WebRamp 700s Reference

For Windows and Macintosh

Copyright

Trademarks

Where to Contact for Help

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 Installation Guide* and the *WebRamp 700s Reference* 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, 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

ramp
NETWORKS

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

B. Sridhar

Sridhar Bathina
Vice President
Engineering Project Management
Ramp Networks, Inc.
February 1, 1999

Warranty and Software License

Your Ramp Networks product is covered by a Limited Warranty. Ramp Networks warrants that the 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. Ramp Networks warrants its software for 90 days from the date of purchase and warrants that the software will execute its programming instructions when properly installed on the computer for which it is intended, and that the media upon which the software is recorded will be free from defects in materials and workmanship under normal use.

During the Limited Warranty period, Ramp Networks will repair or replace the 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. The sole remedy for software shall be to return the media to Ramp Networks for replacement. 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 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 WebRamp.

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 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 PRODUCT. RAMP NETWORKS AND ITS LICENSOR(S) MAKE NO OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, REGARDING THE ENCLOSED 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 PRODUCT IN TERMS OF ITS CORRECTNESS, ACCURACY, RELIABILITY, CURRENTNESS, OR OTHERWISE. THE ENTIRE RISK AS TO THE RESULTS AND PERFORMANCE OF THE 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 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 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 Reference

Thank you for purchasing the WebRamp 700s. The WebRamp 700s acts as a secure barrier between the private LAN and the public Internet to prevent theft, destruction, and modification of data on the LAN by unauthorized Internet users, as well as to filter incoming data for objectionable content from Web sites and Newsgroups.

Audience

This reference is for the network manager or network installer. It assumes that this person has the following background:

- Familiarity with Ethernet networks.
- Knowledge of how to install and handle electronically sensitive equipment.

Organization of This Reference

The WebRamp 700s Reference provides detailed information about the commands and functions of the WebRamp as well as advanced configuration information. This reference complements the “WebRamp 700s Installation Guide”, which provides an introduction to the 700s, installation information, and information about how the WebRamp 700s works with other WebRamp models.

The WebRamp 700s Reference is organized as follows:

Chapter 1, *Managing the WebRamp 700s,* describes how to configure all aspects of the WebRamp 700s using a Web browser. This chapter also contains a command reference section for procedures such as configuring, rebooting and resetting the WebRamp 700s, setting back to defaults, uploading new software, and changing the WebRamp 700s password.

Chapter 2, *WebRamp 700s Plus Configuration*, describes how to configure the Intranet support and other optional functions of WebRamp 700s.

Chapter 3, *Troubleshooting,* lists solutions to commonly encountered problems.

Chapter 4, *Introduction to Networking,* provides a non-technical overview of LANs, the Internet, firewalls, filters, and other topics relevant to the use of the WebRamp 700s. This chapter also includes a discussion of IP addressing.

Appendix A, *Cable Specifications and Pinouts*, provides information about cables and pinout diagrams for all connectors on the WebRamp 700s.

Appendix B, *Technical Specifications,* lists the technical specifications for the WebRamp 700s as a quick reference.

Appendix C, *Optional Direct Connection,* describes how to connect the WebRamp 700s directly to a PC with a Web browser for initial configuration.

Appendix D, *IP Port Numbers*, describes the three ranges of port numbers.

The *Index* provides a cross-reference to terms, features, and commands used throughout the manual.

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(408) 988-5353

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

Chapter

1

Managing the WebRamp 700s

This chapter contains detailed information about the WebRamp 700s management commands and functions. These commands and functions are accessed via 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 dedicated to the major windows and functions within the Web management interface. Topics covered include:

- Using the Web browser
- Network Settings window
- Enabling Network Address Translation (NAT)
- Setting the administrator’s password
- Logging and alerts
- Content filtering and blocking
- Network access rules
- Additional commands and functions

Using the Web Browser

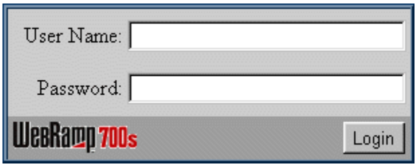
All management functions on the WebRamp 700s are performed from a Web browser application using the WebRamp 700s Web Management Interface. Management can be performed from any computer connected to the same network as the WebRamp 700s. Any computer used for management will be referred to as a Management Station.

The Web Management Interface uses Java technology for security and other functions. For this reason, it is necessary to enable Java and JavaScript on the Management Station's Web browser. It is not necessary to enable these protocols on any other machines on the network, nor is it necessary to enable ActiveX anywhere.

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 they are not blocked if the Java and ActiveX blocking features are enabled on the WebRamp 700s.

NOTE – The Web browser software used must be Java-enabled. The browser must also support HTTP uploads in order to fully manage the WebRamp 700s. If a browser that does not support HTTP uploads is used, certain features, such as updating the software and uploading pre-configured settings, will not work. As of the writing of this manual, only Netscape Navigator 3.0 and above has the necessary features. Netscape Communicator is available on the WebRamp 700s CD.

Type the WebRamp 700s address or host name into the Location field at the top of the browser window and hit the Return key. During initial configuration, this IP address is 192.168.168.168. The Password dialog box, similar to the one shown below, will appear:



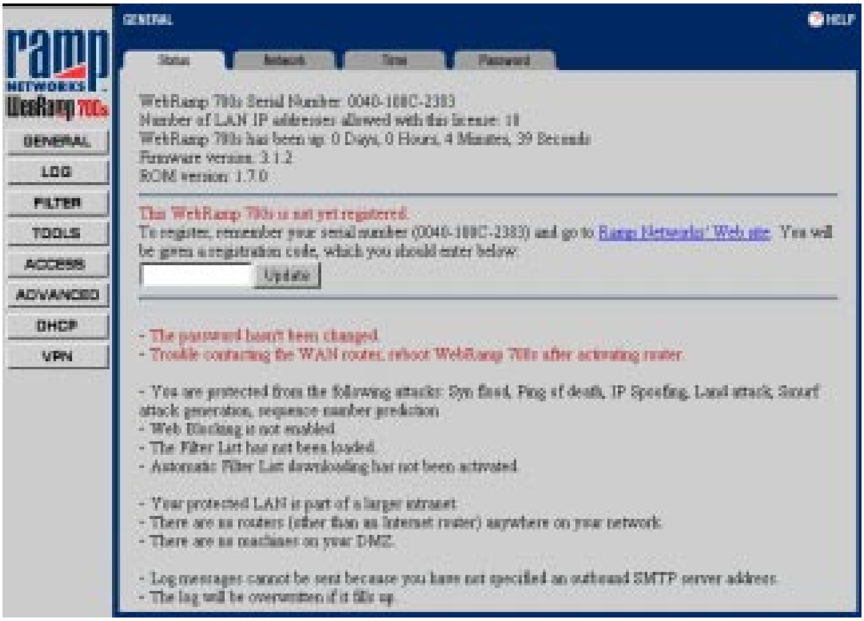
Enter **admin** into the **User Name** field and the password configured during initial configuration into the **Password** field. Click the **Login** button.

