300 series, connect it using an Ethernet cable, and then move the MDI switch until the Link LED comes on.

---

3. Connect the WebRamp 700s to the computers, network, or hub.
   - **Cable or DSL modem.** Connect a straight-through Ethernet cable to one of the first three Ethernet ports on the WebRamp 700s. Connect the other end to the computer. Repeat this for each computer you want to connect directly to the WebRamp 700s (use a crossover cable if connecting a computer directly to port 4).
   - **Router.** Using straight-through Ethernet cables, connect the four LAN ports to the computers or network.
   - **Hub.** If you're connecting additional computers using a hub, attach one end of a straight-through Ethernet cable to port 4 of the WebRamp 700s (which is labeled **To Hub**), and then attach the other end to the hub.
4. Plug the WebRamp 700s power supply into an AC power outlet, and then plug the power supply output cable into the **5VDC/1.5A** port on the back of the WebRamp 700s. The yellow **Test** LED on the WebRamp 700s lights up**.**

   The WebRamp 700s is designed to start up as soon as power is supplied to it. Then, it runs a series of self-diagnostics to check for proper operation. During these diagnostics, which take about 90 seconds, the **Test** LED remains lit.

   When the yellow **test** LED goes off, the WebRamp 700s is properly attached to your modem or network.

By default, all traffic from the LAN to the Internet is allowed, and traffic sourced from the Internet is blocked. The connected computers have access to Internet services such as e-mail, FTP, and the World Wide Web. To allow traffic from the Internet, see Chapter 3, "Managing the WebRamp 700s," for information about setting up access.

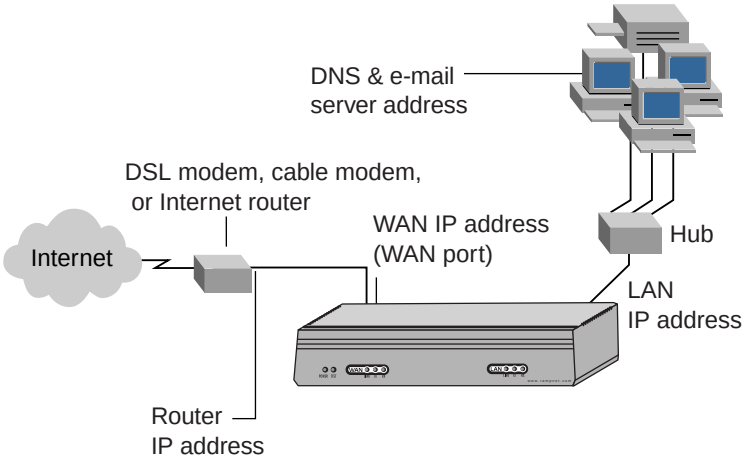
Setting Up the Computer

You can use a Windows computer, a Macintosh computer, or a Unix workstation and a web browser to set up the WebRamp 700s on your network. For initial setup, use the browser-based WebRamp 700s Installation Wizard. Later, in day-to-day management, use the browser to view the WebRamp Web Management Interface, which lets you edit settings and monitor your network activity.

WebRamp 700s Installation Checklist

Before you can configure the WebRamp 700s on a computer or network that uses an Internet router, you need information about the IP addressing on the computer or network. For example, you need DNS addresses, the LAN IP address, the subnet mask address, and the default gateway address (or router address for a Macintosh). You can get this information from your computer, in network settings, or from the Internet service provider (ISP) used to connect the network to the Internet. Figure 2-5 shows an example of a network and the addresses you'll need.

Figure 2-5 Required network addresses



The following checklist lists the network information you need before you run the WebRamp 700s Installation Wizard. When there is a default address, it appears in the third column. You can print this checklist, and then write down the addresses you'll be using so they'll be handy when you're running the Installation Wizard

Information	What it is	Address
WebRamp 700s LAN IP Address	The IP address you use to manage the WebRamp 700s. This address is assigned to the LAN port.	The default IP address is 192.168.1.251
LAN Subnet Mask	The LAN subnet mask determines the range of IP addresses that belong to the protected LAN.	The default subnet mask is 255.255.255.0
Router IP Address (Gateway)	The address of the router that attaches the LAN to the Internet through ISDN, a T1 line, or some other transmission medium. When you're using a cable or DSL modem, the Internet router is located at the ISP's office.	
DNS Server Address	The Domain Name Server (DNS) can be a server either on the LAN or on the Internet. The DNS address is required for downloading new Content Filter Lists and using the Name Lookup tool. May be supplied by the ISP.	
E-mail Server Address (Optional)	The address of the e-mail server used to send log messages. The server can be either on the LAN or on the Internet. For best results, use the same server as is used for LAN e-mail. Once you set up the Webramp 700s, you can use the DNS Name Lookup tool to find the IP address of the e-mail server.	

Information	What it is	Address
If using NAT:		
Public Internet Address (WAN port)	The IP address that the entire network uses to access the Internet. This address is supplied by the ISP.	
WAN Subnet Mask	The WAN subnet mask determines the range of IP addresses that belong to the Internet. Supplied by the ISP.	

Gathering the Network Settings

This section tells you how to gather the network settings required to set up the WebRamp 700s.

With the checklist handy, follow these steps to record the network settings of the computer you're using to set up the WebRamp 700s.

For cable or DSL modems (Windows)

1. From the Start menu, choose **Run.**
2. In the dialog box that appears, type **winipcfg,** and then click **OK.**
3. In the IP Configuration window, click **More Info.** The network information appears.
4. On the checklist, write the information about the IP address, subnet mask, gateway address, and DNS servers.

For cable or DSL modems (Macintosh)

1. From the Apple menu, choose **Control Panel,** and then **TCP/IP.** The TCP/IP control panel appears.
2. On the checklist, write the information about the IP address, subnet mask, router address, and name server address.

For Internet routers (using NAT)

Windows:

1. From the Start menu, choose **Run.**
2. In the dialog box that appears, type **winipcfg,** and then click **OK.**

3. In the IP Configuration window, click **More Info.** The network information appears.
4. On the checklist, write the information about the IP address, subnet mask, gateway address, and DNS servers.

Macintosh:

1. From the Apple menu, choose **Control Panel,** and then **TCP/IP.** The TCP/IP control panel appears.
2. On the checklist, write the information about the IP address, subnet mask, router address, and name server address.

NOTE – If you're using DHCP on a Macintosh computer and the settings don't appear in the TCP/IP control panel, contact your ISP for the information.

For Internet routers (using traditional routing)

Obtain the following network information from your ISP, and then write it on the checklist:

- At least two IP addresses
- Subnet mask
- DNS address

Changing the Computer's IP Address

The WebRamp 700s comes from the factory with the default IP address of 192.168.1.251. For initial setup, you must temporarily change the IP address of the computer to one that is in the same subnet as the WebRamp 700s.

NOTE – You should always write down the existing IP settings of the computer before changing them. You may need to change the computer back to its original settings once you complete the setup of the WebRamp 700s.

For cable or DSL modems (Windows)

1. From the Start menu, choose **Settings,** and then choose **Control Panel.**
2. In the Control Panel window, double-click **Network.**

3. Double-click **TCP/IP**
4. In the TCP/IP Properties window, click **Specify an IP Address.**
5. Enter **192.168.1.250** in the IP Address field.
6. Enter **255.255.255.0** in the Subnet Mask field.
7. Click **OK** and then click **OK** again.
8. Restart the computer.

For cable or DSL modems (Macintosh)

1. From the Apple menu, choose **Control Panels,** and then choose **TCP/IP.**
2. From the Connect Via menu, choose **Ethernet** or **Ethernet Built-in**.
3. From the Configure menu, choose **Manually**.
4. In the IP address field, enter **192.168.1.250.**
5. Clear any existing information from the Router Address and Name Server Address fields.
6. Close the control panel.

For Internet routers (dynamic network on a Windows computer)

1. From the Start menu, choose **Run.**
2. In the dialog box that appears, type **winipcfg,** and then click **OK.**
3. In the IP Configuration window, choose **Ethernet Adapter** from the menu.
4. Click **More Info**.
5. Click the **Release All** button.
6. Click the **Renew All** button.
7. Click **OK**.

For Internet routers (dynamic network on a Macintosh computer)

1. From the Apple menu, choose **Control Panels**, and then choose **TCP/IP**.
2. From the **Connect via** menu, choose **Ethernet** or **Ethernet Built-in.**
3. From the **Configure** menu, choose **Using DHCP Server**.
4. Close the control panel.

For Internet routers (static network on a Windows computer)

For Internet routers on a static network, you must manually change the IP address of the computer to one in the same subnet as the WebRamp 700s (for example, 192.168.1.250).

1. From the Start menu, choose **Settings,** and then choose **Control Panel.**
2. In the Control Panel window, double-click **Network.**
3. In the Network window, click the **Protocols** tab.
4. Choose **TCP/IP Protocol** and then click **Properties.**
5. In the TCP/IP Properties window, click **Specify an IP Address.**
6. Enter **192.168.1.250** in the IP Address field.
7. Enter **255.255.255.0** in the Subnet Mask field.
8. Click **OK** and then click **OK** again.
9. Restart the computer.

For Internet routers (static network on a Macintosh computer)

For Internet routers on a static network, you must manually change the IP address of the computer to one in the same subnet as the WebRamp 700s (for example, 192.168.1.250).

1. From the Apple menu, choose **Control Panels,** and then choose **TCP/IP.**
2. From the Connect Via menu, choose **Ethernet** or **Ethernet Built-in**.

3. From the Configure menu, choose **Manually**.
4. In the IP address field, enter **192.168.1.250.**
5. Clear any existing information from the Router Address and Name Server Address fields.
6. Close the control panel.

Configuring the WebRamp 700s

Once you've changed the settings on the computer you want to use to set up the WebRamp 700s, you can run the Installation Wizard to complete the setup process. Follow these steps:

NOTE – For most networks, configuring your WebRamp 700s is quick and easy; you simply follow the directions in the Installation Wizard. The default settings in the Wizard can be used for most existing networks.

---

1. On the computer you're using to set up the WebRamp 700s, launch the web browser.
2. In the web browser's location or address field type 192.168.1.251, the factory default IP address of the WebRamp 700s.

   Because this is the first time you log on to the WebRamp 700s, the WebRamp Installation Wizard launches automatically.

NOTE – To start the Installation Wizard after initial configuration, open the WebRamp 700s Management Interface and click Tools, then Preferences, and then Launch Wizard. For more information, see "Preferences" in Chapter 3.

---

3. Read the information in the Wizard's Welcome window, confirm you have the information specified, and then click **Next.**
4. In the New Password and Confirm New Password fields, enter a new password and then click **Next**.

   The default user name is **admin** (which you cannot change), and the default password is **password**. The security of the WebRamp 700s depends on the secrecy of the administrator password, so you should change it as soon as possible.

NOTE – Passwords are case-sensitive.

5. From the pull-down menu, select your time zone to set the internal clock of the WebRamp 700s. The internal clock is automatically set by the Network Time Server on the Internet. Click **Next**.

6. Choose a network addressing mode, and then click **Next.**
   - Select **Zero** (**NAT with DHCP Client**) if your ISP is using DHCP in their service. The ISP will dynamically assign an IP address to your WebRamp 700s from their DHCP server.
   - Select **One (NAT Enabled**) if your ISP has supplied you with a single valid (registered) IP address, a WAN subnet mask address, a WAN gateway (router) address, and a DNS server address.

NOTE – Select **One** if you plan on using **One-to-One NAT.**

   - Select **More Than One** to use either **NAT Enabled** or **Standard** mode.

7. Enter the **Public Network Settings**
   - If you selected Zero in step 6, a window appears with a message telling you that your ISP will dynamically assign an IP address to the WebRamp 700s.

     Click **Next** and **go to step 9.**
   - If you selected One in step 6, a window appears with a message telling you that your ISP has provided you with a registered IP address for the WebRamp 700s.

     Click **Next**.
   - If you selected More Than One in step 6, the Optional – Network Address Translation (NAT) window appears.

     Click **Don't Use NAT** if you have registered IP addresses for the WebRamp 700s and all the computers and network devices on your LAN.

     Click **Use NAT** if you do not have registered IP addresses for the WebRamp 700s and all the computers and network devices on the LAN.

     Click **Next.**

8. In the Getting to the Internet Window, replace the settings that appear with the addresses provided by your ISP, and then click **Next**.

9. In the Fill in Information About Your LAN window, enter the LAN IP address (referred to in the window as the web management address) of the WebRamp 700s and the LAN subnet mask address. The default values that appear in the window work for most networks.

   Click **Next.**

10. If desired, enter an **e-mail address** for log delivery.

    You can specify an e-mail address where the WebRamp can automatically send the event log. Enter your e-mail server address and e-mail address. If you don't want the WebRamp to send the event log to an e-mail address, leave the fields blank.

    Click **Next.**

11. If desired, choose to use the **WebRamp 700s DHCP Server**.
    - Verify that **Enable DHCP Server** is selected if you want the WebRamp 700s DHCP server to automatically configure the IP addresses for all the computers and other network devices on your LAN.
    - Deselect **Enable DHCP Server** if you don't want to use the WebRamp 700s DHCP Server, and delete the information in the IP address fields.

12. Click **Next**. A success window appears that shows the WebRamp's current LAN IP address and allows you to register the WebRamp. For information on registering your WebRamp, see the section "Registering Your WebRamp 700s."

NOTE – Write down the IP address information that appears in this window. You may need it later to reconfigure your computer.

Now, depending on your network setup, do the following:

- **For cable or DSL modems,** you need to configure the other computers on the LAN. See the section "Configuring the LAN Computers" for detailed information.
- **For Internet routers,** click **Restart** to restart the WebRamp 700s. When the WebRamp restarts (approximately 90 seconds) click the **Close** button to close the Installation Wizard.

At this time, you may need to reset the IP address of the computer you used to configure the WebRamp. Reset the IP address of the computer according to the information from the last screen of the Installation Wizard. Depending on the computer's operating system, you may need to restart for the changes to take effect.

NOTE – You can verify at any time the current settings of the WebRamp 700s. See the section "Checking Your Settings."

Configuring the LAN Computers

This section is for cable and DSL modem users only, and the configuration steps differ depending on whether you're using the WebRamp 700s DHCP server.

If You're Using the WebRamp 700s DHCP Server

When you choose to use the WebRamp 700s DHCP server, after you complete configuration and restart, you see a message similar to the one shown in Figure 2-6.

Figure 2-6 Using WebRamp 700s DHCP server

At this time, you need to configure the computers on your network so that they can get their IP addresses dynamically from the WebRamp 700s. Follow these steps:

For Windows computers

1. From the **Start** menu, choose **Settings,** and then choose **Control Panel.**
2. Double-click the **Network** icon.
3. Double-click **TCP/IP**
4. Click **Obtain an IP Address Automatically.**
5. Clear any existing information in the **DNS Configuration** and **Gateway** tabs.
6. Click **OK,** and then click **OK** again.
7. Restart the computer.

For Macintosh computers

1. From the Apple menu, choose **Control Panels**, and then choose **TCP/IP**.
2. From the **Connect via** menu, choose **Ethernet** or **Ethernet Built-in.**
3. From the **Configure** menu, choose **Using DHCP Server.**
4. Clear any existing information in the **IP Address**, **Subnet mask**, **Router address**, and **Name server address** fields.
5. Close the control panel.

If You're Not Using a DHCP Server

When you choose not to use the WebRamp 700s DHCP server, after you complete configuration and restart, you see a message similar to the one shown in Figure 2-7.

Figure 2-7 No DHCP server

Before proceeding, note the information on this screen. You need to configure the computers on your network with static IP addresses. These addresses must be in the same subnet as the WebRamp 700s IP address, which is 255.255.255.0.

For Windows computers

1. From the **Start** menu, choose **Settings,** and then choose **Control Panel.**
2. Double-click the **Network** icon.
3. Double-click **TCP/IP**
4. Click **Specify an IP Address**.
5. In the **IP Address** field, enter an IP address (from the range indicated in the window shown in Figure 2-7).
6. Remember that the WebRamp has certain reserved IP addresses. See the section “WebRamp Owners” in Chapter 1 for details.
7. In the **Subnet Mask** field, enter 255.255.255.0.
8. In the Default Gateway field, enter **192.168.1.251**.
9. Click the DNS tab.
10. Enter the host name.

    If your ISP provided a host name, enter that. Otherwise, you can use the computer name.

11. Enter the domain name, if provided by the ISP. Otherwise, leave blank
12. Enter the DNS Service Search Order.

    Click Add and then enter the address provided by your ISP. Repeat for the second address.
13. Click **Add.**
14. Click **OK,** and then click **OK** again.
15. Restart the computers on the LAN to update their network settings.

For Macintosh computers

1. From the Apple menu, choose **Control Panels,** and then choose **TCP/IP**.
2. From the Connect via menu, choose **Ethernet** or **Ethernet Built-in.**
3. From the Configure menu, choose **Manually.**
4. In the IP Address field, enter an IP address (from the range indicated in the window shown in Figure 2-7).
5. In the Subnet Mask field, enter **255.255.255.0**.
6. In the Router address field, enter **192.168.1.251**.
7. In the Name server address field, enter your ISP's DNS number.
8. Close the control panel.

Checking Your Settings

Once the WebRamp 700s has finished restarting and you have reset any necessary computer settings, log back in using the new administrator password.

1. Launch the web browser.
2. Enter http:// 192.168.1.251 in the web browser's address field.
3. Click the **General button** along the left side of the screen, and then click the **Status** tab at the top of the browser window. A window similar to the one shown in Figure 2-8 appears.

Figure 2-8 Status window

The **Status** window displays the current status of the WebRamp 700s. Any problems are listed in red. For example, you may have forgotten to change the default password. Items in red require immediate, corrective action.

General operation status messages, such as enabled hacker attack protection, filter list status, and log settings are listed in black text.

This method of logging in and accessing the Web Management Interface using the buttons along the side of the browser window and the tabs along the top of the browser window is what you will use to manage your WebRamp 700s from now on. For more information, see Chapter 3, “Managing the WebRamp 700s.”

Registering Your WebRamp 700s

Take time now to complete the online Registration in the **Status window.** Registering the WebRamp 700s with Ramp Networks provides access to technical support, software updates, and information about new WebRamp products. Registered users are able to install and activate the Content Filter List and receive a free one month subscription to updated Content Filter Lists.

Chapter

3

Managing the WebRamp 700s

This chapter contains detailed information about the WebRamp 700s management commands and options. These commands and options are accessed using a web browser through the WebRamp 700s web management interface. Use this chapter as a reference when changing the configuration of the WebRamp 700s.

This chapter is divided into sections that describe the major windows and functions within the web management interface. Topics covered include:

- Using a web browser to configure the WebRamp 700s
- Network Settings window
- Enabling Network Address Translation (NAT)
- Setting the date and time
- Setting the Administrator's password
- Log settings and alerts
- Content filtering and blocking
- Network access rules
- Additional commands and functions
- VPN option

Using the Web Browser

All management functions on the WebRamp 700s are performed from a web browser using the WebRamp 700s web management interface. Management can be performed from any computer connected to the same network as the WebRamp 700s. Any computer can be used to administer the WebRamp 700s.

NOTE – The web browser you use must be Java-enabled and support HTTP uploads in order to fully manage the WebRamp 700s. If you use a browser that does not support HTTP uploads, certain features, such as updating the software and uploading pre-configured settings, will not work. Netscape Navigator (version 3.0 and above) and Microsoft Internet Explorer (version 4.0 and above) meet these requirements. For your convenience, Netscape Navigator 4.5 (for Windows and Macintosh) is included on the WebRamp 700s CD.

The web management interface uses Java technology for security and other functions. For this reason, it is necessary to enable Java and JavaScript on any system used to administer the WebRamp 700s. Java and JavaScript need not be enabled on other network machines. ActiveX does not need to be enabled on any of the computers on the LAN.

NOTE – Java itself is not a security risk, but it can be unsafe to run unknown Java applets on the network. Since the Java applets used by the web management interface are all stored in the WebRamp 700s, they originate from the LAN port and are not blocked if the WebRamp's Java and ActiveX blocking features are turned on.

To display the web management interface, type the WebRamp 700s address or host name into the **Location field** at the top of the browser window and press Return. During initial configuration, this IP address is 192.168.1.251. The Password dialog box, shown in Figure 3-1, appears.

Figure 3-1 Password dialog box

Enter **admin** into the **User Name** field and the password configured during initial configuration into the **Password** field. Click **Login**.

NOTE – The WebRamp 700s is configured with “admin” as the user name and “password” as the default password. The user name is not configurable. Passwords are case-sensitive.

For security reasons, the WebRamp 700s sends a slightly different **Authentication** page each time you log into the web management interface. If the password does not grant access to the WebRamp 700s, you may be seeing a cached copy of the page instead of the correct page. Click **Reload** or **Refresh** on the web browser and try again.

Once you enter the administrator’s password, an **authenticated management session** begins. For security reasons, a management session can only be established from a machine which is connected to the **LAN** port. The session times out after 5 minutes of inactivity and the **Authentication** window will no longer appear. You cannot configure this time-out interval.

Along the left side of the window is a row of buttons. When one of these buttons, **General**, **Log**, **Filter**, **Tools**, **Access**, **Advanced**, **DHCP**, and **VPN** is clicked, additional related management functions may be selected by clicking the tab at the top of the window. This button and tab interface allows quick and easy navigation to all management functions. For online help, click the button labeled **Help** on the top of any browser window to view the help files stored in the WebRamp 700s.

General

The General window shows the basic settings for your WebRamp 700s. From this window you can view the current WebRamp 700s status, make changes to the network settings, set the time, and change the password.

Status

The **Status** window displays the current status of the WebRamp 700s. It contains an overview of the WebRamp 700s configuration, as well as any important messages. It’s is a good idea to check this status window after changes are made to ensure the WebRamp 700s is configured properly.

After you've entered the user name and password, a window similar to the one shown below appears. You can also access this window by clicking the **General** button and then clicking the **Status** tab.

Figure 3-2 Status window

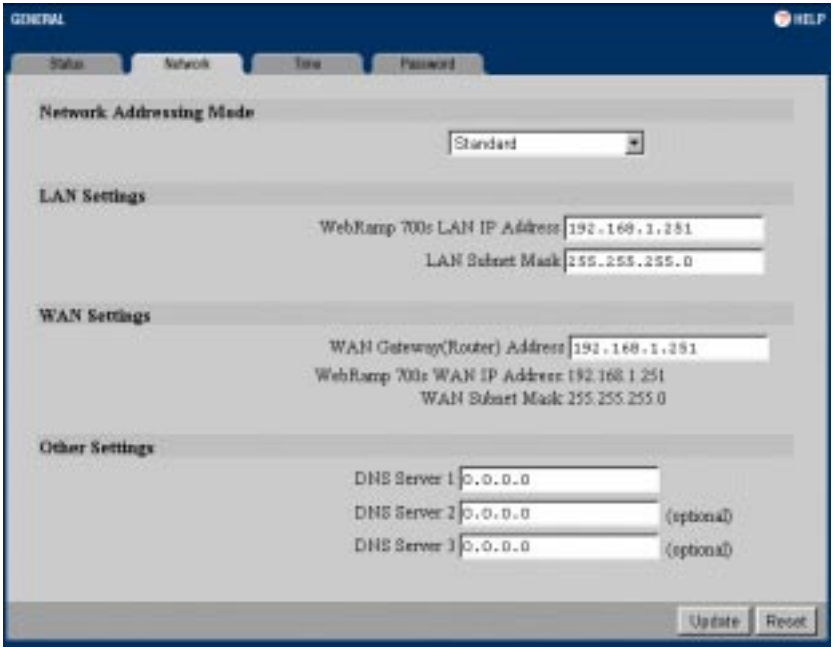
Make sure to complete the online Registration. Registering the WebRamp 700s provides access to technical support and software updates. Only registered users are able to install and activate the Content Filter List, and receive a one month subscription to updated Content Filter Lists at no charge.

Network

Setup your network addressing from the **Network** window. From this window, you can set the LAN, WAN and additional network settings.

At the top of the browser window, click the tab labeled **Network**. A window similar to the following is displayed.

Figure 3-3 Network window



Network Addressing Mode

The **Network Addressing Mode** menu includes three options:

- Use **Standard** if your network uses valid IP addresses and users require authenticated remote access to LAN resources, or when the WebRamp 700s is behind a NAT-enabled router.
- Use **NAT Enabled** if your network uses private TCP/IP addresses with two or more valid IP addresses in a subnet provided by the ISP and there is a WAN router.
- Use **NAT With DHCP Client** if your ISP provides the dynamic IP address from a remote DHCP server on the WAN, such as when a cable modem or xDSL modem is used to provide the Internet connection.

NOTE – If NAT is enabled on your existing router, you must use **Standard** mode for the WebRamp 700s.

Standard

When **Standard** is selected from the **Network Addressing Mode** menu, NAT is disabled. All nodes on the LAN must use valid IP addresses. If there is a router that has NAT enabled, the nodes can use private addresses.

The following information is required:

LAN Settings

- **WebRamp 700s IP Address.** This is the IP address assigned to the WebRamp 700s LAN interface and used to access it for configuration and monitoring. Choose a unique IP address from the LAN address range.
- **LAN Subnet Mask.** This value is used to determine what subnet an IP address belongs to. An IP address has two components, the network address and the host address. For example, suppose you enter the IP address 192.168.1.17. Assuming a Class C subnet mask of 255.255.255.0, the first three numbers (192.168.1) represent the Class C network address and the last number (17) identifies a particular host on this network

WAN Settings

- **WAN Gateway (Router) Address.** The WAN gateway address is the address of the router that attaches the LAN to the Internet through ISDN, a T1 line, or some other transmission medium.
- **WebRamp 700s WAN IP Address.** This value is automatically set to the WebRamp 700s web address.
- **WAN Subnet Mask**. This value is automatically set to the WebRamp 700s LAN Subnet Mask.

Other Settings

- **DNS Server**. A DNS server is used by the WebRamp 700s to look up the addresses of machines used to download the Content Filter List and for the built-in DNS Lookup tool. You can enter additional DNS Server addresses if available.

Enter the required values and click the **Update** button at the bottom of the screen. When the information has been updated, a confirmation message appears in the status line at the bottom of the window.

NOTE – You must restart the WebRamp 700s for changes to take effect.

NAT Enabled

Network Address Translation (NAT) provides anonymity to machines on the LAN by connecting the entire network to the Internet using a single TCP/IP address. This is useful for two purposes:

- It provides additional security because all the addresses on the LAN are invisible to the outside world.
- In cases where a network uses invalid TCP/IP addresses or if addresses are in short supply, NAT can be used to connect the LAN to the Internet without changing the TCP/IP addresses of computers and other devices on the LAN.

When using TCP/IP addresses which have not been assigned by an ISP, it's a good idea to use addresses from a special address range allocated for this purpose. Use the following IP address ranges for private IP networks:

10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255

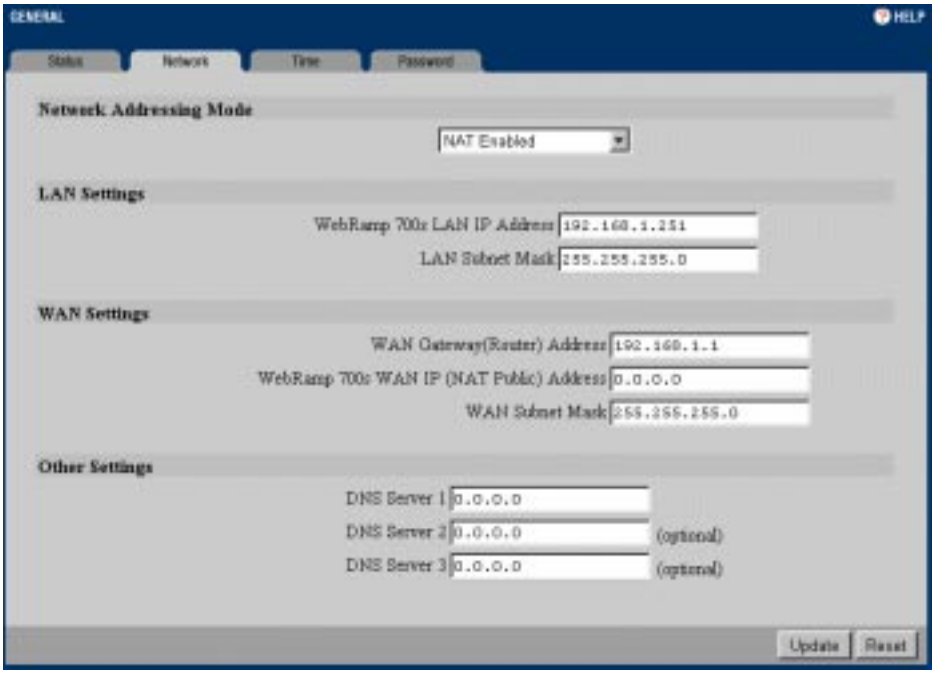
When NAT is enabled, users on the Internet cannot access machines on the LAN unless the computers have been designated as Public LAN Servers. In addition, only one machine per IP protocol is supported as a Public LAN Server. For example, only one machine on the LAN can be accessed using the http (Web) protocol.

One-to-One NAT allows users on the Internet to access machines on the LAN that are "hidden" by NAT. One-to-One NAT also allows access to multiple machines on the LAN over the same IP protocol. For example, **One-to-One NAT** allows an organization to establish a "Web Server Farm" with several machines on the LAN serving Web pages over IP Port 80, or to give authorized users remote access to their office PC. For more information, see One-to-One NAT.

In cases where an address range has arbitrarily been selected, such as where a network uses invalid TCP/IP addresses, Internet sites using that range cannot be accessed from the LAN. For example, if the address range 199.2.23.1-199.2.23.254 is used on the LAN, a Web server on the Internet with the address of 199.2.23.20 will not be accessible.

Select **NAT Enabled** from the **Network Addressing Mode** menu if the network uses private TCP/IP addresses or if addresses are in short supply. A window similar to the following appears.

Figure 3-4 Window with NAT-enabled selected



The following information is required:

LAN Settings

- **The WebRamp 700s LAN IP Address**. This is the IP address assigned to the WebRamp 700s LAN interface and used to access it for configuration and monitoring. Choose a unique IP address from the LAN address range.
- **LAN Subnet Mask**. This value is used to determine what subnet an IP address belongs to. An IP address has two components, the network address and the host address. For example, suppose your enter the IP address 192.168.1.17. Assuming a Class C subnet mask of 255.255.255.0 is used, the first three numbers (192.168.1) represent the Class C network address, and the last number (17) identifies a particular host on this network.

WAN Settings

- **WAN Gateway (Router) Address.** The WAN gateway address is the address of the router that attaches the LAN to the Internet through ISDN, a T1 line, or some other transmission medium.

- **WebRamp 700s WAN IP (NAT Public) Address.** This is the IP address used to access the Internet. It is the only address seen by Internet users and all activity on the Internet from the LAN will seem to originate from this address.
- **WAN Subnet Mask.** The WAN Subnet Mask is used when NAT is enabled.

Other Settings

- **DNS Server**. A DNS server is used by the WebRamp 700s to look up the addresses of machines used to download the Content Filter List and for the built-in DNS Lookup tool. You can enter additional DNS server addresses if available.

Enter the required values and click the **Update** button at the bottom of the screen. When the information has been updated, a confirmation message appears in the status line at the bottom of the window.

NOTE – You must restart the WebRamp 700s for changes to take effect.

When computers on the LAN are using address ranges not in the same subnet as the **NAT Public IP Address**, use the **WebRamp 700s Web Address** as the gateway router address for these computers.

For example, consider the following situation:

- The computers on the LAN have addresses in the private range of 192.168.1.10 to 192.168.1.254.
- The router has the valid Internet address of 128.1.1.1.
- The WebRamp 700s has 128.1.1.25 as the valid Internet address, or **NAT Public IP Address**, and 192.168.1.251 as its **WebRamp 700s Web Address**.

Computers on the LAN require an Internet router address which is in the same subnet. This means that the router address of 128.1.1.1 is invalid for a machine with an address of 192.168.1.10 because the router's address is not within the private range. In this case, use the **WebRamp 700s Web Address** (in this example, 192.168.1.251) as the router for all the machines on the network.

If NAT is active without using addresses in the private range, then using the WebRamp 700s Web Address may not be necessary. For example, if the network was assigned the address range of 199.2.23.1 to 199.2.23.254 by the ISP, NAT is enabled with the public address of 199.2.23.251, and the router address is 199.2.23.1, then the machines on the LAN will not need to be reconfigured because the router address is valid for the subnet.

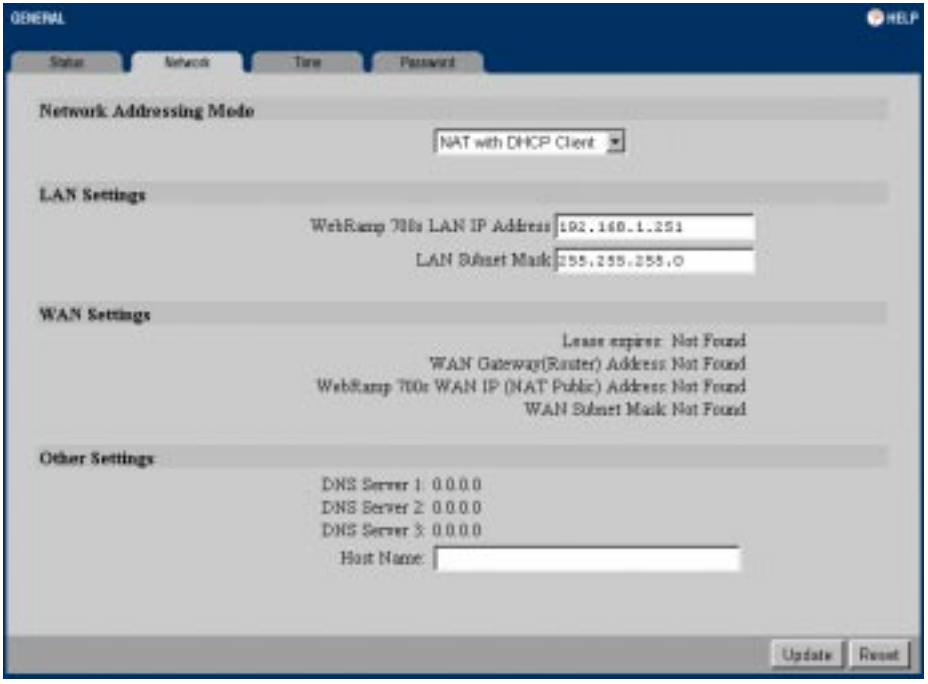
NOTE – NAT and remote access via the Internet are not compatible features because NAT hides the IP addresses of machines on the LAN from the Internet. If NAT is enabled, the only machines on the LAN which can be accessed are those designated as **Public LAN Servers**, which are available to anonymous users on the Internet without authentication.

NAT with DHCP Client

The WebRamp 700s accesses its NAT Public IP address, WAN Router address, and WAN Subnet Mask from a remote DHCP server on the WAN. If a cable modem or xDSL modem is used for the Internet connection, selecting **NAT with DHCP Client** from the **Network Addressing Mode menu.** This selection is required because some cable modems and xDSL ISPs are implementing DHCP in their service.

When you select **NAT with DHCP Client**, a window similar to the following appears.

Figure 3-5 Window with NAT with DHCP client selected



LAN Settings

- **The WebRamp 700s LAN IP Address**. This is the IP address assigned to the WebRamp 700s LAN interface and used to access it for configuration and monitoring. Choose a unique IP address from the LAN address range.
- **LAN Subnet Mask.** This value is used to determine what subnet an IP address belongs to. An IP address has two components, the network address and the host address. For example, suppose you enter the IP address 192.168.1.17. Assuming a Class C subnet mask of 255.255.255.0 is used, the first three numbers (192.168.1) represent the Class C network address, and the last number (17) identifies a particular host on this network.

WAN Settings

- **Lease Expires**. This value indicates when the IP address lease obtained from the DHCP server expires. This value is assigned by the ISP's DHCP server.
- **WAN Gateway (Router) Address.** The WAN router address is assigned by the ISP's DHCP server.
- **WebRamp 700s WAN IP (NAT Public) Address.** This is the IP address used to access the Internet. It is the only address seen by Internet users and all activity on the Internet from the LAN will seem to originate from this address. This value is assigned by the ISP's DHCP server.
- **WAN Subnet Mask.** This value is assigned by the ISP's DHCP server.

Other Settings

- **DNS Server**. A DNS server is used by the WebRamp 700s to look up the addresses of machines used to download the Content Filter List and for the built-in DNS Lookup tool. One or more DNS servers are assigned by the ISP's server.
- **Host Name**. Enter the host name.

Enter the required values and click the **Update** button at the bottom of the screen. When the information has been updated, a confirmation message appears in the status line at the bottom of the window.

NOTE – You must restart the WebRamp 700s for these changes to take effect.

When computers on the LAN are using address ranges not in the same subnet as the **NAT Public IP Address**, the **WebRamp 700s Web Address** is the gateway or router address used by these computers.

For example, consider the following situation:

- The computers on the LAN have addresses in the private range of 192.168.1.10 to 192.168.1.254.
- The router has the valid Internet address of 128.1.1.1.
- The WebRamp 700s has 128.1.1.25 as the valid Internet address, or **NAT Public IP Address**, and uses 192.168.1.251 as the **WebRamp 700s Web Address**.

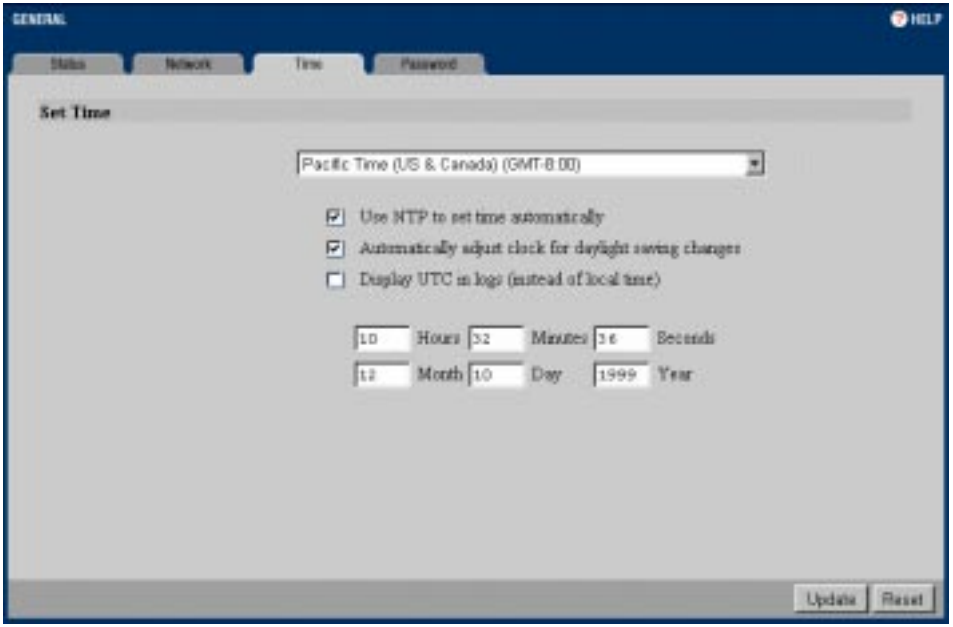
Computers on the LAN require an Internet router address which is in the same subnet. This means that the router address of 128.1.1.1 is invalid for a machine with an address of 192.168.1.10 because the router's address is not within the private range. In this case, use the **WebRamp 700s Web Address** (in this example, 192.168.1.251) as the router for all the machines on the network.

After configuring your WebRamp 700s network settings, you need to restart the WebRamp 700s. See “Restart” for information on restarting the WebRamp 700s.

Set Time

Click the **General** button on the left side of the browser window and then click the **Time** tab at the top of the browser window. A window similar to the following appears.

Figure 3-6 Set Time window



The WebRamp 700s uses the clock to time stamp log events, to automatically update the Content Filter List, and for other internal purposes.

Select the time zone from the pull down menu and click **Use NTP to set time automatically.** This allows the WebRamp 700s to automatically set the local time using Network Time Protocol (NTP).

You can also select to allow automatic adjustments for daylight savings time and to use universal time (UTC) in logs rather than local time.