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 the administrator logs into the Web Management Interface. If the password does not grant access to the WebRamp 700s, it may be because a cached copy of the page is being displayed instead of the correct page. Click **Reload** or **Refresh** on the Web browser and try again.

Once the administrator’s password is entered, an **authenticated management session** is established. For security reasons, a management session can only be established from a machine which is connected to the **LAN** port. The session will time out after 5 minutes of inactivity and the **Authentication** window will be displayed when any management functions are attempted. This time-out interval is not configurable.

Enter the password exactly as defined and click the **Login** button. A window similar to the one shown below is displayed.



WebRamp 700s Serial Number: 0040-108C-2383
Number of LAN IP addresses allowed with this license: 18
WebRamp 700s has been up: 0 Days, 0 Hours, 4 Minutes, 39 Seconds
Firmware version: 3.1.2
ROM version: 1.7.0

This WebRamp 700s is not yet registered.
To register, remember your serial number (0040-108C-2383) and go to Ramp Networks' Web site. You will be given a registration code, which you should enter below.

- The password hasn't been changed
- Trouble contacting the WAN router, reboot WebRamp 700s after activating router.

- You are protected from the following attacks: Syn flood, Ping of death, IP Spoofing, Land attack, Smurf attack generation, sequence number prediction
- Web Blocking is not enabled
- The Filter List has not been loaded
- Automatic Filter List downloading has not been activated

- Your protected LAN is part of a larger intranet
- There are no routers (other than an Internet router) anywhere on your network
- There are no machines on your DMZ

- Log messages cannot be sent because you have not specified an outbound SMTP server address
- The log will be overwritten if it fills up

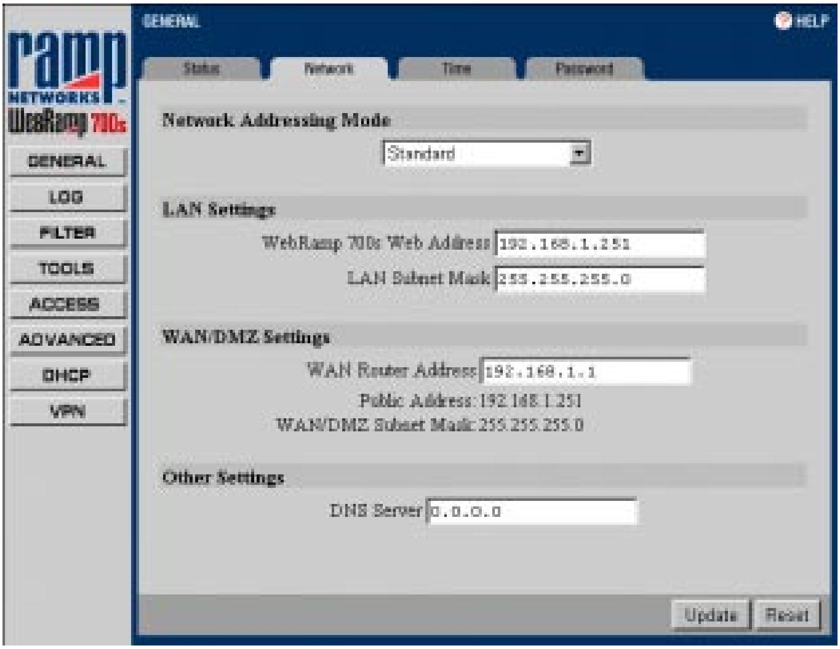
Along the left side of the window is a row of buttons. When one of these buttons, **General**, **Log**, **Filter**, **Tools**, **Access**, **Advanced**, **DHCP**, and **VPN** is clicked, additional related management functions may be selected by clicking on the tab at the top of the window. This button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

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

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 Settings Window

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



Network Addressing Mode

Standard

LAN Settings

WebRamp 700s Web Address 192.168.1.251

LAN Subnet Mask 255.255.255.0

WAN/DMZ Settings

WAN Router Address 192.168.1.1

Public Address: 192.168.1.251

WAN/DMZ Subnet Mask 255.255.255.0

Other Settings

DNS Server 0.0.0.0

Mode

The **Mode** popup menu includes three options: **Standard**, **NAT Enabled**, and **NAT With DHCP Client**. Select **Standard** if the network uses valid IP addresses or the router supports the NAT functionality and it will be used instead of enabling NAT on the WebRamp 700s. Select **NAT Enabled** if the network will use private TCP/IP addresses with two or more valid IP addresses in a subnet provided by the ISP and there is a WAN router. Select **NAT With DHCP Client** if the ISP provides the IP address from a remote DHCP server on the WAN. For example, when a cable modem or xDSL modem is used to provide the Internet connection.

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 the router has NAT enabled, they can use private addresses. The following information is required:

- **LAN Settings**
  - **WebRamp 700s Web Address.** This is the IP address that is given 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, consider the IP address 192.168.228.17. Assuming a Class C subnet mask of 255.255.255.0 is used, the first three numbers (192.168.228.) represent the Class C network address, and the last number (17) identifies a particular host on this network.
- **WAN Settings**
  - **WAN Router Address.** WAN router address, also called the default gateway, is the address of the router that attaches the LAN to the Internet through ISDN, a T1 line, or some other transmission medium.
  - **Public 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.** This server is used by the WebRamp 700s to lookup the addresses of machines used to download the Content Filter List, and for the built-in DNS Lookup tool.

Enter the required values and click the **Update** button at the bottom of the screen to send the configuration data to WebRamp 700s. The operation will take a few seconds to complete. Once completed, a message confirming the update will be displayed in the status line at the bottom of the window.

NOTE – Restart the WebRamp 700s for changes to take effect.

NAT Enabled

NOTE – The WebRamp 700s has NAT enabled by default. If NAT is enabled on your router, then you can use **Standard** mode.

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:

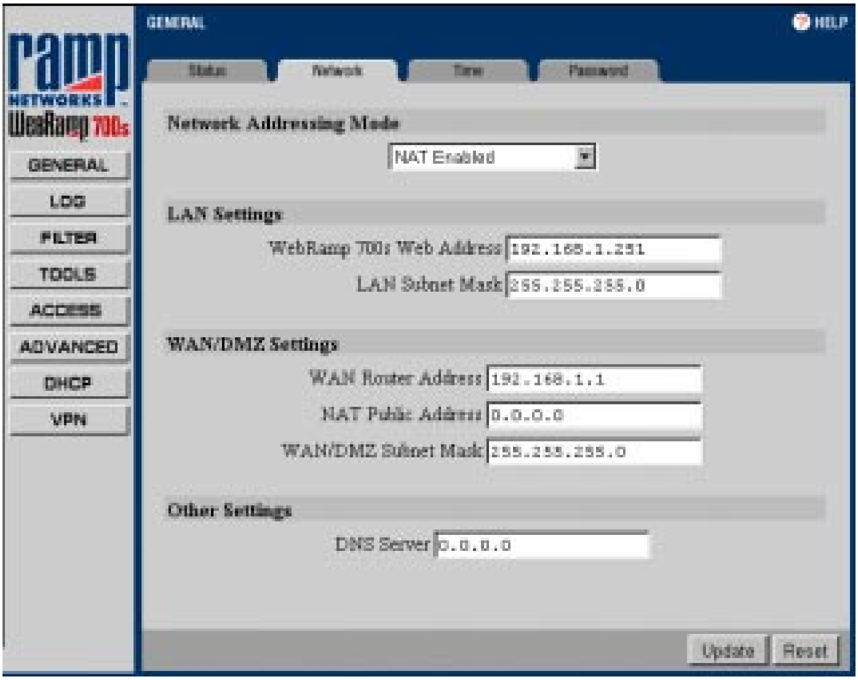
1. Additional security is provided because all the addresses on the LAN are invisible to the outside world.
2. In cases where a network uses invalid TCP/IP addresses or if addresses are in short supply, NAT can be used to connect the LAN to the Internet without changing the TCP/IP addresses of computers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

When using TCP/IP addresses on a LAN which have not been assigned by an Internet Service Provider, it is a good idea to use addresses from a special address range allocated for this purpose. The following IP address ranges are to be used for private IP networks and do not get routed on the Internet:

10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255

In cases where an address range has arbitrarily been selected, such as where a network uses invalid TCP/IP addresses, Internet sites which have been assigned that range will not be accessible from the LAN. For example, if the address range 199.2.23.1-199.2.23.255 is used on the LAN, a Web server on the Internet with the address of 199.2.23.20 will not be accessible.

NAT Enabled should be selected if the network uses private TCP/IP addresses or if addresses are in short supply. To activate Network Address Translation, select **NAT Enabled** from the **Network Addressing Mode** popup. A window similar to the following will be displayed.



Network Addressing Mode

NAT Enabled

LAN Settings

WebRamp 700s Web Address 192.168.1.251

LAN Subnet Mask 255.255.255.0

WAN/DMZ Settings

WAN Router Address 192.168.1.1

NAT Public Address 0.0.0.0

WAN/DMZ Subnet Mask 255.255.255.0

Other Settings

DNS Server 0.0.0.0

The following information is required:

- **LAN Settings**
  - **The WebRamp 700s Web Address**. This is the IP address that is given 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, consider the IP address 192.168.228.17. Assuming a Class C subnet mask of 255.255.255.0 is

used, the first three numbers (192.168.228.) represent the Class C network address, and the last number (17) identifies a particular host on this network.

- **WAN Settings**
  - **WAN Router Address.** WAN router address, also called the default gateway, is the address of the router that attaches the LAN to the Internet through ISDN, a T1 line, or some other transmission medium.
  - **NAT Public Address.** This is the IP address used to access the Internet. It will be the only address seen by Internet users and all activity on the Internet from the LAN will seem to originate from this address. This address must be a valid address and is often supplied by the ISP.
  - **WAN Subnet Mask.** The WAN Subnet Mask is used when NAT is enabled.
- **Other Settings**
  - **DNS Server**. This server is used by the WebRamp 700s to lookup the addresses of machines used to download the Content Filter List, and for the built-in DNS Lookup tool.

Enter the required values and click the **Update** button at the bottom of the screen to send the configuration data to the WebRamp 700s. The operation will take a few seconds to complete. Once completed, a message confirming the update will be displayed at the bottom of the window.

NOTE – It is necessary to 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**, use the **WebRamp 700s Web Address** as the router address used by these computers to access the Internet.

For example, consider the following situation:

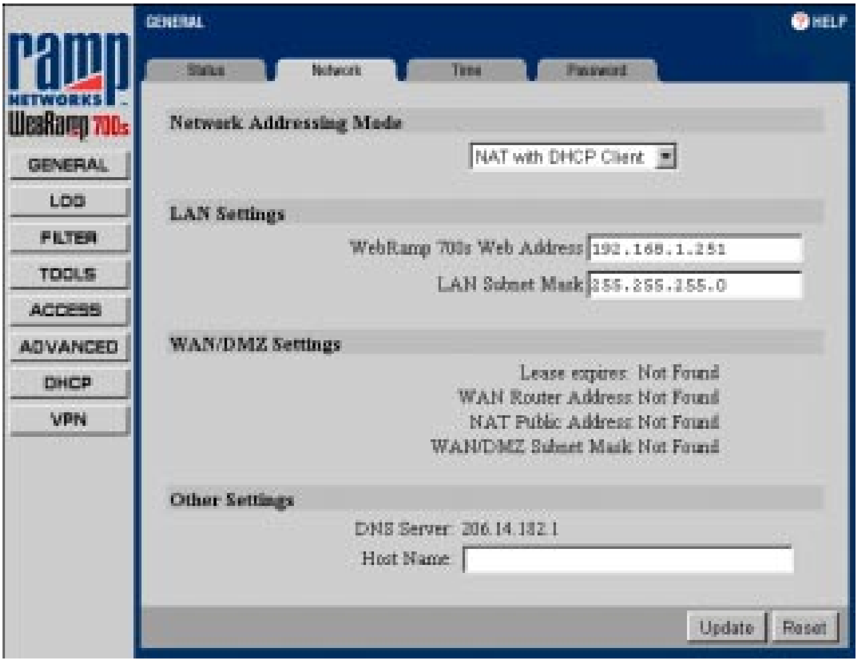
- The computers on the LAN have addresses in the private range of 192.168.168.10 to 192.168.168.255.
- The router has the valid Internet address of 128.1.1.1.
- The the WebRamp 700s has 128.1.1.25 as the valid Internet address, or **NAT Public IP Address**, and 192.168.168.50 as its the **WebRamp 700s 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 192.168.168.10 because the router's address is not within the private range. In this case, use the **WebRamp 700s Web Address** as the router for all the machines on the network - in this case: 192.168.168.50. If NAT is active without using addresses in the private range, then this may not be necessary. For example, if the network was assigned the address range of 199.2.23.1 to 199.2.23.255 by the ISP, NAT is enabled with the public address of 199.2.23.50, 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 can get its NAT Public IP address, as well as WAN Router address, and WAN Subnet Mask from a remote DHCP server on the WAN. If a Cable Modem or xDSL service is used for the Internet connection, selecting **NAT with DHCP Client** from the **Network Addressing Mode** popup may be required as some cable modem and xDSL ISPs are implementing DHCP in their service. If this Mode is selected, a window similar to the following will be displayed.