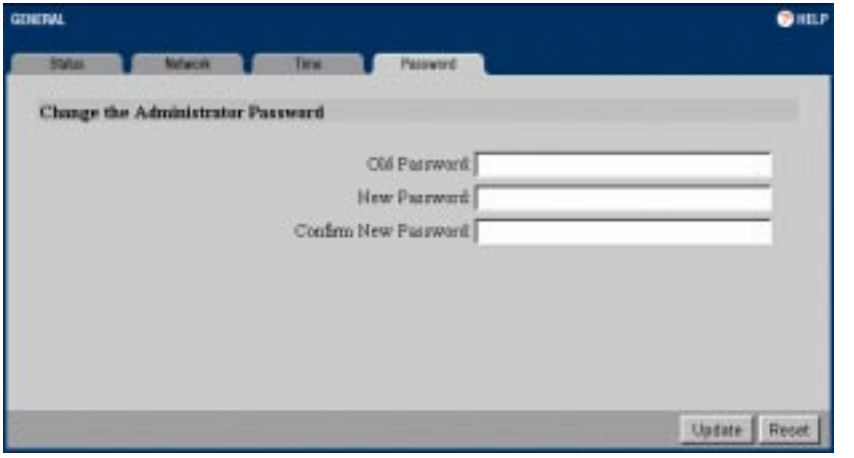
To set the time and date manually, deselect all the check boxes and enter the time (in 24-hour format) and the date.

Click the **Update** button at the bottom of the screen. When the information has been updated, a confirmation message appears in the status line at the bottom of the window.

Password

Click the **General** button on the left side of the browser window and then click the **Password** tab at the top of the browser window. A window similar to the following appears.

Figure 3-7 Password window



The security of the WebRamp 700s is maintained by the use of an Administrator Password. To set this password, enter your current password in the **Old Password** field and then enter a new password in the **New Password** and **Confirm New Password** fields.

Click the **Update** button at the bottom of the screen. When the information has been updated, a confirmation message appears in the status line at the bottom of the window.

NOTE – When setting the password for the first time, remember that the WebRamp 700s is shipped from the factory with the default password set to “password”.

If the password is not entered exactly the same in both **New Password** fields, it is not accepted. Double entry provides protection against mistyping a password and being accidentally locked out of the WebRamp 700s.

NOTE – The password can’t be recovered if it is lost or forgotten. If the password is lost, the WebRamp 700s must be reset to its factory default state. Contact Ramp Network’s Technical Support team for instructions.

Log

The WebRamp 700s allows you to create an activity log and set up different types of alerts. The WebRamp 700s maintains an event log containing events that may be security concerns and alerts you of potential attacks.

The event log can be viewed with your browser using the WebRamp 700s web management interface. For convenience and archival purposes it can also be sent automatically as a tab-delimited text file to any e-mail address. You can set the intervals for automatic e-mail delivery.

In some cases, you may want to be alerted of high-priority information, such as an attack on a server. In such cases, the alert can be sent immediately to the main e-mail address used by the log, or to a different address, such as a paging service.

The following events are logged by the WebRamp 700s:

- Unauthorized connection attempts
- Blocked Web, FTP and Gopher sites, and blocked NNTP Newsgroups
- Blocked ActiveX and Java
- Blocked Cookies and Proxy attempts
- Attacks such as IP spoofing, Ping of death, SYN flood
- Administrator logins
- Successful or unsuccessful loading of the Content Filter List

NOTE – You may wish to carefully monitor the log or you might want to be notified only in the case of important events. If maintaining complete log information is of critical importance, connect the WebRamp 700s to an uninterruptable power supply (UPS) to protect the log information which might be lost during power interruptions.

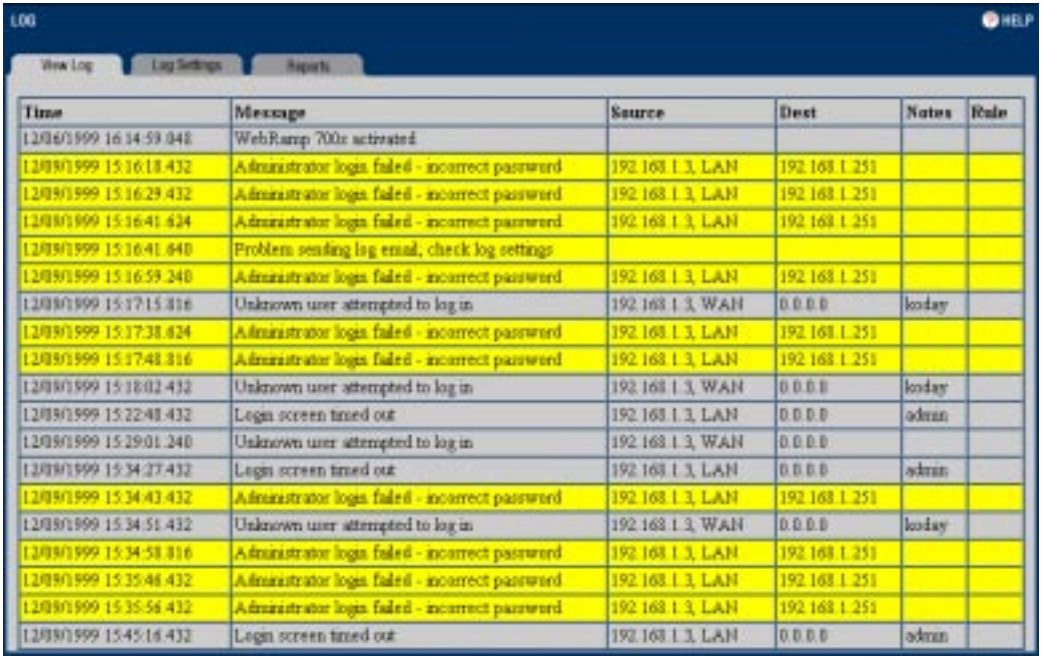
View Log

The log is displayed as a list in a table, but may appear differently when viewed with various browsers. It may be necessary to adjust the browser's font size and other viewing characteristics to improve the readability of the log data. Depending on your browser, you may be able to copy entries from the log and paste them into documents. If cut and paste are disabled, use the **E-mail Log** option and review the log using an e-mail client. Set the **E-mail Log** by clicking **Log Settings** and filling in the appropriate fields.

Each log entry contains the date and time of the event and a brief message. Some entries contain additional information. Much of this information refers to the Internet traffic passing through the WebRamp 700s.

Click the **Log** button on the left side of the browser window and then click the **View Log** tab at the top of the window. A window similar to the following appears.

Figure 3-8 View Log window



Time	Message	Source	Dest	Notes	Rule
12/30/1999 16:14:59.848	WebRamp 700x activated				
12/30/1999 15:16:18.432	Administrator login failed - incorrect password	192.168.1.3, LAN	192.168.1.251		
12/30/1999 15:16:29.432	Administrator login failed - incorrect password	192.168.1.3, LAN	192.168.1.251		
12/30/1999 15:16:41.624	Administrator login failed - incorrect password	192.168.1.3, LAN	192.168.1.251		
12/30/1999 15:16:41.640	Problem sending log email; check log settings				
12/30/1999 15:16:59.240	Administrator login failed - incorrect password	192.168.1.3, LAN	192.168.1.251		
12/30/1999 15:17:15.816	Unknown user attempted to log in	192.168.1.3, WAN	0.0.0.0	kodiay	
12/30/1999 15:17:31.624	Administrator login failed - incorrect password	192.168.1.3, LAN	192.168.1.251		
12/30/1999 15:17:48.816	Administrator login failed - incorrect password	192.168.1.3, LAN	192.168.1.251		
12/30/1999 15:18:02.432	Unknown user attempted to log in	192.168.1.3, WAN	0.0.0.0	kodiay	
12/30/1999 15:22:48.432	Login screen timed out	192.168.1.3, LAN	0.0.0.0	admin	
12/30/1999 15:29:01.240	Unknown user attempted to log in	192.168.1.3, WAN	0.0.0.0		
12/30/1999 15:34:27.432	Login screen timed out	192.168.1.3, LAN	0.0.0.0	admin	
12/30/1999 15:34:43.432	Administrator login failed - incorrect password	192.168.1.3, LAN	192.168.1.251		
12/30/1999 15:34:51.432	Unknown user attempted to log in	192.168.1.3, WAN	0.0.0.0	kodiay	
12/30/1999 15:34:58.816	Administrator login failed - incorrect password	192.168.1.3, LAN	192.168.1.251		
12/30/1999 15:35:46.432	Administrator login failed - incorrect password	192.168.1.3, LAN	192.168.1.251		
12/30/1999 15:35:56.432	Administrator login failed - incorrect password	192.168.1.3, LAN	192.168.1.251		
12/30/1999 15:45:16.432	Login screen timed out	192.168.1.3, LAN	0.0.0.0	admin	

Time

The date and time of each event appears as an entry in the view log window.

Message

A description of each event appears in the **Message** field.

TCP, UDP, or ICMP packets dropped. These log messages describe all traffic blocked from the Internet to the LAN. The source and destination IP addresses of the packet are shown. If the packet was TCP or UDP, the port number, in parentheses, follows each address. If the packet was CMP, the number in

parentheses is the ICMP code. The address information is usually preceded by the name of the service described by either the TCP or UDP port, or the ICMP type in quotation marks.

Web, FTP, Gopher, or Newsgroup blocked. The LAN IP and Ethernet addresses of the machine that attempted to connect to the blocked site or newsgroup are displayed. In most cases, the name of the blocked site is also shown.

ActiveX, Java, or Code Archive blocked. The IP addresses of the source machine and the destination server is shown.

NOTE – When ActiveX or Java code is compressed into an archive it is not always possible to differentiate between the two. If either ActiveX or Java blocking is turned on, all code archives are blocked.

Cookie blocked. The IP addresses of the local machine and the remote server is shown.

Ping of Death, IP Spoof, and SYN Flood Attacks. The IP address of the destination machine which may be under attack, as well as the source address which appears in the packet, is shown. In these attacks, the source address is usually fake and cannot be used to determine the source of the attack.

NOTE – Varying conditions on the Internet can produce situations which may appear to be attacks, even when no one is deliberately attacking one of the machines on the LAN. This is particularly true for SYN Flood attacks. If the log message labels the attack “possible”, or if it happens on an irregular basis, then there is probably no attack in progress. If the log message labels the attack “probable”, contact the ISP to see if they can track down the source of the attack. In either case, the LAN is protected and no further action is required.

Source and Dest

The IP addresses of the source machine and the destination server are shown in the **Source** and **Dest** fields of the **View Log** window.

Notes

Additional information about an event, such as the user login, appears in the **Notes** field.

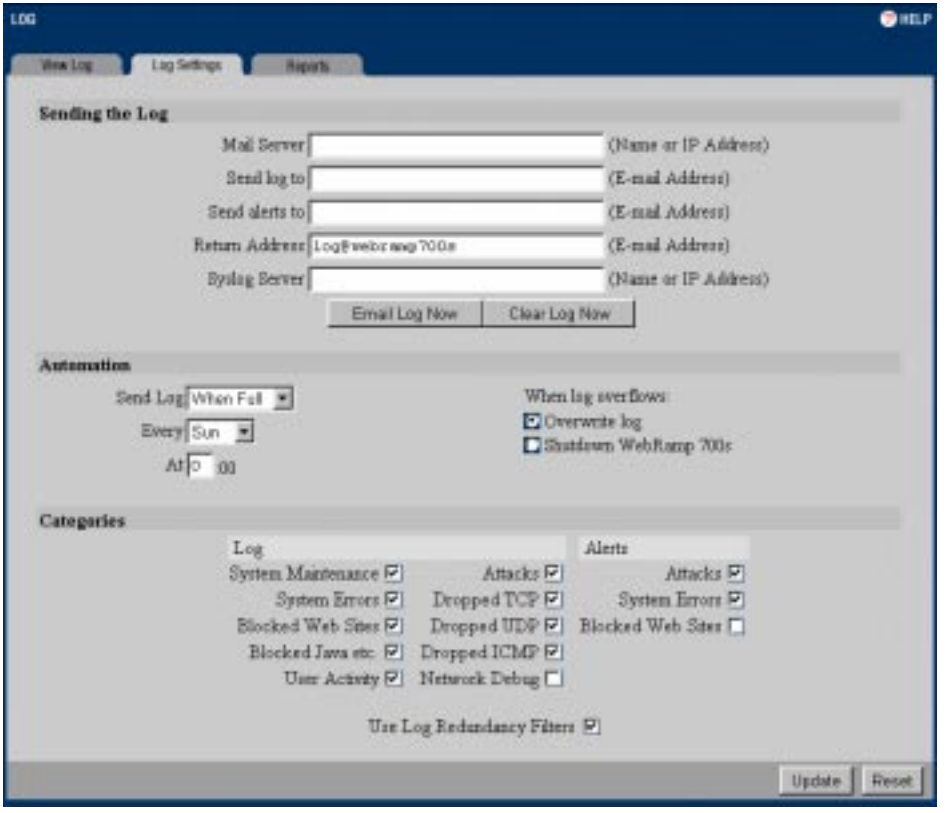
Rule

The Rule field contains a list of rules affected by an event. See ***Access*** for additional information on defining network access rules.

Log Settings

The **Log Settings** window allows you to define where a generated log will be sent. Click the **Log** button on the left side of the browser window and then click the **Log Settings** tab at the top of the window. A window similar to the following appears.

Figure 3-9 Log Settings window



Sending the Log

Enter the following server and e-mail account information:

Mail Server. Enter the numerical TCP/IP address of the SMTP server you want to use to send log or alert messages via e-mail. Your ISP can provide this information. If you leave this field blank, log and alert messages are not sent via e-mail. Use the **DNS Lookup** utility under the **Tools** button to find the IP address of the mail server. See DNS Name Lookup. The Internet has a service called the Domain Name Service (DNS) which allows users to enter an easily remembered host name, such as www.rampnet.com, instead of numerical TCP/IP addresses to access Internet resources. Unfortunately, this service can easily be attacked to confuse the LAN and open security holes. For this reason, the WebRamp 700s requires numerical TCP/IP addresses to be entered in address fields which are used in the firewall function. The WebRamp 700s has a DNS lookup tool which returns the numerical TCP/IP address of a host name.

Send Log To. Enter the fully qualified address (username@mydomain.com) of the e-mail address you want to receive the log messages. After the log is sent, the log file is cleared from the memory of the WebRamp 700s. If you leave this field blank, log messages are not sent via e-mail. The WebRamp 700s checks to see if new software is available for download from Ramp Network's FTP site on a weekly basis. If there is a new software release, an e-mail notification is sent to this address.

Send Alerts To. Alerts are events, such as an attack, which may warrant immediate attention. When an event generates an alert, a message is immediately sent to a specified e-mail address. Enter the fully qualified address (username@mydomain.com) for alert notification. This can be a standard e-mail account or a paging service. If your leave this field blank, alert messages are not sent via e-mail.

Return Address. Enter the e-mail address you want to use as the return address for all log and alert messages. The return address serves two purposes. First, if the mail server uses SPAM filtering, a valid address may be required for mail to be delivered. Second, organizations with multiple WebRamp 700s units can use different e-mail addresses to identify the source of the message. The default entry is "log@webramp700s" and will need to be changed to a valid e-mail address.

Syslog Server. In addition to the standard screen log, the WebRamp 700s can write extremely detailed event log information to an external Syslog server. (Syslog is an industry standard protocol used for capturing log information for devices on a network.) The WebRamp 700s Syslog captures all screen log activity, plus every connection's source and destination IP addresses, IP service, and number of bytes transferred. The WebRamp 700s Syslog support requires an external server running a Syslog daemon on UDP Port 153.

Syslog is a standard feature of UNIX. Links to download shareware and freeware Syslog daemons for Windows and MacOS can be found at *www.rampnet.com/support/700s/faq.html*.

Enter the Syslog server's IP address in the **Syslog Server** field.

E-mail Log Now. Immediately sends the log to the address in the **Send Log To** field and then clears the log.

Clear Log Now. Deletes the contents of the log.

Automation

Enter the following information to automatically send an e-mail log:

Send Log. This menu specifies when to send e-mail log messages: daily, weekly, or only when the log is full. If you select the daily option, specify a time. If you select the weekly option, specify a day of the week and a time. If you have selected the weekly or daily option and the log fills up, it is automatically e-mailed to the **Send Log To** address and cleared.

When log overflows. In some cases, the log buffer may fill up, for example, there may be a problem with the mail server that prevents the log from being e-mailed. When there is overflow, the default option is to overwrite the log, discarding its contents. You can choose instead to have the WebRamp 700s shut down, which prevents any further traffic from traveling through without being logged.

Categories

Select the log and alert messages you wish to have generated.

Log. Click the checkbox to set the following log message categories:

- **System Maintenance.** When selected, generates log messages showing general system maintenance activity, such as administrator logins, automatic loading of Content Filter Lists, activation and restarting the WebRamp 700s. On by default.
- **System Errors.** When selected, generates log messages showing problems with DNS, e-mail, and automatic Content Filter List loading. On by default.
- **Blocked Web Sites.** When selected, generates log messages showing Web sites, newsgroups, or other services blocked by the Content Filter List, by keywords, or for any other reason. On by default.

- **Blocked Java, and so on.** When selected, generates log messages showing Java, ActiveX, and Cookies which are blocked by the WebRamp 700s. On by default.
- **User Activity.** When selected, generates log messages showing any successful or unsuccessful user logins. On by default.
- **Attacks.** When selected, generates log messages showing SYN Floods, Ping of Death, IP Spoofing, and attempts to manage the WebRamp 700s from the Internet. On by default.
- **Dropped TCP.** When selected, generates log messages showing blocked incoming TCP connections. On by default.
- **Dropped UDP.** When selected, generates log messages showing blocked incoming UDP packets. On by default.
- **Dropped ICMP.** When selected, generates log messages showing blocked incoming ICMP packets. On by default.
- **Network Debug.** When selected, generates log messages showing Ethernet broadcasts, ARP resolution problems, ICMP redirection problems, and NAT resolution problems. This category is intended for experienced network administrators. Off by default.

Alerts. Alerts are events, such as an attack, which may warrant immediate attention. When an event generates an alert, a message is immediately sent to the e-mail account defined in the Send alerts to field on the Log Settings window.

- **Attacks.** When selected, generates an alert message for all log entries that are categorized as an **Attack**. On by default.
- **System Errors.** When selected, generates an alert message for all log entries that are categorized as a System Error. On by default.
- **Blocked Web Sites.** When selected, generates an alert message for all log entries that are categorized as a Blocked Web Site. Off by default.

Use Log Redundancy Filters. This option prevents the generation of duplicate consecutive log messages. Because of network retry mechanisms, duplicate consecutive messages are common. If the **Use Log Redundancy Filters** box is checked, a log entry identical to the previous entry is not generated.

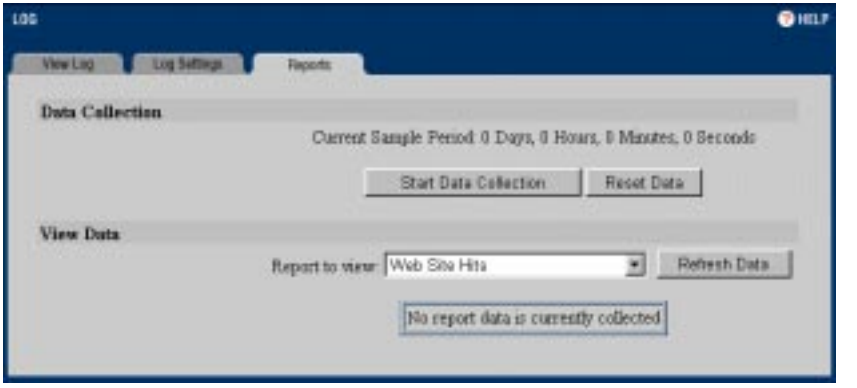
When you've finished editing the **Log Settings**, click the **Update** button at the bottom of the screen. When the information has been updated, a confirmation message appears in the status line at the bottom of the window.

Reports

The WebRamp 700s is able to perform a rolling analysis of the event log to show the top 25 most accessed Web sites, the top 25 users of bandwidth by IP address, and the top 25 services that consume the most bandwidth.

Click the **Log** button on the left side of the browser window and then click the **Reports** tab at the top of the window. A window similar to the following appears.

Figure 3-10 Reports window



Data Collection

The WebRamp 700s allows collection of data.