Network Addressing Mode

NAT with DHCP Client

LAN Settings

WebRamp 700s Web Address: 192.168.1.251

LAN Subnet Mask: 255.255.255.0

WAN/DMZ Settings

Lease expires: Not Found

WAN Router Address: Not Found

NAT Public Address: Not Found

WAN/DMZ Subnet Mask: Not Found

Other Settings

DNS Server: 206.14.182.1

Host Name:

- **LAN Settings**
  - **The WebRamp 700s Web Address**. This is the IP address that is given 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, consider the IP address 192.168.228.17. Assuming a Class C subnet mask of 255.255.255.0 is used, the first three numbers (192.168.228.) represent the Class C network address, and the last number (17) identifies a particular host on this network.
- **WAN Settings**
  - **Lease Expires**. This value shows when the IP address lease obtained from the DHCP server expires. This value is assigned by the ISP's DHCP server.
  - **WAN Router Address.** WAN router address is assigned by the ISP's DHCP server.

  - **NAT Public Address.** This is the IP address used to access the Internet. It will be 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.** The WAN Subnet Mask is used when NAT is enabled. This value is assigned by the ISP's DHCP server.
- **Other Settings**
  - **DNS Server**. This server is used by the WebRamp 700s to lookup the addresses of machines used to download the Content Filter List, and for the built-in DNS Lookup tool. This value is assigned by the DHCP server.
  - **Host Name**. Enter the host name.

Enter the required values and click the **Update** button at the bottom of the screen to send the configuration data to the WebRamp 700s. The operation will take a few seconds to complete. Once completed, a message confirming the update will be displayed at the bottom of the window.

NOTE – 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**, use the **WebRamp 700s Web Address** as the router address used by these computers for accessing the Internet.

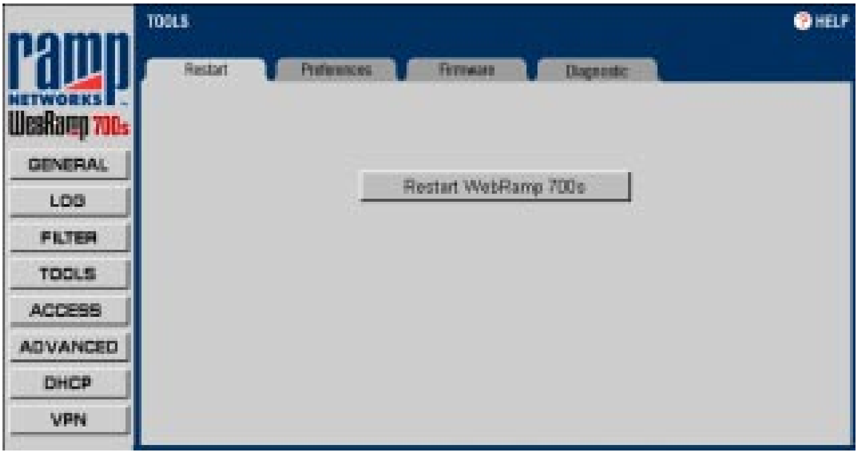
For example, consider the following situation:

- The computers on the LAN have addresses in the private range of 192.168.168.10 to 192.168.168.255.
- The computers on the LAN have addresses in the private range of 192.168.168.10 to 192.168.168.255.
- 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 192.168.168.50 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 192.168.168.10 because the router's address is not within the private range. In this case, use the **WebRamp 700s Web Address** as the router for all the machines on the network - in this case: 192.168.168.50.

Restart the WebRamp 700s

Click the button labeled **Tools** at the left side of the browser window. Then, click the tab labeled **Restart**. A window similar to the following will be displayed.

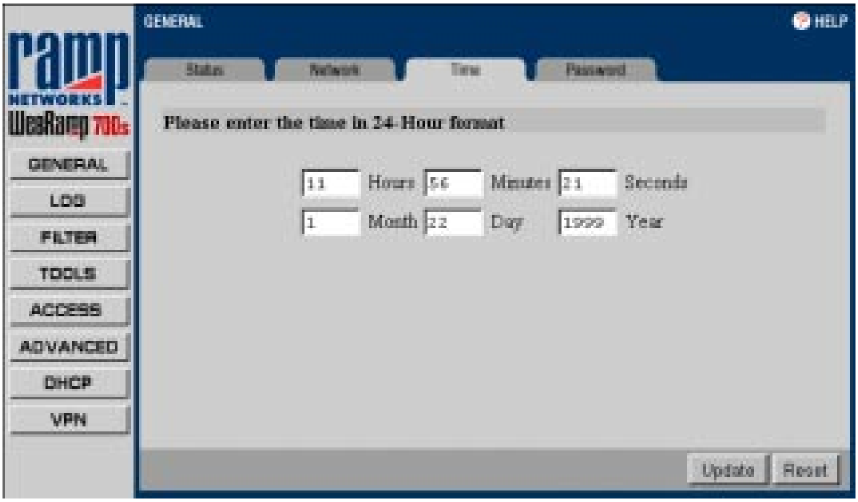


Click the button labeled **Restart the WebRamp 700s**, then the **Yes** button to confirm the restart and send the restart command to the WebRamp 700s. The restart will take about 90 seconds, during which time the WebRamp 700s will be unreachable from the Web browser and all network traffic through it will be halted.

NOTE – If initial configuration is being done, remember to reset the IP address of the Management Station back to its original setting once completed. Depending on the operating system of the Management Station, it may be necessary to restart the Management Station for the change to take effect.

Set Date and Time

Click the tab labeled **Time** at the top of the browser window. A window similar to the following will be displayed.



Please enter the time in 24-Hour format

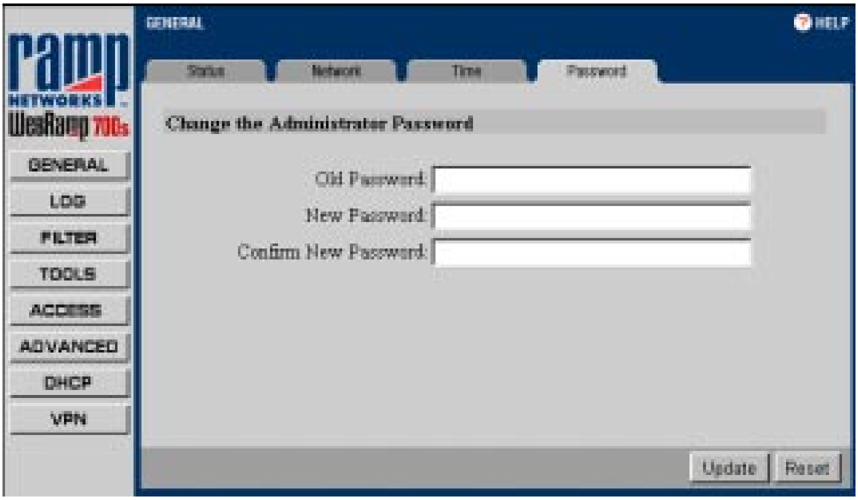
11 Hours 56 Minutes 21 Seconds
1 Month 22 Day 1999 Year

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

Enter the time in 24-hour format and click the **Update** button to send the configuration data to the WebRamp 700s. The operation will take a few seconds to complete. Once completed, a message confirming the update will be displayed in the status line at the bottom of the window.

Set Admin Password

Click the tab labeled **Password** at the top of the browser window. A window similar to the following will be displayed.



Change the Administrator Password

Old Password:

New Password:

Confirm New Password:

The security of the WebRamp 700s is maintained by the use of an Administrator Password. To set this password, enter the old password in the **Old Password** field, and the new password in the **New Password** and **Confirm New Password** fields and click the **Update** button to send the configuration data to the WebRamp 700s. The operation will take a few seconds to complete. Once completed, a message confirming the update will be displayed 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, the operation will fail. This is done to protect against mistyping a password and being accidentally locked out of the WebRamp 700s.

NOTE – The password cannot be recovered if it is lost or forgotten. If the password is lost, it will be necessary to reset the WebRamp 700s to its factory default state. Please contact Ramp Network’s Technical Support team for instructions.

Logging and Alerts

The WebRamp 700s maintains an event log, which contains events that may be security concerns. This log may be viewed with a browser using the WebRamp 700s Web-managed interface or automatically and periodically sent as a tab-delimited text file to any E-mail address for convenience and archival purposes.

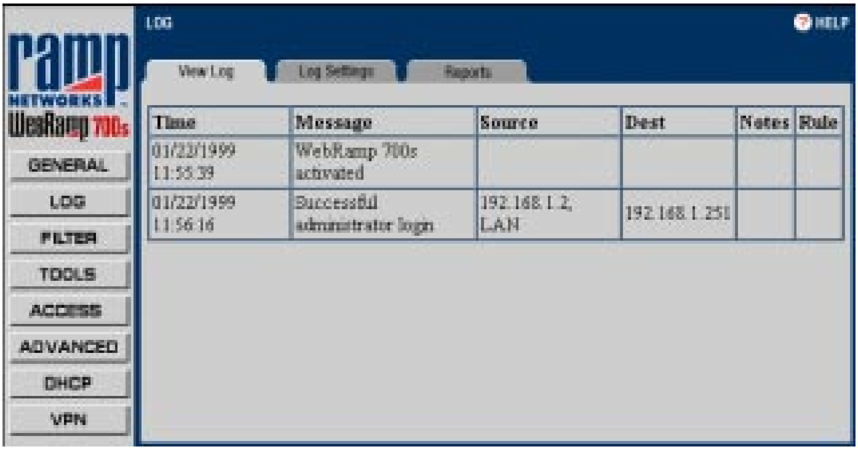
In some cases, the administrator may wish to be alerted of high-priority information, such as an attack on a server. In such cases, this information may be immediately E-mailed, either to the main E-mail address used by the log, or to a different address, such as a paging service.

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/unsuccessful loading of the Content Filter List

NOTE – Some administrators may wish to carefully monitor the log, whereas others may wish only to be notified of important events. If maintaining complete log information is of critical importance, connect the WebRamp 700s to an uninterruptable power supply (UPS) to protect current log information, which is lost during power interruptions.

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



Time	Message	Source	Dest	Notes	Rule
01/22/1999 11:55:39	WebRamp 700s activated				
01/22/1999 11:56:16	Successful administrator login	192.168.1.2, LAN	192.168.1.251		

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 display the log data most efficiently. Depending on the browser, it should be possible to copy entries from the log and paste them into documents. Alternatively, use the **E-mail Log** function and review the log with an E-mail client rather than with a Web browser. Set the **E-mail log** by clicking **Log Settings** and filling in the appropriate fields.

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

- **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 will be shown. If the packet was TCP or UDP, the port number, in parentheses, will follow each address. If the packet was CMP, the number in parentheses will be 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 a machine that attempted to connect to the blocked site or newsgroup will be displayed. In most cases, the name of the site which was

blocked will also be shown. In addition, there will be a field labeled **Code** which contains one or more lowercase letters. These correspond to the Content Filter List categories as follows:

a = Violence/profanity
b = Partial nudity
c = Full nudity
d = Sexual acts
e = Gross depictions
f = Intolerance
g = Satanic/cult
h = Drug culture
i = Militant/extremist
j = Sex education
k = Gambling/illegal
l = Alcohol/tobacco

Descriptions of these categories are listed in this manual.

- **ActiveX, Java, or Code Archive blocked**. The IP addresses of the source machine and the destination server will be shown.

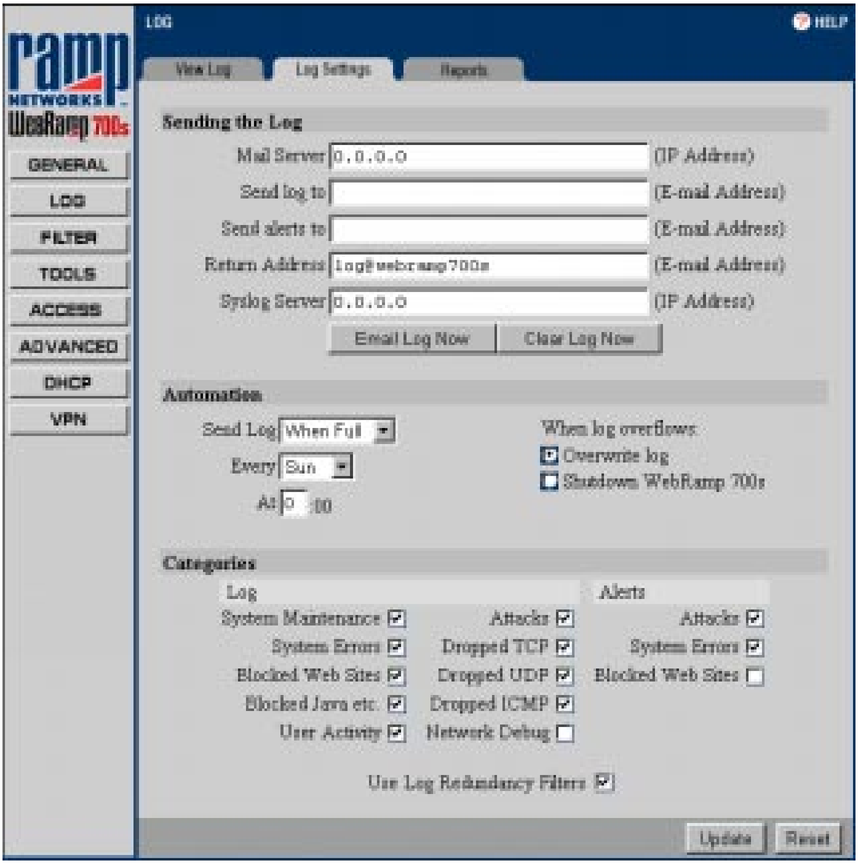
NOTE – When ActiveX or Java code is compressed into an archive it is not always possible to differentiate between the two. If either ActiveX or Java blocking is enabled, all code archives will be blocked.

- **Cookie blocked.** The IP addresses of the local machine and the remote server will be 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, will be shown. In these attacks, the source address shown will usually be fake and usually cannot be used to determine the source of the attack.