Current Sample Period. Displays the current sample period.

Start Data Collection. By default, log analysis is turned off. Click the **Start Data Collection** button to begin log analysis. (When log analysis is turned on, this button reads **Stop Data Collection**.)

Reset Data. Click the **Reset** button to clear the report statistics and begin a new sample period. The sample period is also reset when data collection is stopped or started and when the WebRamp 700s is restarted.

View Data

This field allows you to define how log information is viewed.

Report to View. Select the desired report from the Report to view menu:

- **Web Site Hits** displays a table showing the URL for the 25 most often accessed Web sites and the number of hits to those sites during the current sample period. Use this report to help determine if the majority of Web access is to sites considered applicable to your primary business function. If leisure, sports, or other similar sites are on this list, it may signal the need to change or more strictly enforce your organization's Acceptable Use Policy.
- **Bandwidth Usage by IP Address** displays a table showing the IP Address of the 25 top users of Internet bandwidth and the number of megabytes transmitted during the current sample period.

NOTE – If you're using DHCP, remember that the IP address assigned to a computer can change. It may be necessary to check the DHCP server logs to correctly identify which computer is listed in the report.

- **Bandwidth Usage by Service** displays a table showing the name of the 25 top Internet services, such as HTTP, FTP, RealAudio, and so on during the current sample period. Use this report to help you determine if the Internet services being used are appropriate for your organization. If services such as video or push broadcasts are consuming a large portion of the available bandwidth, it may signal the need to change or more strictly enforce your organization's Acceptable Use Policy.

Refresh Data. Click **Refresh Data** to refresh the data.

Filter

The **Filter** window allows you to set up content filtering and blocking.

NOTE – Content Filtering only applies to nodes on the LAN Port.

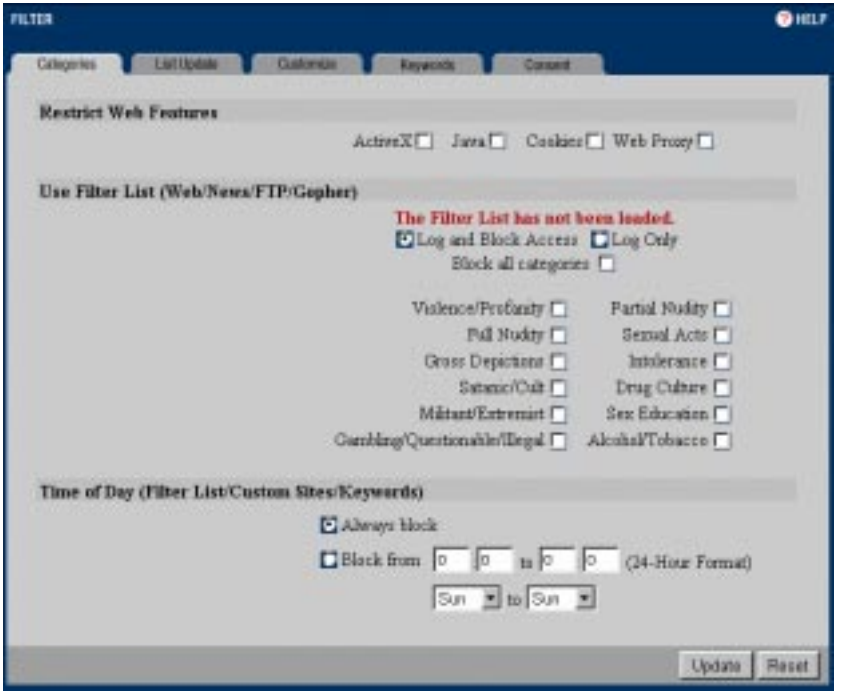
Categories

From the **Categories** window you select the options you want to include in your content filtering and blocking. The options are grouped into three main categories:

- Restrict Web Features
- Use Filter List (Web/News/FTP/Gopher)
- Time of Day (Filter List/Custom Sites/Keywords)

Click the **Filter** button on the left side of the browser window and then click the **Categories** tab at the top of the window. A window similar to the following appears.

Figure 3-11 Categories window



Restrict Web Features

ActiveX. ActiveX is a programming language used to embed small programs in Web pages. It is generally considered an insecure protocol since it is possible for malicious programmers to write controls that can delete files, compromise security, or cause other damage.

Java. Java is also used to embed small programs (known as *applets*) in Web pages. It is generally considered safer than ActiveX since it has more safety mechanisms. You may choose, however, to filter out Java since there have been instances of bugs in these safety mechanisms.

Cookies. Cookies are used by Web servers to track usage. Cookies result in a more user-friendly Web by providing service based on ID. Unfortunately, cookies can be programmed not only to identify the visitor to a site, but also to track that visitor's activities. Because they represent a potential loss of privacy, you may choose to block cookies.

Web Proxy. When a proxy server is located on the WAN, it is possible for LAN users to circumvent content filtering by pointing to this proxy server. This option eliminates access to proxy servers located on the WAN. It has no effect on proxy servers located on the LAN. For example, a user on the LAN could configure their Web browser to point to one of the many public Web proxies on the Internet. When that user requests a Web page, their Web browser formats the request for the proxy server, hiding it from the content filter. As a result, the user is able to access unfiltered content on the Internet.

Use Filter List

The Content Filter List blocks access to sites which fall within specific categories. The WebRamp 700s uses a Content Filter List that is managed by The Learning Company's CyberNOT Oversight Committee. This committee is made up of members from a wide range of social, political, and civic organizations, including the National Association for the Advancement of Colored People (NAACP), the Gay and Lesbian Alliance Against Defamation (GLAAD), Morality in Media, women's rights groups, the teacher's union, as well as a superintendent of schools, a social worker, a psychologist, and a minister. When you register the WebRamp 700s, you automatically receive a one-month subscription to the Content Filter List updates.

Log and Block Access. When selected, logs the attempt and blocks access to all the sites on the Content Filter, Custom Sites, and Keyword lists.

Log Only. When selected, logs and then allows access to all sites on the Content Filter, Custom Sites, and Keyword lists. This options lets you monitor appropriate usage without restricting access.

Block all Categories. When selected, blocks access to sites in all the categories.

Following is a list of the Content Filter categories:

- **Violence/Profanity (graphics or text).** Pictures or text exposing extreme cruelty, or physical or emotional acts against any animal or person which are primarily intended to hurt or inflict pain. Obscene words, phrases, and

profanity are defined as text that uses, but is not limited to, censored words more often than once every 50 messages (Newsgroups) or once a page (Web sites).

- **Partial Nudity.** Pictures exposing the female breast or full exposure of either male or female buttocks except when exposing genitalia. (Excludes all swimsuits, including thongs.)
- **Full Nudity.** Pictures exposing any or all portions of the human genitalia. Excluded from the Partial Nudity and Full Nudity categories are sites containing nudity or partial nudity of a wholesome nature. For example: Web sites containing publications such as National Geographic or Smithsonian Magazine. Or sites hosted by museums such as the Guggenheim, the Louvre, or the Museum of Modern Art.
- **Sexual Acts (graphics or text).** Pictures or text exposing anyone or anything involved in explicit sexual acts and or lewd and lascivious behavior, including masturbation, copulation, pedophilia, and intimacy involving nude or partially nude people in heterosexual, bisexual, lesbian or homosexual encounters. Also includes phone sex ads, dating services, and adult personals, CD-ROMs, and videos.
- **Gross Depictions (graphics or text).** Pictures or descriptive text of anyone or anything which are crudely vulgar or grossly deficient in civility or behavior, or which show scatological impropriety. Includes such depictions as maiming, bloody figures, or indecent depiction of bodily functions.
- **Intolerance (graphics or text).** Pictures or text advocating prejudice or discrimination against any race, color, national origin, religion, disability or handicap, gender, or sexual orientation. Any picture or text that elevates one group over another. Also includes intolerant jokes or slurs.
- **Satanic/Cult (graphics or text).** Pictures or text advocating devil worship, an affinity for evil or wickedness, or the advocacy to join a cult. A cult is defined as: a closed society that is headed by a single individual where loyalty is demanded and leaving is punishable.
- **Drug Culture (graphics or text).** Pictures or text advocating the illegal use of drugs for entertainment. Includes substances used for other than their primary purpose to alter the individual's state of mind, such as glue sniffing. This would exclude currently illegal drugs legally prescribed for medicinal purposes (e.g., drugs used to treat glaucoma or cancer).
- **Militant/Extremist (graphics or text).** Pictures or text advocating extremely aggressive and combative behaviors, or advocacy of unlawful political measures. Topics include groups that advocate violence as a means to achieve

their goals. Includes “how to” information on weapons making, ammunition making, or the making or use of pyrotechnics materials. Also includes the use of weapons for unlawful reasons.

- **Sex Education (graphics or text).** Pictures or text advocating the proper use of contraceptives. This topic would include condom use, the correct way to wear a condom and how to put a condom in place. Also included are sites relating to discussion about the use of the Pill, IUD’s, and other types of contraceptives. In addition to the above, this category will include discussion sites on discussing diseases with a partner, pregnancy, and respecting boundaries. Excluded from this category are commercial sites wishing to sell sexual paraphernalia.
- **Gambling/Questionable/Illegal.** Pictures or text advocating materials or activities of a dubious nature which may be illegal in any or all jurisdictions, such as illegal business schemes, chain letters, copyright infringement, computer hacking, phreaking (using someone’s phone lines without permission), and software piracy. Also includes text advocating gambling relating to lotteries, casinos, betting, numbers games, on-line sports, or financial betting, including non-monetary dares.
- **Alcohol & Tobacco.** Pictures or text advocating the sale, consumption, or production of alcoholic beverages and tobacco products.

Time of Day

Time of Day allows you to define the time periods during which Content Filtering is in effect. For example, Content Filtering could be turned on in a school during normal school hours to protect students, but turned off after hours to give teachers complete access to the Internet. Similar time restraints could be set to allow employees complete access to the Internet after normal business hours.

NOTE – Time of Day restrictions only apply to the Content Filter, Custom Sites, and Keywords. Consent and Restrict Web Features, such as ActiveX, Java, Cookies and Web Proxy are not affected.

Always Block. When selected, Content Filtering is always active and Time of Day limitations are not enforced. On by default.

Block from...to. When selected, Content Filtering is only active during the time interval and days specified. Enter the time period (in 24-hour format) and select the starting and ending day of the week that Content Filtering will be enforced.

List Update

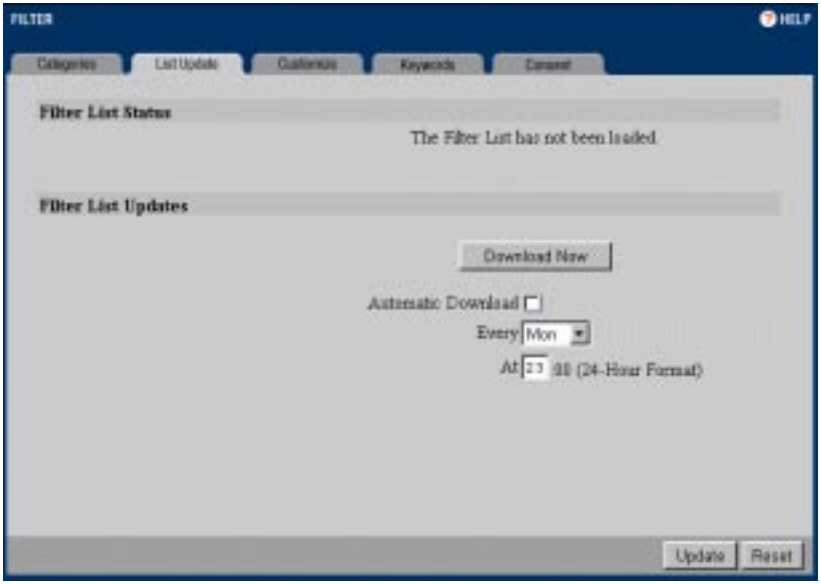
Since content on the Internet is constantly changing, the Content Filter List should be updated on a weekly basis. List subscriptions are available; please contact Ramp Networks Sales for information. The WebRamp 700s can automatically load new lists every week.

Registering the WebRamp 700s with Ramp Networks allows you to install and activate the Content Filter List and to receive a one month subscription to updated Content Filter Lists at no charge.

NOTE – Host names, and not TCP/IP addresses, are used for all filtering operations because many blocked sites operate server pools, where many machines service a single host name, making it impractical and difficult to add and maintain the numerical addresses of every server in the pool. Host names are also used because many sites included in the Content Filter List regularly change their IP server address to try to bypass the Content Filter Lists. This makes maintaining a current list subscription critical for effective content filtering.

Click the **Filter** button on the left side of the browser window and then click the **List Update** tab at the top of the window. A window similar to the following appears.

Figure 3-12 List Update window



Filter List Status

The **Filter List Status** displays information about the currently loaded Content Filter List. The creation date of the current active list is displayed at the top of the window.

Filter List Updates

Select from the following update options:

Download Now. Click this button to immediately download and install a new Content Filter List. This process requires a current subscription to the Content Filter List updates and may take a couple of minutes, depending on Internet traffic conditions. Since it is necessary to restart the WebRamp 700s once the download is complete, it's a good idea to download new lists when LAN access to the Internet is at a minimum.

Automatic Download. Check this box to set automatic, weekly downloads of the Content Filter List. Select the day of the week and the time of the day for the download. A current subscription to the Content Filter List updates is required.

Since the WebRamp 700s is automatically restarted when the new list is installed, it's a good idea to choose a day and time when LAN access to the Internet is at a minimum.

Click the **Update** button at the bottom of the screen. When the information has been updated, a confirmation message appears in the status line at the bottom of the window.

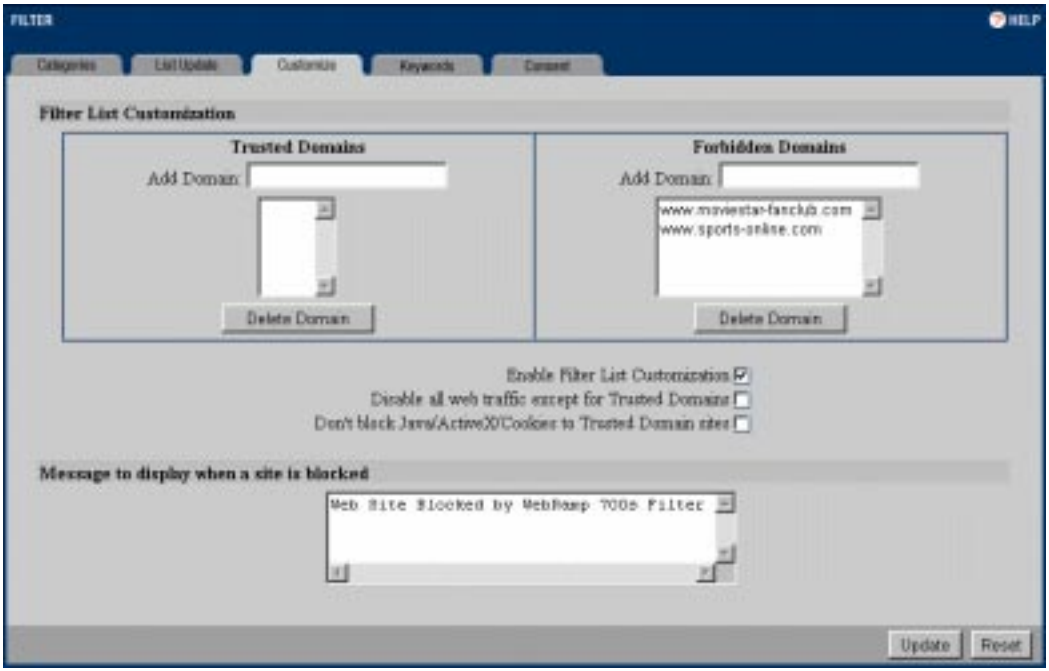
NOTE – The WebRamp 700s does not ship with the Content Filter List installed. Registering WebRamp 700s with Ramp Networks installs the current Content Filter List and allows automatic updates during the 30 day evaluation, as well as during the term of any optional Content Filter List subscription you may purchase. Because of the rapid changes on the Internet, Content Filter Lists expire after 30 days. Once expired, a new Content Filter List must be installed to continue filtering content specified on the Content Filter List.

Customize

The WebRamp 700s allows you to customize the Content Filter List by adding or removing sites. For example, if a local radio station runs a contest on its Web site that is disrupting normal classroom Internet use, you can block access to that site. Or, you may want to block sites that appear on the **Top Web Site Hits** from the **Log Report** which are not objectionable, but are considered an inappropriate use of the Internet connection. For example, if sites such as "www.sports-online.com" or "www.moviestar-fanclub.com" frequently appear as a top Web attraction and offer no value, you can deny access to those sites.

Click the **Filter** button on the left side of the browser window and then click the **Customize** tab at the top of the window. A window similar to the following appears.

Figure 3-13 Customize window



Filter List Customization

Customize access to web sites using the **Trusted Domain** and **Forbidden Domain** features.

Trusted and Forbidden Domains. To allow access to a Web site which appears in the Content Filter List, enter its host name, such as “www.ok-site.com” in the Trusted Domains text field. Do not enter the complete URL of the site, that is, do not include “http://”. All subdomains will be allowed. For example, entering “yahoo.com” also allows “www.yahoo.com”, “my.yahoo.com”, “sports.yahoo.com”, and so on. You can enter up to 256 entries in the Trusted Domains list.When you have finished editing the Trusted Domains list, click the Update button at the bottom of the screen. When the information has been updated, a confirmation message appears in the status line at the bottom of the window.

To remove a site from the **Trusted Domains List**, select its name and click the **Delete Domain** button. Users will no longer be able to access that site from the LAN.

To block access to a Web site which does not appear in the Content Filter List, enter its host name, such as “www.bad-site.com” in the **Forbidden Domains** text field. Do not enter the complete URL of the site, that is, do not include “http://”. All subdomains will be blocked. For example, entering “yahoo.com” also blocks “www.yahoo.com”, “my.yahoo.com”, “sports.yahoo.com”. You can enter up to 256 entries in the **Forbidden Domains** list. When you have finished editing the **Forbidden Domains** list, click the **Update** button at the bottom of the screen. When the information has been updated, a confirmation message appears in the status line at the bottom of the window.

To remove a site from the **Forbidden Domains List**, select its name and click the **Delete Domain** button. Once the domain has been deleted, users will no longer be able to access that site from the LAN.

- **Enable Content Filter List Customization**. To deactivate the Content Filter List Customization option, deselect the **Enable Content Filter List Customization** checkbox and then click the **Update** button. Content Filter List Customization can be turned on and off without re-entering all site names, does not have to be re-entered when the Content Filter List is updated, and does not expire.
- **Disable web traffic except for Trusted Domains**. When the **Disable all web traffic except for Trusted Domains** box is selected, the WebRamp 700s only allows access to web sites on the Trusted Domains list. With careful screening, this can be close to 100% effective at blocking pornography and other objectionable material.
- **Don’t block Java/ActiveX/Cookies to Trusted Domain sites**. When this option is selected, the WebRamp 700s permits Java, ActiveX and Cookies from sites on the **Trusted Domains** list. In certain cases, it may be desirable to allow Java, ActiveX or Cookies from sites that are known and trusted. For example, blocking Cookies requires users to reconfigure My Yahoo (or any other site that uses Cookies to customize its content) each time they visit the site.

Message to display when a site is blocked

When a user attempts to access a site blocked by the WebRamp 700s Content Filter List, they see the message entered in this box. The default message is “Web Site Blocked by the WebRamp 700s Filter”. Any message of up to 255 characters (including embedded HTML) can be entered in this screen.