NOTE – Varying conditions on the Internet can produce conditions which may cause the appearance of an attack, 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 calls the attack “possible”, or if it happens on an irregular basis, then there is probably no attack in progress. If the log message calls 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 steps must be taken.

Log Settings

Click the button labeled **Log** on the left side of the browser window and then click the tab labeled **Log Settings** at the top of the window. A window similar to the following will be displayed.



Sending the Log

Mail Server 0.0.0.0 (IP Address)
Send log to (E-mail Address)
Send alerts to (E-mail Address)
Return Address log@webramp700s (E-mail Address)
Syslog Server 0.0.0.0 (IP Address)

Automation

Send Log When Full
Every Sun
At 0 :00

When log overflows:
☑ Overwrite log
□ Shutdown WebRamp 700s

Categories

Log				Alerts	
System Maintenance	☑	Attacks	☑	Attacks	☑
System Errors	☑	Dropped TCP	☑	System Errors	☑
Blocked Web Sites	☑	Dropped UDP	☑	Blocked Web Sites	□
Blocked Java etc.	☑	Dropped ICMP	☑		
User Activity	☑	Network Debug	□		

Use Log Redundancy Filters ☑

Sending the Log

- **Mail Server**. To enable sending log or alert messages via E-mail it is necessary to enter the numerical TCP/IP address of the SMTP server. The Internet Service Provider used to connect the network to the Internet should be able to provide this information. If this field is left blank, log and alert messages will not be sent via E-mail. The **DNS Lookup** utility under the **Tools** button may be used to find the IP address of the mail server.
- **Send Log To.** This is the E-mail address to which log files will be sent and must be a fully qualified address (username@mydomain.com). Once sent, the log file is cleared from the memory of the WebRamp 700s. If this field is left blank, log messages will not be 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 an E-mail account, or E-mail pager. Enter the fully qualified E-mail address (username@mydomain.com) to which alert messages will be sent in this field. This may be a standard E-mail account or, quite often, a paging service. If this field is left blank, alert messages will not be sent via E-mail.
- **Return Address.** Enter an E-mail address in this field which the WebRamp 700s will use as the Return Address for all log and alert messages sent. This serves two functions. First, if the mail server has SPAM filtering enabled, a valid address may be required for mail to be delivered. Second, organizations with multiple WebRamp 700s units may use different E-mail addresses to identify the source of the message. The default entry is “log@webramp700s”.
- **Syslog Server.** In addition to the standard screen log, the WebRamp 700s is able to 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 are 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.

Automatic

- **Send Log.** This pop-up menu is used to configure the frequency of log messages being sent as E-mail: daily, weekly, or only when the log is full. If the weekly or the daily option is selected, specify the day of the week and the time of day when the E-mail should be sent. If the weekly option is selected, specify which day of the week the E-mail should be sent. If the weekly or daily option is selected 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, which may happen if there is a problem with the mail server and the log cannot be successfully E-mailed. The default behavior in this situation is to overwrite the log and discard its contents. However, there is an option to have the WebRamp 700s shut down instead, which prevents any further traffic from traveling through without being logged.

Log Categories

Click the checkbox to enable or disable the generation of the following log message categories.

- **System Maintenance.** When enabled, log messages showing general system maintenance activity, such as administrator logins, automatic loading of Content Filter Lists, activation and restarting the WebRamp 700s, will be generated. Enabled by default.
- **System Errors.** When enabled, log messages showing problems with DNS, E-mail, and automatic Content Filter List loading will be generated. Enabled by default.
- **Blocked Web Sites.** When enabled, log messages showing Web sites, newsgroups, or other services blocked by the Content Filter List, by keyword, or for any other reason will be generated. Enabled by default.
- **Blocked Java, ActiveX, and Cookies.** When enabled, log messages showing Java, ActiveX, and Cookies which are blocked by the WebRamp 700s will be generated. Enabled by default.

- **User Activity.** When enabled, log messages showing any successful or unsuccessful user logins will be generated. Enabled by default.
- **Attacks.** When enabled, log messages showing SYN Floods, Ping of Death, IP Spoofing, and attempts to manage the WebRamp 700s from the Internet will be generated. Enabled by default.
- **Dropped TCP.** When enabled, log messages showing blocked incoming TCP connections will be generated. Enabled by default.
- **Dropped UDP.** When enabled, log messages showing blocked incoming UDP packets will be generated. Enabled by default.
- **Dropped ICMP.** When enabled, log messages showing blocked incoming ICMP packets will be generated. Enabled by default.
- **Network Debug.** When enabled, log messages showing Ethernet broadcasts, ARP resolution problems, ICMP redirection problems, and NAT resolution problems will be generated. This category is intended for experienced network administrators. Disabled by default.

Alert Categories

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 enabled, all log entries that are categorized as an **Attack** will be generated as an alert message. Enabled by default.
- **System Errors.** When enabled, all log entries that are categorized as a System Error will be generated as an alert message. Enabled by default.
- **Blocked Web Sites.** When enabled, all log entries that are categorized as a Blocked Web Site will be generated as an alert message. Disabled by default.

Use Log Redundancy Filters

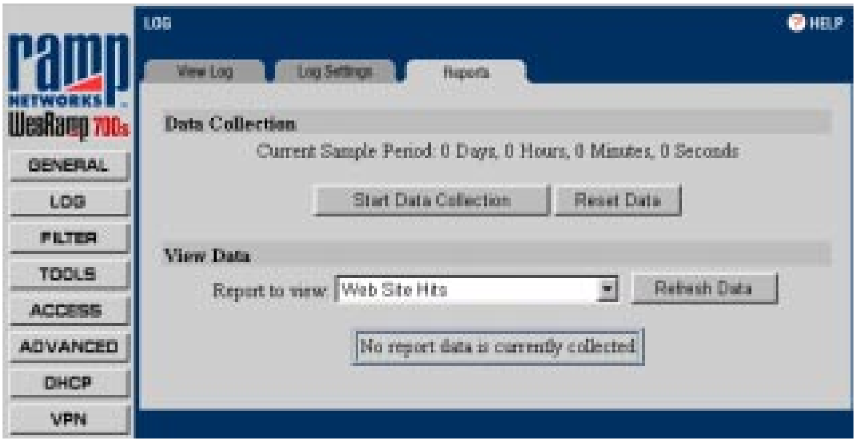
Prevents duplicate consecutive log messages from being generated. Because of network retry mechanisms, duplicate consecutive messages are common. If the **Use Log Redundancy Filters** box is checked, a log entry identical to the previous entry will not be generated. Enabled by default.

Click the **Update** button to send the configuration data to the WebRamp 700s. The operation will take a few seconds to complete. Once completed, a message confirming the update will be displayed at the bottom of the window.

Log 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 button labeled **Log** on the left side of the browser window and then click the tab labeled **Reports** at the top of the window. A window similar to the following will be displayed.



Current Sample Period: 0 Days, 0 Hours, 0 Minutes, 0 Seconds

Report to view: Web Site Hits

No report data is currently collected

Data Collection

The WebRamp 700s allows collection of data.