For example, entering the following will display a descriptive message explaining why the site was blocked, with links to the Acceptable Use Policy and the Network Administrator’s e-mail address:

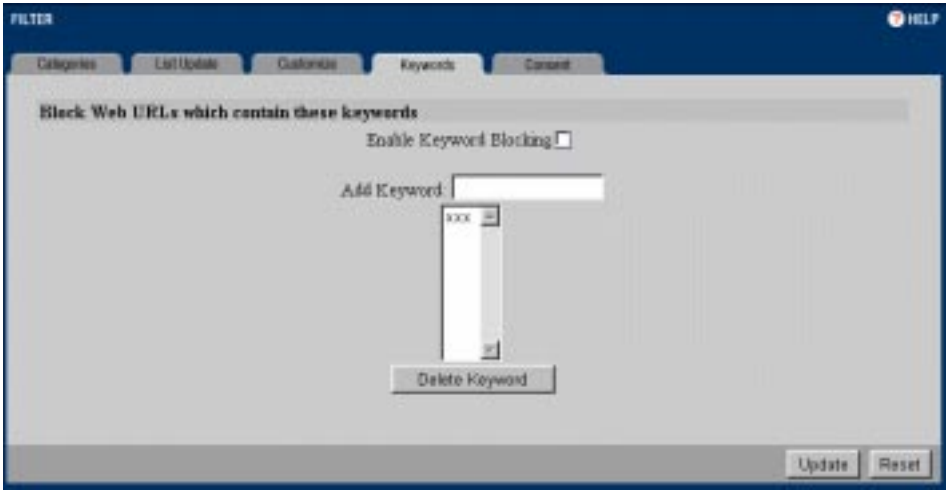
Access to this site was denied because it appears to violate this organization's <A HREF=http://www.your-domain.com/acceptable_use_policy.htm>Acceptable Use Policy</A>. Please contact the <A HREF="mailto:admin@your-domain.com">Network Administrator</A> if you feel this was in error.

Keywords

The WebRamp 700s allows you to block URLs containing keywords. This functions as a second line of defense against objectionable material. For example, if the keyword "XXX" is entered, the pornographic site www.new-site.com/xxx.html would be blocked, even if it were not included in the Content Filter List.

Click the **Filter** button on the left side of the browser window and then click the **Keywords** tab at the top of the window. A window similar to the following appears.

Figure 3-14 Keywords window



NOTE – It is important to use caution when enabling this feature. For example, blocking the word "breast" may stop access to objectionable or pornographic sites, but it would also block access to sites on breast cancer.

To use this option, select the **Enable Keyword Blocking** option and then click the **Update** button at the bottom of the screen. When the information has been updated, a confirmation message appears in the status line at the bottom of the window.

Enter the keyword to block in the **Add Keyword** field and click the **Update** button at the bottom of the screen. When the information has been updated, a confirmation message appears in the status line at the bottom of the window. The keyword then appears in the keyword list.

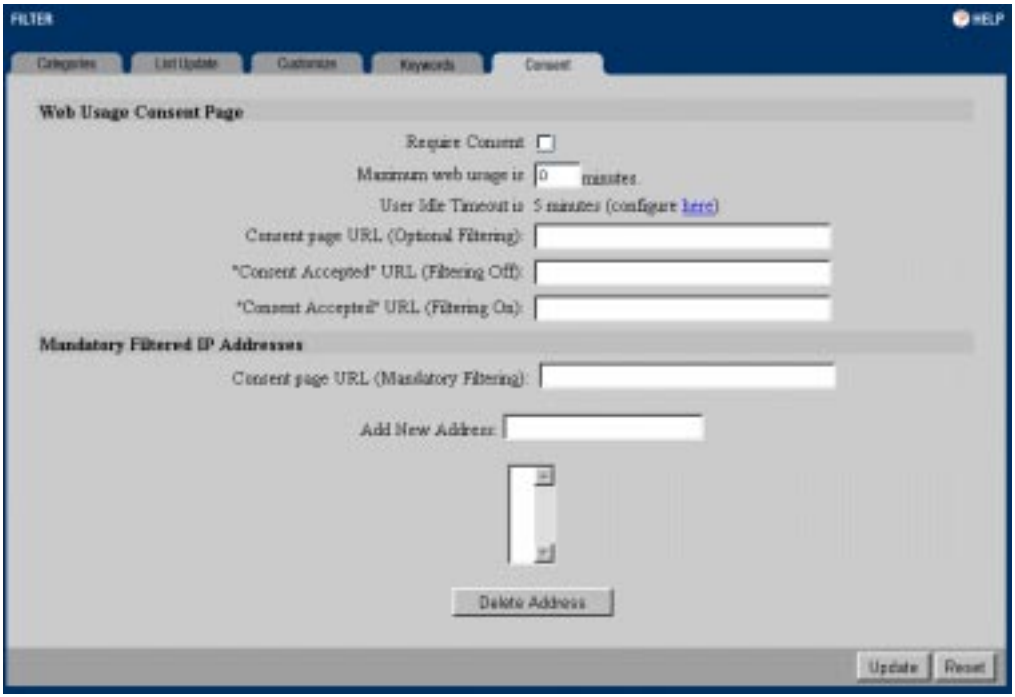
To remove a keyword, select the keyword to be removed from the list and click the **Delete Keyword** button. The operation takes a few seconds. When completed, a confirmation message appears in the status line at the bottom of the window.

Consent

Consent allows you to specify which computers are always filtered and which are filtered only when the user requests such protection. You can also set up Consent so that users are required to agree to the terms outlined in your organization's Acceptable Use Policy before they can continue browsing the Web.

Click the **Filter** button on the left side of the browser window and then click the **Consent** tab at the top of the window. A window similar to the following appears**.**

Figure 3-15 Consent window



Web Usage Consent Page

In an environment where there are more users than computers, such as a classroom or library, you may wish to impose time limits on web usage

Require Consent. Select this option to activate the **Consent** options.

Maximum Web Usage Is. Enter the time limit, in minutes, in this field. If you leave this field at the zero (0) default value, there are no time limits.

User Idle Timeout. After a period of inactivity, the WebRamp 700s requires users to agree to the terms outlined in the consent page before they can continue browsing the web. To set this value, click the link to the **Users** window and enter the time in the **Idle Timeout** field.

Consent page URL (Optional Filtering). When a user begins an Internet session on a computer that is not always filtered, they see a consent page and are given the option to access the Internet with or without content filtering. You create this page in HTML. It may contain the text of or links to the **Acceptable Use Policy (AUP)**.

NOTE – A separate Web server is required to host the consent page and the AUP. The IP address must point to that server, not to the WebRamp 700s.

The page must also contain links to the pages that define if filtering is turned on or off. The link for unfiltered access must be *IP address/filename.html*. The link for filtered access must be *IP address/filename.html*.

"Consent Accepted" URL (Filtering Off). When a user accepts the terms outlined in the consent page and chooses to access the Internet without Content Filtering, they are shown a page which confirms their selection. You create this page. Enter the URL of this page in the **"Consent Accepted" (Filtering Off)** field. This page must reside on a Web server and be accessible as a URL by users on the LAN.

"Consent Accepted" URL (Filtering On). When a user accepts the terms outlined in the consent page and chooses to access the Internet with Content Filtering on, they are shown a page which confirms their selection. You create this page. Enter the URL of this page in the **"Consent Accepted" (Filtering On)** field. This page must reside on a Web server and be accessible as a URL by users on the LAN.

Mandatory Filtered IP Addresses

Enter the following information to specify mandatory filtering for specific addresses on the LAN:

Consent page URL (Mandatory Filtering). When a user begins an Internet session on a computer where content filtering is mandatory, they are shown a consent page that you create in HTML. This file may contain the text from the **Acceptable Use Policy** and notification that violations of the **AUP** will be blocked and logged. This page must reside on a Web server and be accessible as a URL by users on the LAN.

This page must also contain a link to a page that defines that the user agrees to have filtering on. The link must be *IP address/filename.html*.

Enter the URL of this page in the **Consent page URL (Mandatory Filtering)** field and click the **Update** button at the bottom of the screen. When the information has been updated, a confirmation message appears in the status line at the bottom of the window.

Add New Address. The WebRamp 700s can be configured to always provide content filtering for certain computers on the LAN. Enter the IP addresses of these computers in the **Add New Address** field and click the **Update** button. You can enter up to 128 IP addresses.

Delete Address. To remove a computer from the list of filtered computers, select the IP address in the **Mandatory Filtered IP Addresses** list and click the **Delete Address** button.

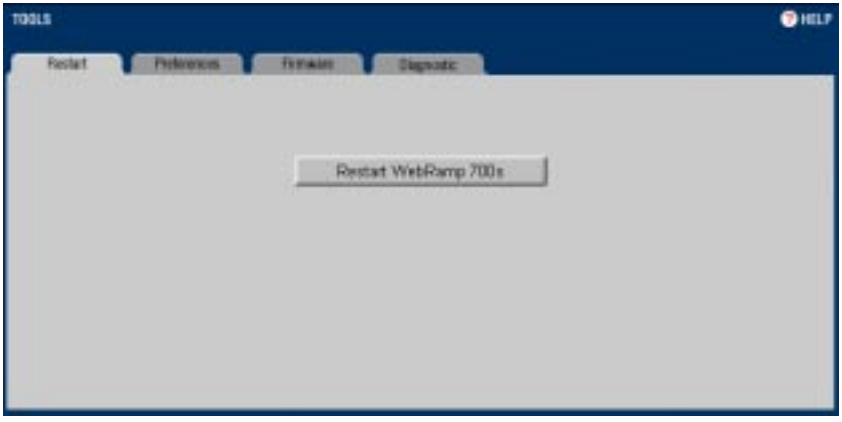
Tools

Use the **Tools** button to access the WebRamp 700s configuration settings including preferences, firmware upgrades and diagnostics.

Restart

After you have configured your Network Addressing, restart your WebRamp 700s. Click the **Tools** button on the left side of the browser window and then click the **Restart** tab at the top of the window. A window similar to the following appears.

Figure 3-16 Restart window



Click the **Restart WebRamp 700s** button and click **Yes** to confirm the restart. The restart takes about 90 seconds, during which time the WebRamp 700s cannot be reached from the Web browser and all network traffic through it is halted.

NOTE – After completing your initial configuration, remember to set your IP address back to its original setting. Depending on your operating system, it may be necessary to restart for the change to take effect.

Preferences

Settings for the WebRamp 700s can be saved and retrieved for backup purposes. This process is also recommended when upgrading the WebRamp 700s software.

This page also provides options to restore the WebRamp's factory defaults and launch the WebRamp 700s Installation Wizard.

Click the **Tools** button on the left side of the browser window and then click the **Preferences** tab at the top of the window. A window similar to the following appears.

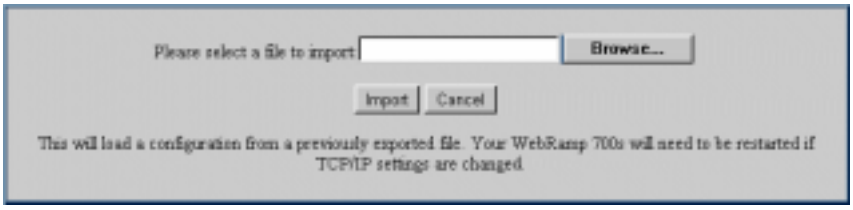
Figure 3-17 Preferences window

Import Settings File

A previously exported file can be imported back into the WebRamp 700s.

Click the **Import** button. A window similar to the following appears.

Figure 3-18 Import settings window



Click the **Browse** button and select the file you want to import, then click the **Import** button.

You must restart the WebRamp 700s for the settings to take effect.

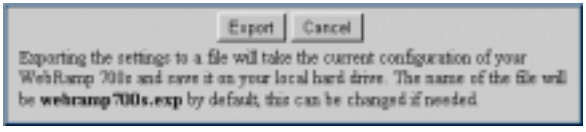
NOTE – The Web browser software being used for the Import Settings function must support HTTP uploads. Netscape Navigator (version 3.0 and above) and Microsoft Internet Explorer (version 4.0 and above) meet these requirements. For your convenience, Netscape Navigator 4.5 (for Windows and Macintosh) is included on the WebRamp 700s CD.

Export Settings File

You can save the WebRamp 700s configuration information to a **preferences file** on a local system, and then load it back into the WebRamp 700s when it's needed.

Click the **Export** button. A window similar to the following appears.

Figure 3-19 Export window

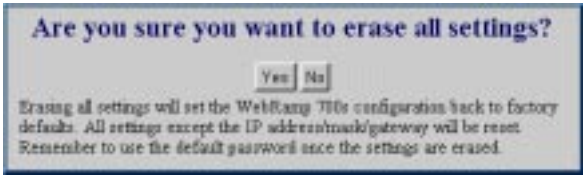


A copy of your current WebRamp 700s configuration settings is saved to your local hard drive. The file is named **webramp700s.exp** by default. You can change the name of this file once it is saved on your hard drive if desired. It will take about a minute to export your WebRamp 700s settings.

Restore Factory Default Settings

The **Restore** button can be used to clear all configuration information and restore the WebRamp 700s to its factory state. All settings except the IP address, mask, and gateway will be reset. Use the default password once the factory default settings are restored.

Figure 3-20 Restore factory defaults



NOTE – The WebRamp 700s Web Address and LAN Subnet Mask, found in the Network tab under the General button, will not be reset.

Installation Wizard

The WebRamp 700s Installation Wizard runs by default the first time you start up the WebRamp 700s CD and steps you through the initial configuration of your WebRamp 700s. In most cases, you will edit the WebRamp 700s configuration using the screen in the web management interface. If you do need to use the Wizard, click the **Launch Wizard** button.

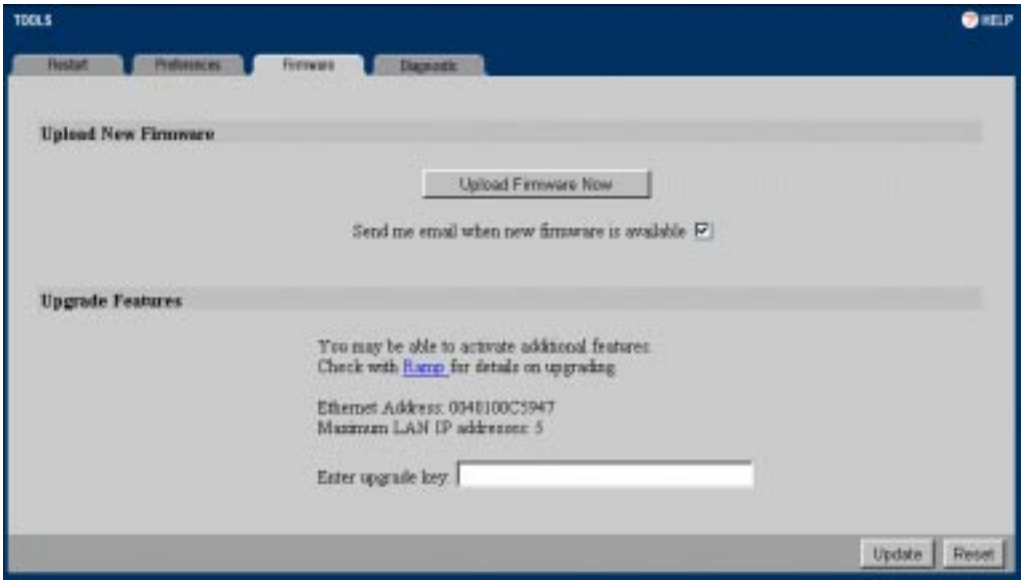
Firmware

The WebRamp 700s has flash memory and can be easily upgraded with new software.

NOTE – When updating the software, all settings, with the exception of the WebRamp 700s Web Address, LAN Subnet Mask, and WAN Router Address are reset to their factory default values. It's a good idea to export the WebRamp 700s settings before uploading new software and then import them after the upgrade is completed.

To upgrade the WebRamp 700s software, click the **Tools** button on the left side of the browser window and then click the **Firmware** tab at the top of the window. A window similar to the following appears.

Figure 3-21 Firmware window



Upload New Firmware

To upload the latest firmware, click the **Upload Firmware Now** button. A window similar to the following appears.

Figure 3-22 Upload Firmware window

When new firmware is uploaded, some settings are erased. For this reason, it is necessary to save the WebRamp 700s preferences to a local disk so that they can be restored later. Click **Yes** if you have saved your preferences or **No** if you need to export your settings before continuing.

Once the settings have been saved to a file, click **UpLoad Firmware Now** again and click **Yes**.

Current software images can be found by following the link to the Ramp Networks FTP site located at ftp://ftp.rampnet.com/700s/software/.

Click the **Browse** button and select the software file from a local hard drive or server on the LAN to begin the upload. Click the **Upload** button after selecting the software file.

NOTE – When uploading the firmware to the WebRamp 700s, it is important not to interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted this way, it may cause the WebRamp 700s to not respond to management log in attempts.

You must restart the WebRamp 700s for the changes to take effect.

Send me email when new firmware is available. To be automatically notified when new firmware is available, click this option and click the **Update** button at the bottom of the screen. When this option is turned on, the WebRamp 700s checks the Ramp Networks FTP site for new firmware once a week. If new firmware is available, you will receive an e-mail message containing the new version's release notes.

NOTE – The Web browser software being used to load new software into the WebRamp 700s must support HTTP uploads. Netscape Navigator (version 3.0 and above) and Microsoft Internet Explorer (version 4.0 and above) meet these requirements. For your convenience, Netscape Navigator 4.5 (for Windows and Macintosh) is included on the WebRamp 700s CD.

Upgrade Features

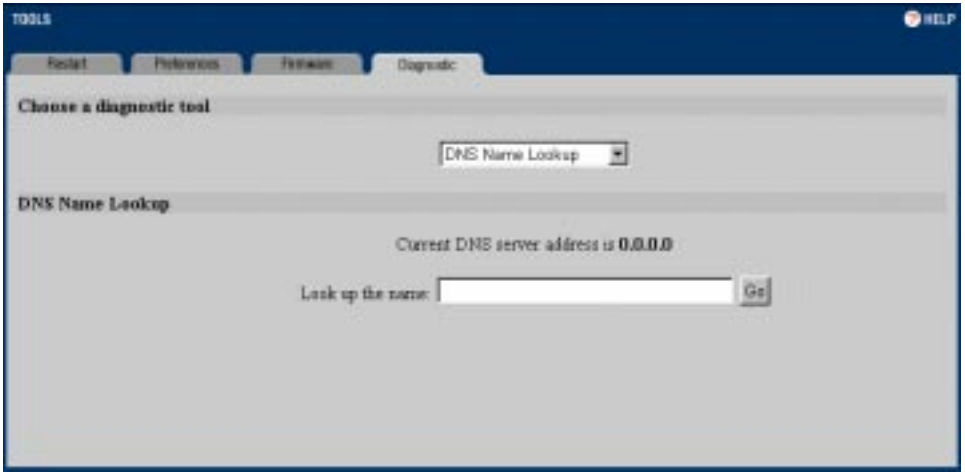
You may be able to activate additional features. Check the Ramp Networks web site for details by clicking the Ramp link in the window.

Enter upgrade key. When a feature upgrade is purchased, an eight digit **Activation Key** and instructions for registering the feature upgrade are included. Once registration is completed, an Upgrade Key is issued. Enter this key in the **Enter upgrade key field** and click the **Update** button at the bottom of the screen. Follow the instructions that are included with the feature upgrade for configuration.

Diagnostics

The **Diagnostics** window contains several tool options for managing the WebRamp 700s. Click the **Tools** button on the left side of the browser window and then click the **Diagnostic** tab at the top of the window. A window similar to the following appears.

Figure 3-23 Diagnostics window



Choose a Diagnostic Tool

This menu allows you to select from several diagnostic tools including:

- DNS Name Lookup Tool
- Find Network Path
- Ping
- Packet Trace
- Tech Support Report

DNS Name Lookup. The Internet has a service called the Domain Name Service (DNS) which allows users to enter an easily remembered host name, such as www.rampnet.com, instead of numerical TCP/IP addresses to access Internet resources. Unfortunately, this service can easily be attacked to confuse the LAN and open security holes. For this reason, the WebRamp 700s requires numerical TCP/IP addresses to be entered in address fields which are used in the firewall function. The WebRamp 700s has a DNS lookup tool which returns the numerical TCP/IP address of a host name.

Select **DNS Name Lookup** from the **Choose a Diagnostic Tool** menu.

Enter the host name in the **Look up the Name** field and click **Go**. The WebRamp 700s queries the DNS server and displays the result at the bottom of the window.

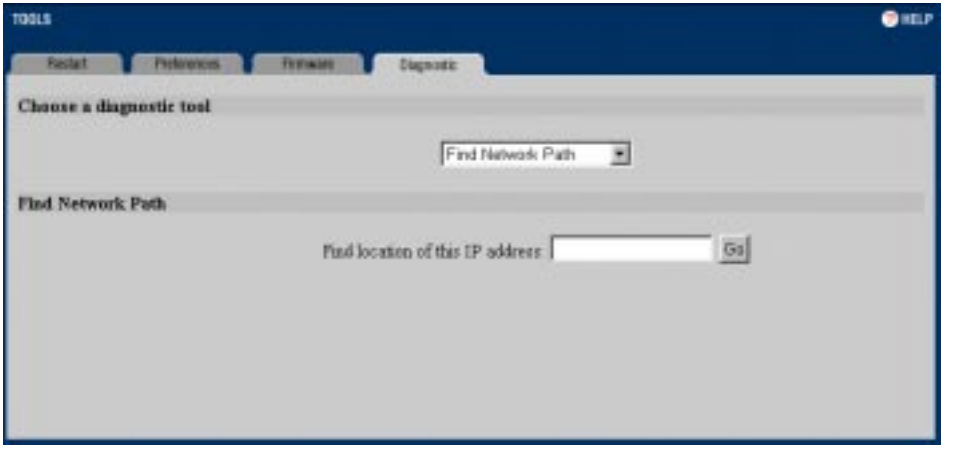
NOTE – In order for the Name Lookup feature to function, the IP address of the DNS server must be entered in the Network Settings tab (accessed by clicking the General button).

Find Network Path

The **Find Network Path** tool shows the port location for the LAN, WAN, and IP host. This helps you determine if the WebRamp 700s is properly configured. For example, if the WebRamp 700s "thinks" that a machine known to be on the Internet is located on the LAN port, then there is a problem with the configuration of the Network or Intranet settings. **Find Network Path** also shows which router a node is using, if the target node is behind a router, and, when it is, the Ethernet address of the target node or router. This can help isolate router configuration problems.

Select **Find Network Path** from the **Choose a diagnostic tool** menu. A window similar to the following appears.

Figure 3-24 Diagnostics window



Enter the IP address in the **Find location of this IP address** field and click the **Go** button. The test takes a few seconds to complete. Once completed, a message showing the results appears at the bottom of the window.

If the network path is incorrect, check the **Intranet** and **Static Routes** settings**.**

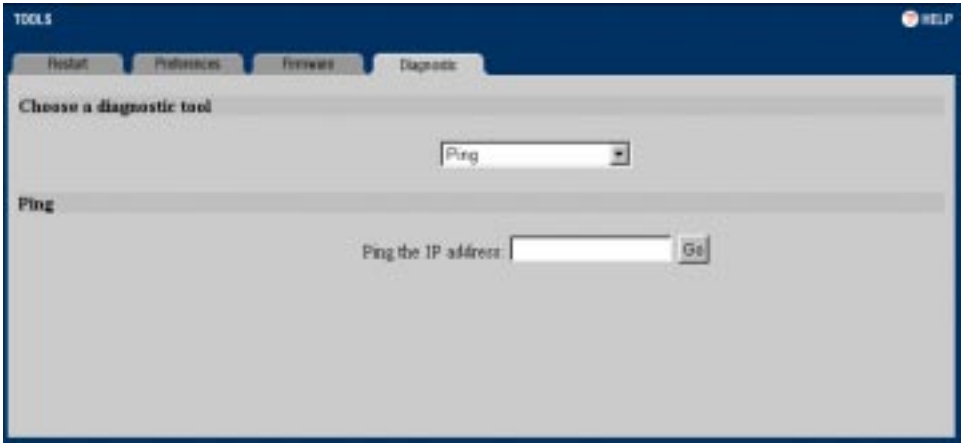
NOTE – Find Network Path requires an IP address. You can use the WebRamp 700s DNS Name Lookup tool to find the IP address of a host.

PING

The **Ping** test bounces a packet off a machine on the Internet back to the sender. This test shows if the WebRamp 700s is able to contact the remote host. If users on the LAN are having problems accessing Internet services, try pinging the DNS server, or other machine at the ISP's location. If this test is successful, try pinging devices outside the ISP. This will help you determine if the problem lies with the ISP's connection.

Select **Ping** from the **Choose a diagnostic tool** menu. A window similar to the following appears.

Figure 3-25 Ping diagnostics tool



Enter the IP address in the **Ping the IP address** field and click the **Go** button. The test takes a few seconds to complete. Once completed, a message showing the results appears at the bottom of the window.

NOTE – Ping requires an IP address. You can use the WebRamp 700s DNS Name Lookup tool to find the IP address of a host.

Packet Trace

The **Packet Trace** tool tracks the status of a data packet or communications stream as it moves from source to destination. This tool helps you determine if a packet or communications stream is being stopped at the WebRamp 700s or is lost on the Internet.

To interpret the output of this tool when using TCP, you need to understand the three-way handshake that occurs for each communications stream. When a host on an IP network establishes a connection with a remote host, it sends a “SYN” (Synchronize) packet. The remote host then responds with a “SYN,ACK” (Synchronize Acknowledgment). The host then responds with another “ACK” to the remote host, beginning the data transfer.

The following packet trace example shows a Web session from a host on the LAN (207.88.211.116) to a server on the Internet (204.71.200.74):

1. **1**TCP sent [SYN]

   From 207.88.211.116 / 1937 (00:a0:4b:05:96:4a)

   To 204.71.200.74 / 80 (02:00:cf:58:d3:6a)

   LAN client sends SYN to remote host.

2. **2** TCP received [SYN,ACK]

   From 204.71.200.74 / 80 (02:00:cf:58:d3:6a)

   To 207.88.211.116 / 1937 (00:a0:4b:05:96:4a)

   Remote host sends SYN,ACK to LAN client.

3. **3**TCP sent [ACK]

   From 207.88.211.116 / 1937 (00:a0:4b:05:96:4a)

   To 204.71.200.74 / 80 (02:00:cf:58:d3:6a)

   LAN client sends a final ACK, and the data transfer begins.

When the WebRamp 700s is used, the packet trace of the three-way handshake changes as the WebRamp 700s passes data from the LAN to WAN port, and back.

1. **1**TCP received on LAN [SYN]

   From 192.168.1.158 / 1282 (00:a0:4b:05:96:4a)

   To 204.71.200.74 / 80 (02:00:cf:58:d3:6a)

   WebRamp 700s receives SYN from LAN client.

2. **2** TCP sent on WAN [SYN]TCP sent on WAN [SYN]

   From 207.88.211.116 / 1937 (00:40:10:0c:01:4e)

   To 204.71.200.74 / 80 (02:00:cf:58:d3:6a)

   WebRamp 700s forwards SYN from LAN client to remote host.

3. **3** TCP received on WAN [SYN,ACK]

   From 204.71.200.74 / 80 (02:00:cf:58:d3:6a)

   To 207.88.211.116 / 1937 (00:40:10:0c:01:4e)

   WebRamp 700s receives SYN,ACK from remote host.

4. **4**TCP sent on LAN [SYN,ACK]

   From 204.71.200.74 / 80 (02:00:cf:58:d3:6a)

   To 192.168.1.158 / 1282 (00:a0:4b:05:96:4a)

   WebRamp 700s forwards SYN,ACK to LAN client.

5. **5**TCP received on LAN [ACK]

   From 192.168.1.158 / 1282 (00:a0:4b:05:96:4a)

   To 204.71.200.74 / 80 (02:00:cf:58:d3:6a)

   Client sends a final ACK, and waits for start of data transfer.

6. **6**TCP sent on WAN [ACK]

   From 207.88.211.116 / 1937 (00:40:10:0c:01:4e)

   To 204.71.200.74 / 80 (02:00:cf:58:d3:6a)

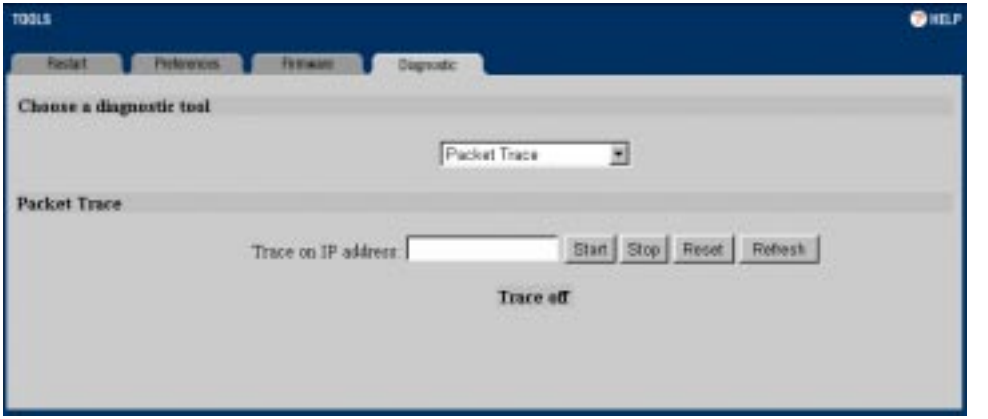
   WebRamp 700s forwards client's ACK to remote host and waits for start of data transfer.

This passing of packets from port to port is then shown in the packet trace for all packets sent and received as part of the data transfer.

When using packet traces to isolate network connectivity problems, look for the location where the three-way handshake is breaking down. This will help determine if the problem is with the WebRamp 700s configuration, or if there is a problem on the Internet.

Select **Packet Trace** from the **Choose a diagnostic tool** menu. A window similar to the following appears**.**

Figure 3-26 Packet trace diagnostics tool



NOTE – Packet Trace requires an IP address. You can use the WebRamp 700s DNS Name Lookup tool to find the IP address of a host.

Enter the IP address of the remote host in the **Trace on IP address** field.

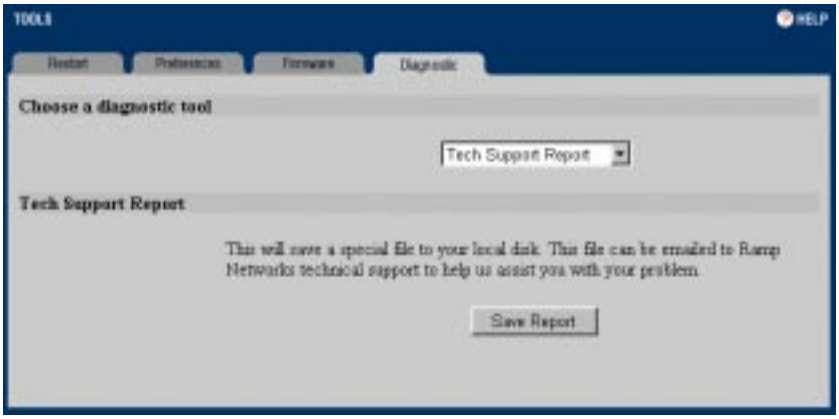
- **Start.** Click the **Start** button to start an IP session with the remote host using an IP client, such as Web, FTP, or Telnet. Instead of a host name, such as "www.yahoo.com", use the IP address in the **Trace on IP address** field.
- **Refresh.** Click the **Refresh** button to display the packet trace information.
- **Stop.** Click **Stop** to terminate the packet trace.
- **Reset.** Click Reset to clear the results.

Tech Support Report

The **Tech Support Report** generates a detailed report of the WebRamp 700s configuration and status, and saves it to the local hard disk. This file can then be e-mailed to Ramp Networks at support@rampnet.com to help assist with a problem. If you receive a case number after submitting the report, be sure to include this case number in all correspondence to help Ramp Networks better service the tech support request.

Select **Tech Support Report** from the **Choose a diagnostic tool** menu. A window similar to the following appears.

Figure 3-27 Tech support report diagnostics tool



Click the **Save Report** button to save the report as a text file to the local disk.

Access

Network Access Rules are management tools that allow the administrator to define rules extending the WebRamp 700s firewall functions.

By default, stateful packet inspection of the WebRamp 700s allows all communications to the Internet that originates from the LAN, and blocks all traffic to the LAN that originates from the Internet.

This behavior is defined by the “Default” stateful packet inspection rule enabled in the WebRamp 700s:

- Allow all sessions originating from the LAN to the WAN
- Deny all sessions originating from the WAN to the LAN

Additional Network Access Rules may be defined to extend or override the default rules.

For example, Network Access Rules may be created which:

- Block all traffic of a certain type, such as IRC (Internet Chat), from the LAN to the Internet.
- Allow certain types of traffic, such as Lotus Notes database synchronization, from the Internet to a specific host on the LAN.
- Allow access to a Web server to everyone but competitors.

- Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

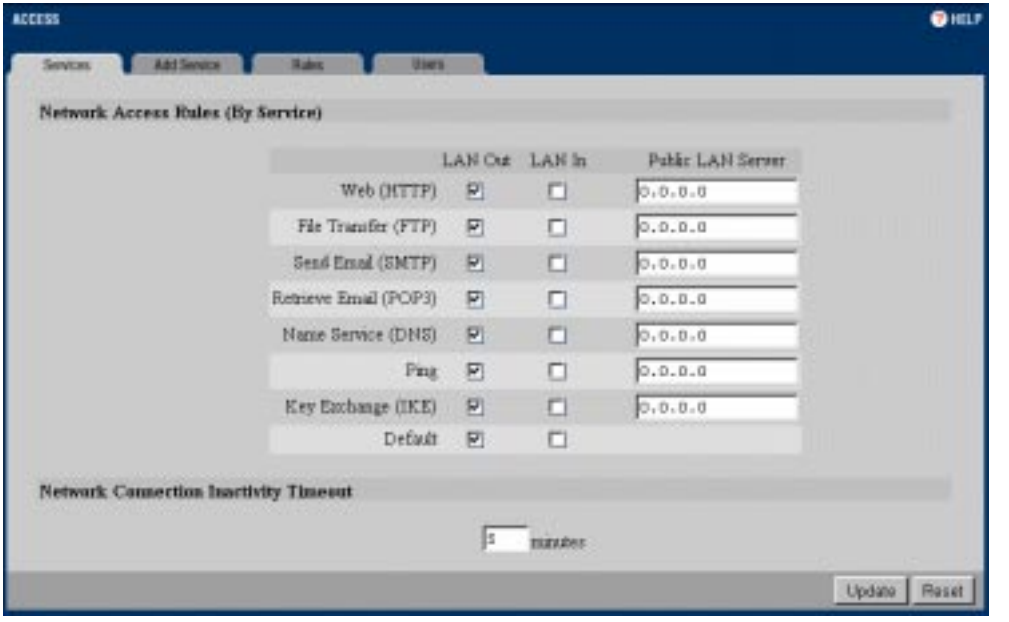
These custom rules work by evaluating network traffic's source IP address and port, Destination IP address and port, IP protocol type, and comparing them to rules set by the administrator. Network Access Rules take precedence, and may override the WebRamp 700s stateful packet inspection.

NOTE – The ability to define Network Access Rules is a very powerful tool. Using custom rules, it is possible to disable all firewall protection or block all access to the Internet. Use extreme caution when creating or deleting Network Access Rules.

Services

The **Services** window allows you to setup and define your Network Access Rules by service. Click the **Access** button on the left side of the browser window and then click the **Services** tab at the top of the window. A window similar to the following appears.

Figure 3-28 Services window



Network Access Rules (By Service)

Rules are sorted from the most specific at the top, to the most general at the bottom. At the bottom of the table is the **Default** rule. Rules may be created to override the behavior of the **Default** rule. For example, the **Default** rule allows users on the LAN to access all Internet services, including NNTP News. You can choose, however, to block LAN access to NNTP by deselecting the **LAN Out** box to the right of the NNTP News service.

LAN Out. When selected, users on the LAN can access servers of that type. When not selected, users on the LAN cannot access servers of that type. **LAN Out** is selected by default (users are allowed access). When the **Alert Icon** is displayed to the right of the checkbox, there is a Custom Rule in the **Rules** tab section that modifies the behavior of the listed Network Access Rule.

LAN In. When selected, users on the Internet can access all hosts on the LAN via that protocol. When not selected, access to the protocol is not permitted from the Internet to the LAN. **LAN In** is deselected by default (users cannot access hosts); use caution when turning on this option. When the **Alert Icon** is displayed to the right of the checkbox, there is a Custom Rule in the **Rules** tab section that modifies the behavior of the listed Network Access Rule.

NOTE – The **LAN In** option appears only when you're working in Standard mode.

Public LAN Server. A Public LAN Server is a single host on the LAN that handles all traffic originating from the Internet to the LAN of a specific protocol, such as HTTP. A Public LAN Server is designated by entering its IP address in the **Public LAN Server** field. If a server is not designated for a certain protocol, enter 0.0.0.0 in the field.

Network Connection Inactivity Timeout

If a connection to a server outside the LAN remains idle for more than five minutes, the WebRamp 700s closes the connection. Without this timeout, it is possible that connections could stay open indefinitely, creating potential security holes. The **Inactivity Timeout** can be increased if users frequently complain of dropped connections in applications such as Telnet and FTP.

NOTE – If there is an SMTP or POP 3 e-mail server or gateway on the LAN that is used to send and receive Internet e-mail, enter its IP address in the SMTP field. If you don't enter the IP address, users on the LAN won't be able to receive Internet e-mail.

When you've finished editing the **Network Access Rules**, click the **Update** button at the bottom of the screen. When the information has been updated, a confirmation message appears in the status line at the bottom of the window.

You must restart the WebRamp 700s for these changes to take effect.

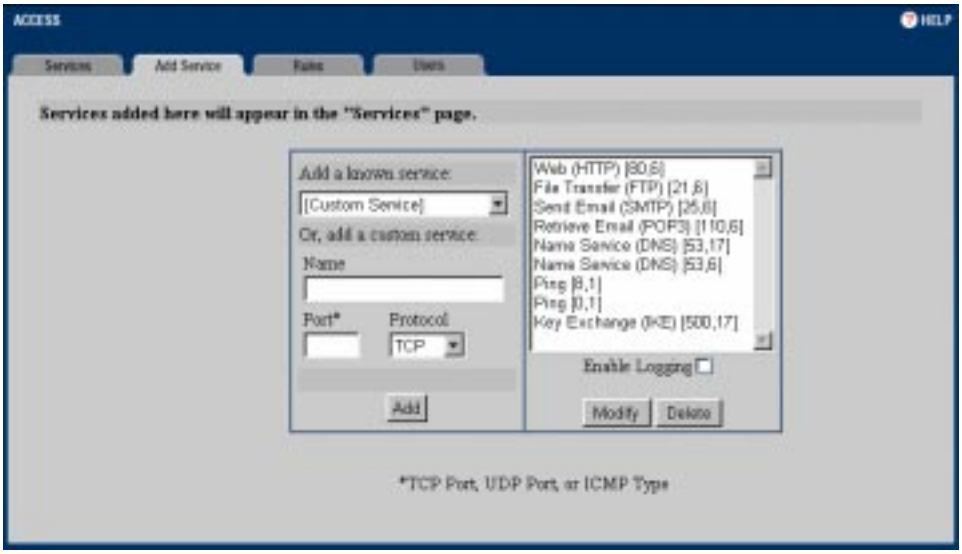
Only traffic of the specific protocol will be allowed to each server designated as a Public LAN Server, although a single server can be specified for more than one protocol. For example, if an FTP and a Web server are running on the same machine, you enter the same IP address in both the "http" and "ftp" fields.

Add Service

You can add support for a protocol not listed in the **Services** window.

Click the **Access** button on the left side of the browser window and then click the **Add Service** tab at the top of the window. A window similar to the following appears.

Figure 3-29 Add Service window



The scrolling list on the right side of the screen displays all IP protocols which are currently defined and will appear in the **Services** window. Next to the name of the protocol, two numbers appear in brackets. The first number indicates the IP port number which defines the service (either TCP Port, UDP Port, or ICMP Type). The second number indicates the IP protocol type (6 for TCP, 17 for UDP, or 1 for ICMP).

NOTE – There may be more than one entry with the same name. For example, the default configuration has two entries labeled “Name Service (DNS)”. These are UDP port 53 and TCP port 53. Entries with identical names are grouped together and treated as a single service. The WebRamp 700s supports up to 128 entries.

Add a known service. To add support for a well-known service by name, select the name of the service from the **Add a known service** menu and click the **Add** button. The new service appears in the listbox to the right, along with its numeric protocol description. Note that some well-known services will add more than one entry to the list box.

Custom Service. To add a custom service, choose **Custom Service** from the **Add a known service** menu, then type a unique name, such as “CC:mail” or “Microsoft SQL” into the **Name** field. Next, enter the IP port number in the **Port*** field and select the IP protocol type from the **Protocol** menu. Click **Add** and the new service appears in the list box.