- **Start Data Collection.** By default, the log analysis function is disabled. Click the **Start Data Collection** button to begin log analysis. When log analysis is enabled, the button will read Stop **Data Collection**.
- **Reset Data.** Click the **Reset Data** 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

- **Current Sample Period.** Displays the current sample period reflected in the reports.
- **Report to View.** Select the desired report from the Display Report popup menu. The options are **Web Site Hits**, **Bandwidth Usage by IP Address**, and **Bandwidth Usage by Service**. These reports are explained below.

- **Web Site Hits**. Selecting **Web Site Hits** from the **Display Report** popup menu will display a table showing the URL for the 25 most often accessed Web sites and the number of hits to that site during the current sample period.

  The **Web Site Hits.** This report will help ensure the majority of Web access is to sites considered applicable to the 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 the organization's Acceptable Use Policy.

- **Bandwidth Usage by IP Address**. Selecting **Bandwidth Usage by IP Address** from the **Display Report** popup menu will display 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 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.

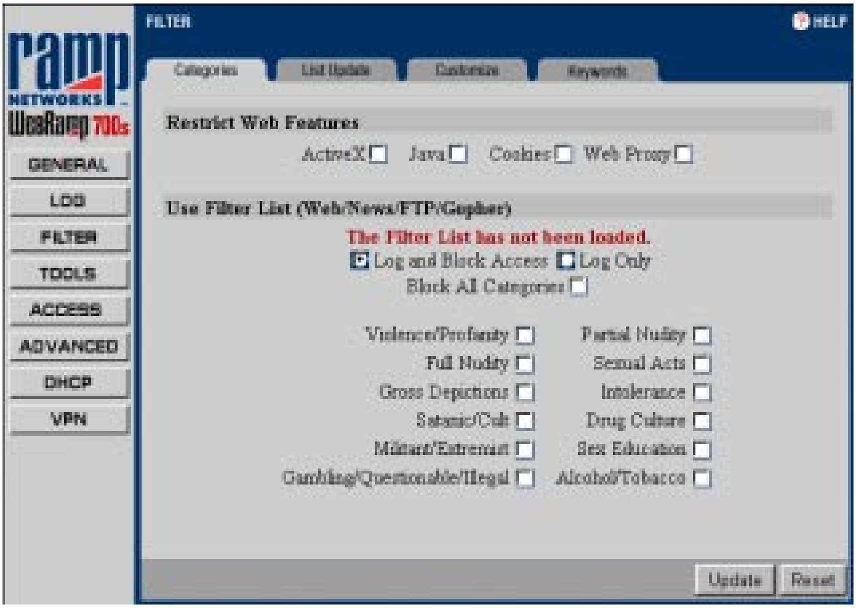
- **Bandwidth Usage by Service**. Selecting **Bandwidth Usage by Service** from the **Display Report** popup menu will display a table showing the name of the 25 top Internet services, such as HTTP, FTP, RealAudio, etc. during the current sample period.

  The **Bandwidth Usage by Service** report is useful to make sure the Internet services being used are appropriate for the 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 the organization's Acceptable Use Policy.

- **Refresh Data**. Pressing the **Refresh Data** button refreshes the data.

Content Filtering and Blocking

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



Restrict Web Features

ActiveX □ Java □ Cookies □ Web Proxy □

Use Filter List (Web/News/FTP/Gopher)

The Filter List has not been loaded.

☒ Log and Block Access □ Log Only

Block All Categories □

Violence/Profanity □ Partial Nudity □
Full Nudity □ Sexual Acts □
Gross Depictions □ Intolerance □
Satanic/Cult □ Drug Culture □
Militant/Extremist □ Sex Education □
Gambling/Questionable/Illegal □ Alcohol/Tobacco □

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

The options are grouped into two main categories:

- Restrict Web Features
- Use Filter List (Web/News/FTP/Gopher)

Restrict Web Features

- **ActiveX**. ActiveX is a programming language that is used to embed small programs in Web pages. It is generally considered an insecure protocol to allow into a network 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, also called applets, in Web pages. It is generally considered safer than ActiveX since it has more thorough safety mechanisms. However, some administrators may choose 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 lead to a user-friendly Web by providing service based on ID. Unfortunately, cookies can be programmed not only to identify the visitor to the site, but also to track that visitor's activities. Because they represent a potential loss of privacy, some administrators may choose to block cookies.
- **Web Proxy.** When a proxy server is located on the WAN, it is possible for LAN users pointing to this proxy server to circumvent content filtering. This feature disables access to proxy servers located on the WAN. It has no effect on those 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 WebRamp 700s utilizes a Content Filter List that is managed by Microsystems' CyberNOT Oversight Committee to block access to sites which have been classified to fall within the following categories. 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, and the PTO, as well as a superintendent of schools, a social worker, a psychologist, and a minister. When the WebRamp 700s is first purchased, upon registration, a one month subscription to the Content Filter List updates is included.

- **Log and Block Access**. When selected, the WebRamp 700s will log the attempt and block access to all sites on the Content Filter, custom, and keyword lists.
- **Log Only.** When selected, the WebRamp 700s will log and then allow access to all sites on the Content Filter, custom, and keyword lists. This function gives the network manager the ability to monitor appropriate usage without restricting access.

- **Block all Categories**. When selected, the WebRamp 700s blocks all 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 is 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 by: 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 (graphics or text)

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 (graphics or text)

Pictures or text advocating the sale, consumption, or production of alcoholic beverages and tobacco products.

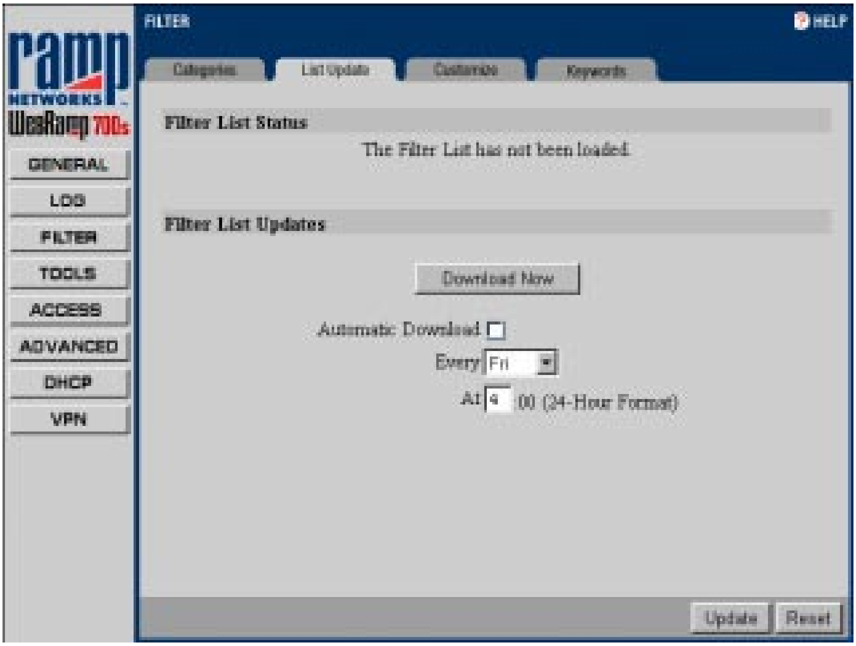
List Update

Since content on the Internet is constantly changing, the Content Filter List used by the WebRamp 700s 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. The **List Update** tab is used to configure the auto-loading of new lists.