Visit ds.internic.net/rfc/rfc1700.txt for a list of well-known IP port numbers.

NOTE – If multiple entries with the same name are created, they are grouped together as a single service and may not function as expected.

You can choose to stop logging specific events which are usually written to the internal screen log of the WebRamp 700s. For example, if LINUX’s authentication protocol is filling the log with useless entries, you can configure all activity for this service so that it is ignored by the screen log. To turn off logging for a specific service, select the service name in the list, deselect the **Enable Logging** option, and then click **Modify**.

To delete a service, select the service name in the list and click **Delete**. For services with multiple entries, you can choose to delete only a single Port/Protocol combination from the list. For example, deleting the entry marked “Name Service (DNS) [53,6]” deletes just the TCP portion of the service.

Rules

Network Access Rules evaluate network traffic’s Source IP address, Destination IP address, and IP protocol type to decide if the IP traffic is allowed to pass through the firewall. Custom rules take precedence and may override the default stateful packet inspection of the WebRamp 700s.

NOTE – The ability to define Network Access Rules is a very powerful tool. Using custom rules, it is possible to disable all firewall protection or block all access to the Internet. *Use extreme caution* when creating or deleting Network Access Rules.

NOTE – Network Access Rules will not disable protection from Denial of Service attacks, such as SYN Flood, Ping of Death, and so on. However, it is possible to create vulnerabilities to attacks that exploit vulnerabilities in applications, such as WinNuke.

Understanding the Network Access Rule Hierarchy

The rule hierarchy has two basic concepts:

- Specific rules override general rules.
- Equally specific **Deny** rules override **Allow** rules.

When evaluating rules, the WebRamp 700s uses the following criteria:

- A rule defining a specific service is more specific than the **Default rule**.
- A defined Ethernet link, such as LAN or WAN, is more specific than *****.
- A single IP address is more specific than an IP address range.
- Rules are listed in the web management interface window from most specific to least specific, and rules at the top of the window override the rules listed at the bottom of the window.

Network Access Rule Logic List

It is important to fully consider the logic behind a new rule before it is added. The following list will help you when you're creating new rules:

- State the intent of the rule. For example, "This rule will restrict all IRC access from the LAN to the Internet." Or, "This rule will allow a remote Lotus Notes server to synchronize over the Internet to an internal Notes server."
- Is the intent of the rule to allow or deny traffic?
- What is the flow of the traffic: from the LAN to the Internet or from the Internet to the LAN?
- List which IP services will be affected.
- List which computers on the LAN will be affected.
- List which computers on the Internet will be affected. The more specific, the better. For example, if traffic is being allowed from the Internet to the LAN, it is better to allow only certain machines on the Internet to access the LAN.

Once the logic of the rule has been defined, it is critical to consider the security ramifications of the rule:

- Will this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?
- Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?

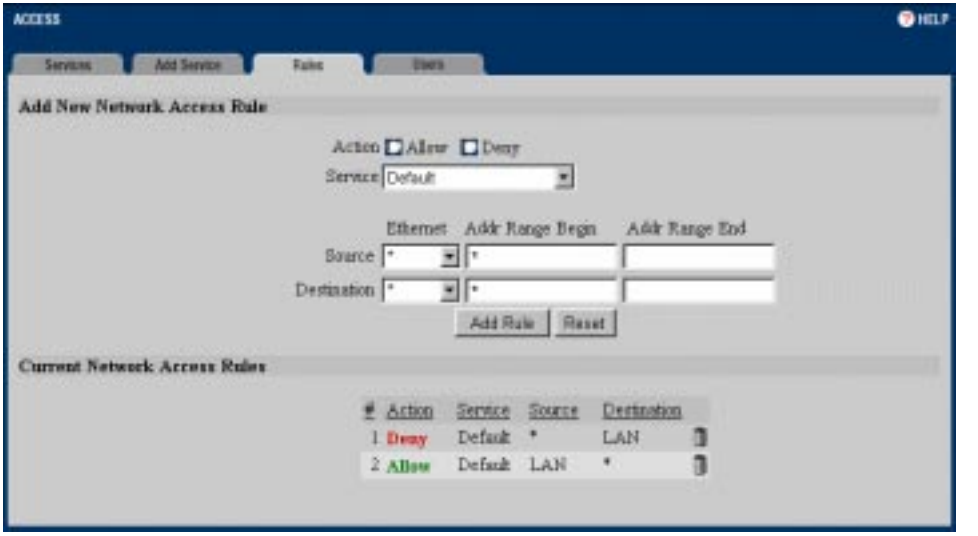
- Will this rule allow Internet users access to resources on the LAN in a manner that may create an undue security vulnerability? For example, if NetBIOS ports (UDP 137, 138, 139) are allowed from the Internet to the LAN, Internet users may be able to connect to PCs with file sharing enabled.
- Does this rule conflict with any existing rules?

Add New Network Access Rule

Adding rules is simply a matter of plugging the information into the correct fields in the **Rules** window.

Click the **Access** button on the left side of the browser window and then click the **Rules** tab at the top of the window. A window similar to the following appears.

Figure 3-30 Rules window



Action. Select **Allow** or **Deny** depending on the intent of the rule (as defined by item 2 in the “Network Access Rule Logic List”).

Service. Select the IP protocol from the **Service** menu (as defined by item 4 in the “Network Access Rule Logic List”). If the protocol is not listed, you need to add it using the **Add Service** window.

Source. Select the Network Access Rule's source port, **LAN** or **WAN** from the **Ethernet** pull-down menu. After selecting the source port, enter the address range parameters.

NOTE – The DMZ option is currently unavailable.

- **Addr Range Begin...End.** If there will be IP address restrictions on the source of the traffic, such as keeping competitors off the company's Web site, enter the starting and ending IP addresses of the range in the **Addr Range Begin** and **Addr Range End** boxes. If all IP addresses are to be affected, enter * in the **Addr Range Begin** field.

Destination. Select the Network Access Rule's destination port, **LAN** or **WAN** from the **Ethernet** menu. After selecting the destination port, enter the address range parameters.

- **Addr Range Begin...End.** If there will be IP address restrictions on the destination of the traffic, such as limiting Telnet access to a remote office, enter the starting and ending IP addresses of the range in the **Addr Range Begin** and **Addr Range End**, respectively. If all IP addresses are to be affected, enter * in the **Addr Range Begin** field.

Current Network Access Rules

All configured Network Access Rules are listed in the table under the section titled **Current Network Access Rules**. The rules are listed from most to least specific. To delete a rule, click the **Trash Can** at the far right of the rule.

Examples

The following examples will illustrate methods for creating Network Access Rules:

Blocking LAN access to specific protocols

This example shows how to block all LAN access to NNTP servers on the Internet.

1. Click the **Access** button on the left side of the browser window, then click the **Rules** tab.
2. Click **Deny** in the **Action** option.
3. From the **Service** menu, choose **News (NNTP)**. If the service is not listed in the menu, add it in the **Add Service** window.
4. Select **LAN** from the **Source Ethernet** menu.

5. Since all computers on the LAN are to be affected, enter * in the **Source Addr Range Begin** field.
6. Select **WAN** from the **Destination Ethernet** menu.
7. Since the intent is to block access to all NNTP servers, enter * in the **Destination Addr Range Begin** field.
8. Click the **Add Rule** button**.**

Block access to specific users

This example shows how to create a rule which will block a certain range of computers, such as a competitor, from accessing the public Web server on the LAN.

1. Click the **Access** button on the left side of the browser window, then click the **Rules** tab.
2. Click **Deny** in the **Action** option.
3. From the **Service** menu, choose **Web (HTTP)**.
4. Select **WAN** from the **Source Ethernet** menu.
5. Enter the blocked network's starting IP address in the **Source Addr Range Begin** field and the blocked network's ending IP address in the **Source Addr Range Begin** field.
6. Select * from the **Destination Ethernet** menu.
7. Since the intent is to block access to all servers, enter * in the **Destination Addr Range Begin** field.
8. Click the **Add Rule** button.

Enabling Ping

By default, the WebRamp 700s does not respond to pings from the Internet. However, Ping is a tool that many ISPs use to verify that the Internet connection is active. Step 3 of this example limits the source to allow only the ISP to ping the WebRamp 700s.

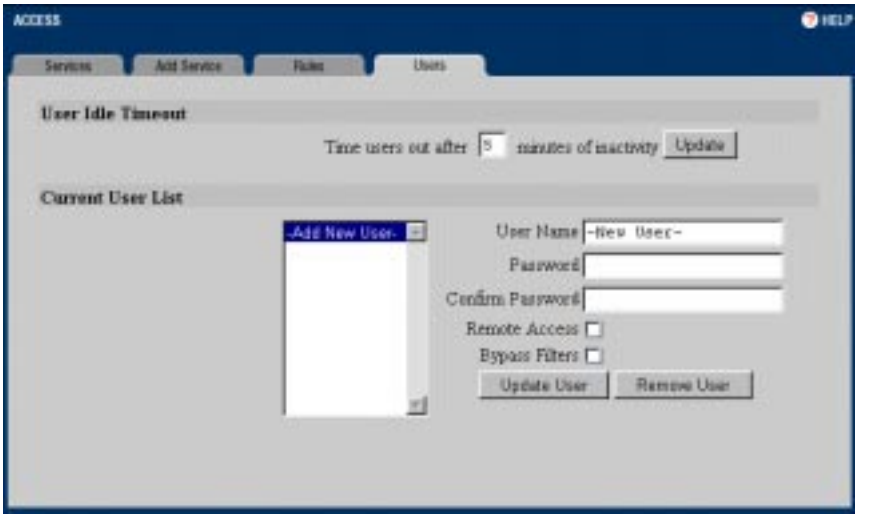
1. Click the **Access** button on the left side of the browser window, then click the **Rules** tab.
2. Click **Allow** in the **Action** option.
3. From the **Service** menu, choose **Ping**. Select **WAN** from the **Source Ethernet** menu.
4. Enter the starting IP address of the ISP's network in the **Source Addr Range Begin** field and the network's ending IP address in the **Source Addr Range End** field.
5. Select **LAN** from the **Destination Ethernet** menu.
6. Since the intent is to allow a ping only to the WebRamp 700s, enter the WebRamp 700s Web Address in the **Destination Addr Range Begin** field.
7. Click the **Add Rule** button.

Users

The WebRamp 700s provides an authentication mechanism which gives authorized users access to the LAN from remote locations on the Internet as well as a means to bypass the content filtering and blocking from the LAN to the Internet.

Click the **Access** button on the left side of the browser window and then click the **Users** tab at the top of the window. A window similar to the following appears.

Figure 3-31 Users window



User Idle Timeout

This sets the maximum period of inactivity before a user is required to re-establish an Authenticated Session. Enter the desired number of idle time minutes and click the **Update** button at the right side of the screen. **User Idle Timeout** applies to **Remote Access** and **Bypass Filters**.

Current User List

All currently defined users are listed in this window.

Add New User. Select **Add New User** from the **Current User List**.

User Name. Enter the new user's login name in the **User Name** field.

Password and **Confirm Password**. Enter the user's password in the Password field and again in the Confirm Password field. It is important to use a password that cannot be easily guessed by someone else. Avoid using names of friends, family, pets, places, and so on. Good passwords can be created by making up nonsense words, such as "dwizdell", using random letters and numbers, such as "a7fe2j42", or by including non-alphanumeric ASCII characters in words, such as "r&newerx". Passwords are case sensitive.

Remote Access. Allows unrestricted access to the LAN from a remote location on the Internet.

Bypass Filters. Allows unrestricted access to the Internet from the LAN, bypassing Web, News, Java, and ActiveX blocking.

Press **Update User** after you have entered all of the new user information.

NOTE – User names are not case sensitive (“john” is equivalent to “JOHN” or “John”), but passwords are case sensitive (“password” is not the same as “Password”).If you are having trouble having a password accepted, check the Caps Lock key on your keyboard to be sure it is not on.

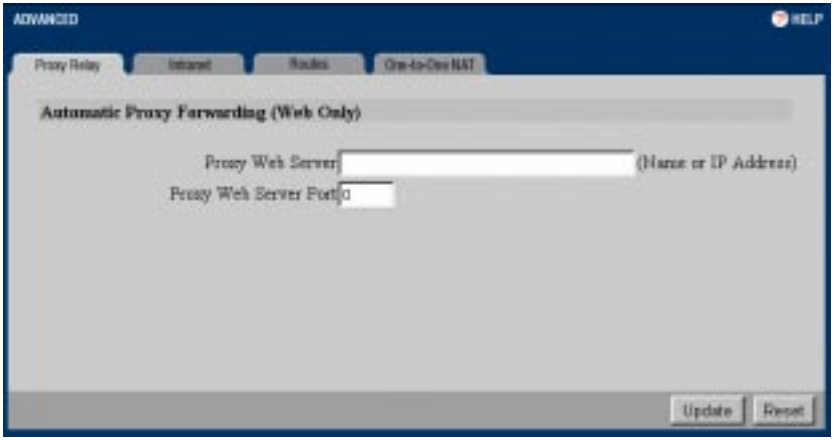
The WebRamp 700s supports up to 250 users. An upgrade is required to support the maximum number of users.

To change a user’s password or privileges, select the user name, make the changes, and then click the **Update User** button. To delete a user, select the name and click the **Remove User** button.

Advanced

The Advanced window displays a summary of the currently enabled features and allows you to enable additional features after purchasing an upgrade from Ramp Networks. Click the button labeled **Advanced** at the left side of the browser window. A window similar to the following appears.

Figure 3-32 Advanced window



This window displays a summary of the currently enabled features, as well as a field to enter a serial number to enable additional features.

Proxy Relay

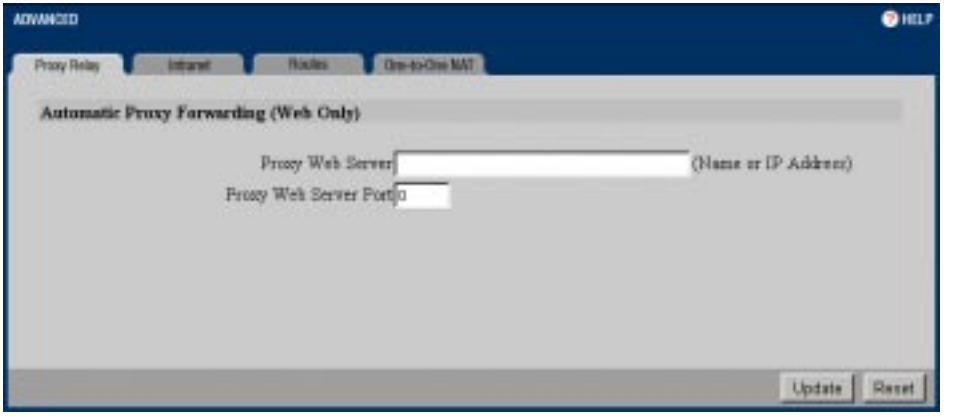
A proxy server intercepts all requests to the Web server to see if it can fulfill the requests by returning a locally stored copy of the requested information. Normally, when you use a proxy server, each client must be configured to support the proxy, which can make proxy servers difficult to administer.

If a proxy server is already installed on the LAN, you can move the proxy to the WAN and turn on **Automatic Proxy Forwarding (Web Only)**, instead of configuring each individual client to point to the proxy server. Because the WebRamp 700s can automatically forward all Web proxy requests to the proxy server, no client configuration is required.

NOTE – The proxy server must be located on the WAN; it cannot be located on the LAN.

Click the **Advanced** button on the left side of the browser window then click the **Proxy Relay** tab at the top of the window. A window similar to the following appears.

Figure 3-33 Proxy Relay window



Enter the name or the WebRamp 700s IP address, 192.168.1.251, in the **Proxy Web Server Address** field and the proxy's IP port in the **Proxy Web Server Port** field.

Click the **Update** button at the bottom of the screen. When the information has been updated, a confirmation message appears in the status line at the bottom of the window.

Intranet Support

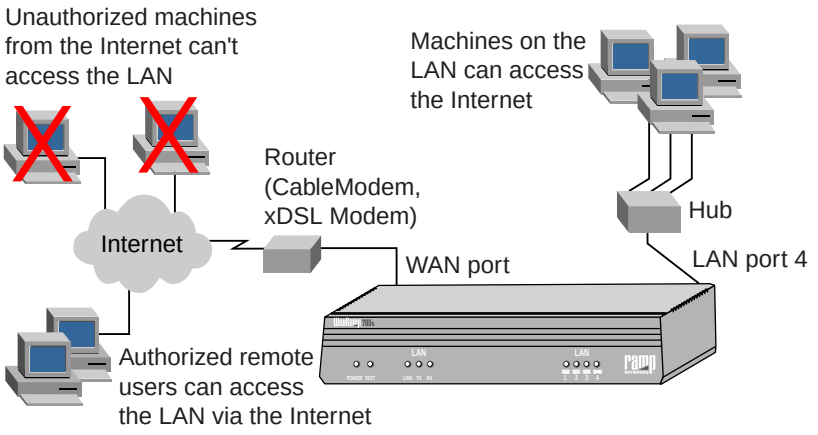
In some cases, it is desirable to prevent access to certain resources by unauthorized users on the LAN. For example, a school's administration office may be placed behind the WebRamp 700s to restrict access to its computers by users in the Student Computer Lab. Similarly, an organization's accounting, research, or other sensitive resources may be protected against unauthorized access by other users on the same network.

By default, protected LAN users can only access the Internet and cannot access other devices between the WAN port and the Internet. Additional configuration is required to enable access to the area between the WebRamp 700s WAN port and the Internet (an Intranet).

Creating a firewall

To create a firewall, you need to connect the WebRamp700s between the free and restricted segments on the LAN, as shown below.

Figure 3-34 Firewall



Installation

1. Connect the Ethernet LAN ports on the back of the WebRamp 700s to the network segment that you want to protect against unauthorized access.
2. Connect the Ethernet WAN port on the back of the WebRamp 700s to the rest of the network.

NOTE – Devices connected to the WAN port do not have firewall or content filter protection. It is suggested that another Internet security appliance from the WebRamp product family be used to protect these computers.

3. Plug the WebRamp 700s power supply into an AC power outlet, then plug the power supply output cable into the **5VDC/1.5A** port on the back of the WebRamp 700s**.**

Configuration

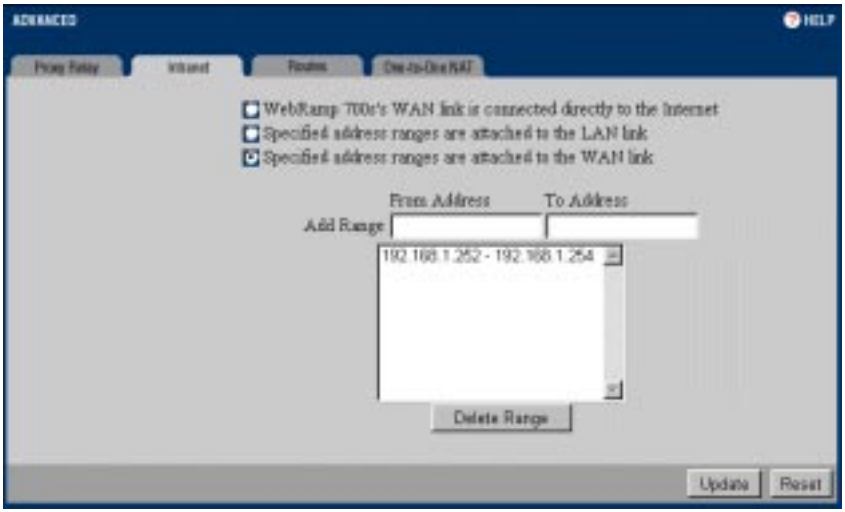
To create a firewall, you need to specify the IP addresses of the protected machines. This can be done in one of two ways: either specify which machines *are* members of the segment with restricted access (inclusive), or specify which machines *are not* members of the segment with restricted access (exclusive).

When you're using the inclusive method, the IP addresses of the machines which are connected to WebRamp 700s LAN ports are specified. This method would be used in cases such as a small accounting office in a large LAN, where it may be easier to identify the small number of machines with restricted access rather than the larger number of machines on the corporate network.

When you use the exclusive method, the IP addresses of the machines connected to WebRamp 700s WAN port are specified. This method would be used in cases such as a large school district with a small student computer lab, where it would be easier to specify the small number of machines on the WAN which are not protected by the Intranet firewall, rather than the larger number of machines which are protected.

Click the **Advanced** button on the left side of the browser window and then click on the **Intranet** tab at the top of the window. A window similar to the following appears.

Figure 3-35 Intranet window



Typically, it will be easier to enter the IP addresses from the smaller number of machines. These addresses may be entered individually, or as a range.

WebRamp 700s WAN link is connected directly to the Internet router. Select this option if the WebRamp 700s is protecting the entire network. This is the default setting.

Specified address ranges are attached to the LAN link. Use this option when it is easier to specify which devices are on the LAN. If a machine's IP address is not specified, all communications through the WebRamp 700s for that machine are not blocked.

Specified address ranges are attached to the WAN link. Select this option when it is easier to specify which devices are on the WAN port.

Add Range. To enter a range of addresses, such as the 51 IP addresses from 199.2.23.50 to 199.2.23.100, enter the starting address in the **From Address** field and the ending address in the **To Address** field. An individual address is entered in the **From Address** field only. You can enter up to 64 address ranges.

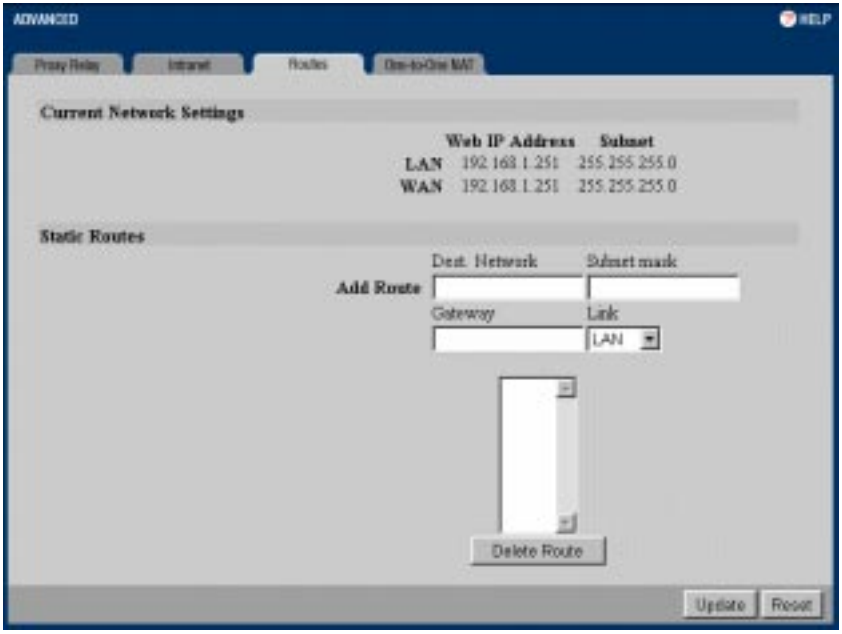
Click the **Update** button at the bottom of the screen. When the information has been updated, a confirmation message appears in the status line at the bottom of the window.

Routes

If the LAN has internal routers, you need to enter their addresses and network information into the WebRamp 700s.

Click the **Advanced** button on the left side of the browser window and then click the **Routes** tab at the top of the window. A window similar to the following appears.

Figure 3-36 Routes window



Current Network Settings

The current network settings for your WebRamp 700s are displayed in this window.

Static Routes

Static routes are used if the LAN is segmented into subnets, either for size or practical considerations. For example, a subnet can be created which contains an organization's graphic design shop, isolating it from traffic on the rest of the LAN.

- **LAN.** The IP Address and Subnet on the WebRamp 700s LAN port are displayed at the top of the window. (These are configured by clicking the **General** button and then clicking the **Network** tab.)
- **WAN.** The IP address of the WAN port is displayed. It will differ from that of the LAN port if NAT is enabled. (This is configured by clicking the **General** button and then clicking the **Network** tab**.)** The **Subnet Mask** is displayed.

Add Route. Enter the destination network of the router in the **Dest Network** field and the IP address of the router as it appears on the WebRamp 700s subnet in the **Gateway** field. Select which port the router is connected to from the **Link** menu (LAN or WAN).You may need to check the configuration of the LAN routers in order to find this information.

Click the **Update** button at the bottom of the screen. When the information has been updated, a confirmation message appears in the status line at the bottom of the window.

One-to-One NAT

One-to-One NAT creates a relationship which maps valid external addresses to internal addresses hidden by NAT. This allows access to machines with an internal address at their corresponding external valid IP address.

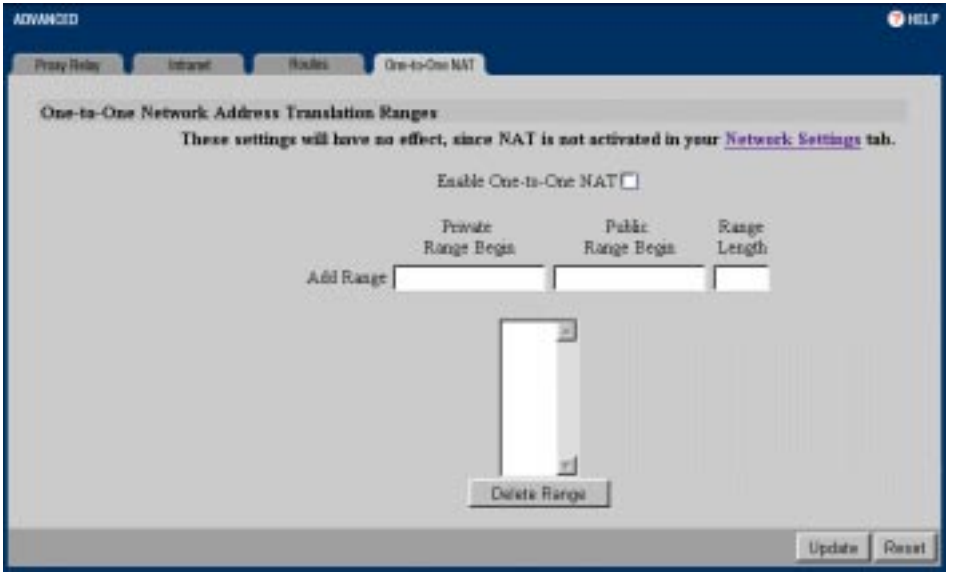
The following table shows a sample one-to-one NAT relationship between public (external) IP addresses assigned by an ISP, and corresponding private (internal) IP addresses:

Private IP Address	Public IP Address
192.168.1.20	202.3.169.44
192.168.1.21	202.3.169.45
192.168.1.22	202.3.169.46
192.168.1.23	202.3.169.47
192.168.1.24	202.3.169.48
192.168.1.25	202.3.169.49
192.168.1.26	202.3.169.50

NOTE – The NAT Public IP Address *cannot* be included in a range.

Click the **Advanced** button on the left side of the browser window and then click the **One-to-One NAT** tab at the top of the window. A window similar to the following appears.

Figure 3-37 One-to-One NAT window



One-To-One Network Address Translation Ranges

Enable One-to-One NAT. To use One-to-One NAT, select the Enable One-to-One NAT option.

Private Range Begin. Enter the beginning IP address of the private address range in the **Private Range Begin** field**.**

Public Range Begin. Enter the beginning IP address of the public address range in the Public Range Begin field. This address is assigned by the ISP.

NOTE – Do not include the NAT Public IP Address in a range.

Range Length. Enter the number of IP addresses for the range. The range length cannot exceed the number of valid IP address. You can add up to 64 ranges. To map a single address, use a **Range Length** of **1.**

Click the **Update** button at the bottom of the screen. When the information has been updated, a confirmation message appears in the status line at the bottom of the window.

You must restart the WebRamp 700s for the changes to take effect.

NOTE – One-to-One NAT does not change firewall operation. Access to machines on the LAN from the Internet is not allowed unless Network Access Rules are set or Authenticated User sessions are established**.**

DHCP Server

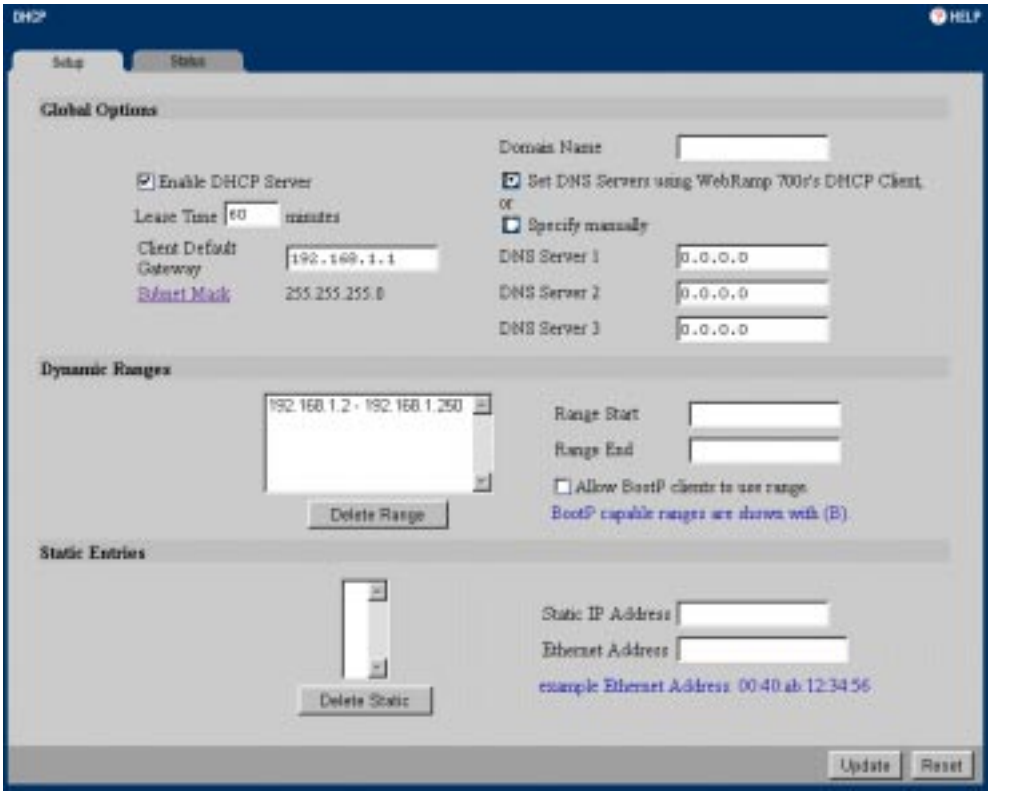
DHCP (Dynamic Host Configuration Protocol) allows computers on a network to access their TCP/IP settings from a centralized server.

Setup

Enter and change your DHCP server settings in the **Setup** window.

Click the **DHCP** button at the left side of the browser window. A window similar to the following appears.

Figure 3-38 DHCP Setup window



DHCP offers completely centralized management of TCP/IP client configurations, including IP addresses, gateway address, DNS address and more.

Global Options

Enable DHCP Server. To use the DHCP server, select the **Enable DHCP Server** option. The server is used by default. Do not use this DHCP server if there is already a DHCP server on the LAN or if you use manual addressing on the LAN computers.

Lease Time. The Lease Time is the amount of time that the TCP/IP address is given to the client machine, before the DHCP server attempts to renew the address. If the client still requires the use of the TCP/IP address, the DHCP Server continues to allow the client the use of that TCP/IP address for the same

amount of time. If the client no longer requires the TCP/IP address, the address is freed and returns to the pool of available addresses. The default value is 60 minutes.

Client Default Gateway. Enter the IP address of the WAN router used by LAN clients to access the Internet. If there is no WAN router, for example, if you access the Internet using a cable modem or DSL modem, enter the IP address of the WebRamp 700s in this field.

Subnet Mask. This value is used to determine what subnet an IP address belongs to. An IP address has two components, the network address and the host address. For example, suppose you enter the IP address 192.168.1.17. Assuming a Class C subnet mask of 255.255.255.0 is used, the first three numbers (192.168.1) represent the Class C network address, and the last number (17) identifies a particular host on this network. This value is set by clicking the **General** button and then clicking the **Network** tab.

Domain Name. Enter the registered domain name for the network in the Domain Name field, for example, “your-domain.com”.

DNS Server. The DNS Server translates host names into the numeric IP addresses used to route information to the correct machine. You can use multiple DNS servers to improve performance and reliability. Enter the TCP/IP address of one or more optional DNS servers in these fields.

Dynamic Ranges

When a client requests a TCP/IP address and the requester is a DHCP client, the WebRamp 700s DHCP server leases an address from the dynamic range.

NOTE – Before assigning an address from the dynamic range to a requesting client, the WebRamp 700s verifies that the address is not being used by another machine on the LAN.

Range Start...Range End. To create a range of dynamic IP addresses, enter the starting number in the **Range Start** field and the ending address in the **Range End** field. Click the **Update** button at the bottom of the screen. When the information has been updated, a confirmation message appears in the status line at the bottom of the window.

Delete Range. To remove a range of addresses from the dynamic pool, select the range from the dynamic ranges list and click the **Delete Range** button. The operation will take a few seconds to complete. When the range has been deleted, a confirmation message appears in the status line.

Allow BootP clients to use range. Select this option if you want dynamic BootP clients to be configured when they boot. Dynamic BootP clients do not have an IP address assigned to their MAC address. They are similar to DHCP clients, except that leases are not supported.

Static Entries

Static Range. Static addresses are used by machines that support BootP or those which require a fixed IP address, for example, machines running Web or FTP servers. When a a static address is assigned, a machine always gets the same IP address. This is not always true for dynamic addresses, whether it's a DHCP or dynamic BootP client.

Static IP Address and **Ethernet Address**. To create a static IP address, enter an IP address and the Ethernet (MAC) address of the client and then click the **Update** button at the bottom of the screen. When the information has been updated, a confirmation message appears in the status line at the bottom of the window.

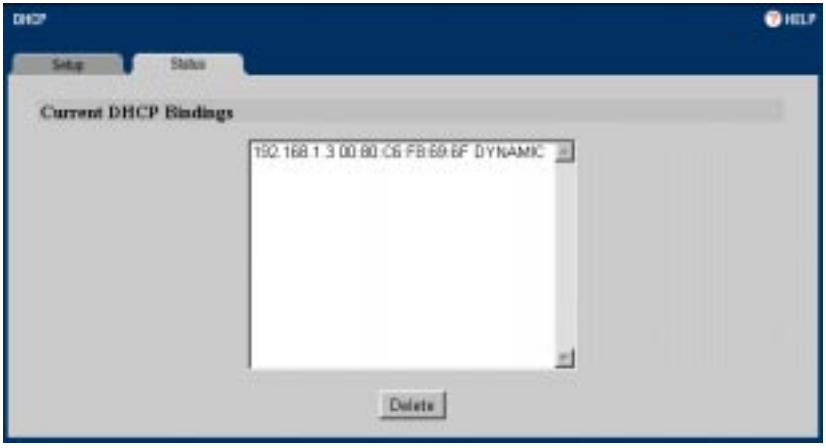
Delete Static. To remove a static address, select it from the Static Addresses list and click the **Delete Static** button. The operation will take a few seconds to complete. When the address has been deleted, a confirmation message appears in the status line at the bottom of the window.

Status

The DHCP Status window shows the details on the current bindings, IP and MAC address of the bindings, and the type of binding (Dynamic, Dynamic BootP, or Static BootP).

Click the **DHCP** button at the left side of the browser window and then click the **Status** tab at the top of the browser window. A window similar to the following appears.

Figure 3-39 DHCP Status window



To delete a binding, select the binding from the list and then click **Delete**. This frees the IP address in the DHCP server. The operation will take a few seconds to complete. When the binding has been deleted, a confirmation message is displayed in the Status line at the bottom of the window.

Click the **Refresh** or **Reload** button to reload the list of bindings. This may be necessary because Web pages are not automatically refreshed and new bindings may have been issued since the page was loaded.

VPN

The WebRamp 700s may be configured to support the Virtual Private Network (VPN) Point to Point Tunneling Protocol (PPTP). Once configured, the WebRamp 700s allows PPTP traffic from the Internet to the PPTP server on the LAN, and then to resources on the LAN.

The LAN IP Address (192.168.1.10) of the PPTP server must be entered in the Services screen. For more information, see Add Service.

If NAT is enabled, the address of the LAN server will be translated. For example, if the Web server on the LAN with the address 192.168.1.10 is entered in the Public LAN Server's “http” field, and the NAT Public IP Address is 200.200.200.200, users on the Internet will need to access 200.200.200.200.

NOTE – If PPTP is enabled, it is critical to maintain the security of the PPTP server. Make sure all security patches are installed and caution users to guard their account information.

Summary

The **Summary** window describes current VPN features and status.

Configure

The **Configure** window allows you to configure your VPN connection. An optional IPSec VPN Upgrade is available from Ramp Networks. See the Ramp Networks Online Store for information on upgrades.

Web site: **www.rampnet.com/order/index.html**

Phone: 1(408) 988-5353

Fax: 1(408) 988-6363

e-mail: sales@rampnet.com

Appendix

A

Technical Specifications

The WebRamp 700s Firewall has the following specifications:

Hardware Specifications

- CPU: MC 68360 @ 33mHz
- RAM: 4MB
- ROM: 128KB
- Flash: 2MB
- Real time clock (Year 2000 compliant)
- Convection cooled: no internal fan needed

Interfaces

- (5) 10BaseT

Power

- 5V / 1.5A AC adapter (included) for either 110v or 220v

Dimensions

- 8 x 4.25 x 1.5 inches
- 20 x 15.0 x 3.8 cm

Weight

- 1 lbs.
- .4 kg

LEDs (on front of unit)

- Power
- Test

LEDs Per Ethernet interface

- Link
- Transmit
- Receive

Appendix

B

IP Port Numbers

The port numbers are divided into three ranges: the Well Known Ports, the Registered Ports, and the Dynamic and/or Private Ports.

The Well Known Ports are those from 0 through 1023.

The Registered Ports are those from 1024 through 49151.

The Dynamic and/or Private Ports are those from 49152 through 65535.

Well Known Port Numbers

The Well Known Ports are controlled and assigned by the Internet Assigned Numbers Authority (IANA) www.iana.org, and on most systems can only be used by system processes, or by programs executed by privileged users. Many popular services, such as Web, FTP, SMTP/POP3 e-mail, DNS, and so on operate in this port range.

The assigned ports use a small portion of the possible port numbers. For many years the assigned ports were in the range 0-255. Recently, the range for assigned ports managed by the IANA was expanded to ports 0-1023.

Registered Port Numbers

The Registered Ports are not controlled by the IANA and on most systems can be used by ordinary user processes or programs executed by ordinary users.

While the IANA cannot control uses of these ports, it does list uses of these ports as a convenience.

The Registered Ports are in the range 1024-65535.

Visit ds.internic.net/rfc/rfc1700.txt for a list of IP port numbers.

Appendix

C

Installing a Proxy Server

Installing a proxy server improves the speed of web access on the LAN and lessens the load on the Internet connection.

There are several shareware and freeware proxy servers that run under Windows 95 and NT, as well as UNIX and Linux. Commercial products from Microsoft, Netscape, and others are available for Windows, MacOS, and UNIX.

Installation

The following example describes how to install a proxy server on the WAN port.

NOTE – When a proxy server is installed on the WAN port, it is important that you configure the WebRamp 700s **Intranet** settings to allow LAN users to access the proxy. If this is not done, users will not be able to access the proxy.

---

1. **Install Proxy Server**

   Install and configure the proxy server software using a valid IP address. Plug the proxy server into an Ethernet hub connected to the WebRamp 700s WAN port.

2. **Configure Intranet settings**

In the WebRamp 700s interface, click the **Advanced** button on the left side of the browser window, and then click the **Intranet** tab. In the window, select the **Specified Address Ranges Are Attached to the WAN Link** option, enter the proxy server's IP address range**,** and then click **Update**. For a detailed description of all Intranet settings, see Configuration.

3. **Configure web Proxy Relay**

   In the WebRamp 700s interface, click the Advanced button on the left side of the browser window, and then click the **Proxy Relay** tab. Enter the name or the IP address and the port information for the web proxy relay, and then click **Update.** After configuration, all web traffic will be directed to the proxy, which will fulfill all requests, without your needing to reconfigure any web browsers on the LAN.

Index

F

G

H

I

J

K

L

M

N