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

It is important to note that Host names, and not TCP/IP addresses, are used for all filtering functions for several reasons. One reason is 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. Another reason is the fact that many sites which are included in the Content Filter List regularly change the IP address of the server to try to bypass the Content Filter Lists. This makes maintaining a current list subscription critical for effective content filtering.

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



Filter List Status

The Filter List has not been loaded.

Filter List Updates

Automatic Download □

Every Fri

At 4 :00 (24-Hour Format)

Filter List Status

The **Filter List Status** displays the filters currently loaded.

Filter List Update

- **Download Now**. Click this button to immediately download and install a new Content Filter List. This process may take a couple of minutes, depending on Internet traffic conditions and requires a current subscription to the Content Filter List updates. Since it is necessary to restart the WebRamp 700s once the download is complete, which causes a momentary interruption of Internet access, it is a good idea to download new lists when LAN access to the Internet is at a minimum.
- **Automatic Download.** Check this box to enable automatic, weekly downloads of the Content Filter List. Also select the day of the week and the time of the day when the new list should be retrieved. Since the WebRamp 700s will be automatically restarted when the new list is installed, it is a good

idea to choose a day and time when LAN access to the Internet is at a minimum. A current subscription to the Content Filter List updates is required.

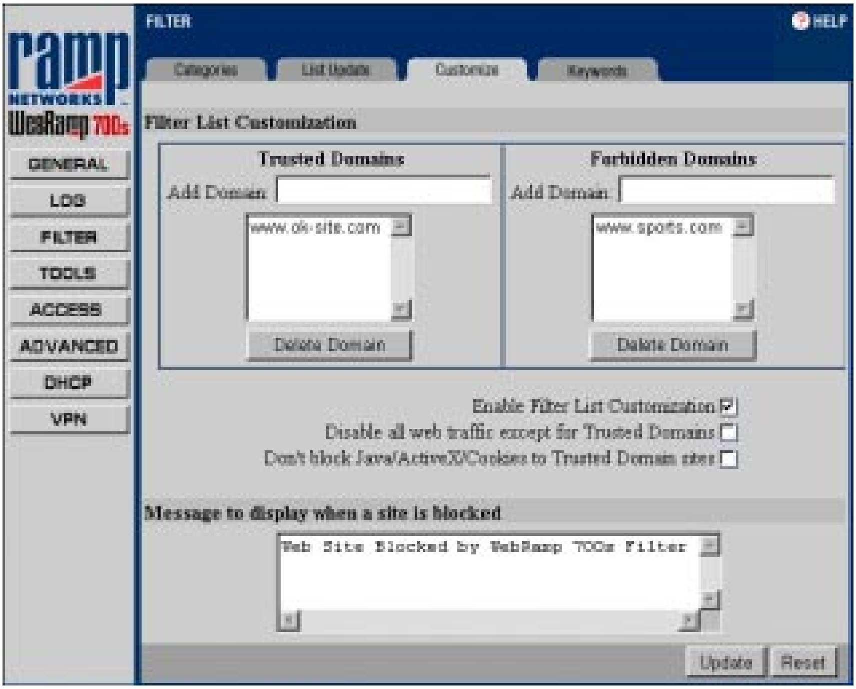
Click the **Update** button on the screen to send the configuration data to the WebRamp 700s. The operation will take a few seconds to complete. Once completed, a message confirming the update will be displayed at the bottom of the window.

Once loaded, the creation date of the current active list will be displayed at the top 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 that may be purchased. Because of the rapid changes on the Internet, Content Filter Lists expire 30 days after they are created. Once expired, a new Content Filter List must be installed to continue content filtering using the Content Filter List. No blocking or logging will occur aside from those sites manually added to the Custom Content Filter List. Once the registration form is completed, an account permitting access to download the Content Filter List will be created, usually within one hour. Follow the “Download Now” instructions to install the initial Content Filter List.

Customize

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



Filter List Customization

Trusted Domains

Add Domain:

www.ok-site.com

Forbidden Domains

Add Domain:

www.sports.com

Enable Filter List Customization ☑

Disable all web traffic except for Trusted Domains ☐

Don't block Java/ActiveX/Cookies to Trusted Domain sites ☐

Message to display when a site is blocked

Web Site Blocked by WebRamp 700s Filter

The WebRamp 700s allows the administrator to customize its Content Filter List features by adding or removing sites from the Content Filter List.

For example, if a local radio station runs a contest on its Web site that is disrupting normal classroom Internet use, a school's Technology Coordinator can easily add that site to the **Forbidden Domains** list**.**

Sites on **Top Web Site Hits** from the **Log Report** which are not objectionable, but are considered inappropriate use of the Internet connection may also be blocked. 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, access to them may be blocked by adding them to the **Forbidden Domains** list. Up to 256 entries are supported in the **Forbidden Domains** list.

To allow access to a Web site which appears in the Content Filter List, enter its host name, such as “www.ok-site.com” into the text field labeled **Trusted Domains** and click **Update**. 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” will also allow “www.yahoo.com”, “my.yahoo.com”, “sports.yahoo.com”, etc. Up to 256 entries are supported in the **Trusted Domains** list.

Click the **Update** button to send the update to the WebRamp 700s. The operation will take a few seconds to complete. Once completed, a message confirming the update will be displayed at the bottom of the window.

To disable access to a site which was previously added to the **Trusted Domains List**, select its name in the list box, and click the **Delete Domain** button to send the update to the WebRamp 700s. The operation will take a few seconds to complete. Once completed, a message confirming the update will be displayed at the bottom of the window. Users will no longer be able to access that site from the LAN.

To block a Web site which does not appear in the Content Filter List, enter its host name, such as “www.bad-site.com” into the text field labeled **Forbidden Domains**. 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” will also block “www.yahoo.com”, “my.yahoo.com”, “sports.yahoo.com”, etc.

Click the **Update** button to send the update to the WebRamp 700s. The operation will take a few seconds to complete. Once completed, a message confirming the update will be displayed at the bottom of the Web browser window.

To remove a site which was previously added in the **Trusted Domains List**, select its name in the list box, and click the **Delete Domain** button to send the update to the WebRamp 700s. The operation will take a few seconds to complete. Once completed, a message confirming the update will be displayed at the bottom of the window. 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, uncheck the box labeled **Enable Content Filter List Customization** and then click the **Update** button. Content Filter List Customization may be enabled and disabled without re-entering all site names, does not have to be re-entered when the Content Filter List is updated each week and does not expire.

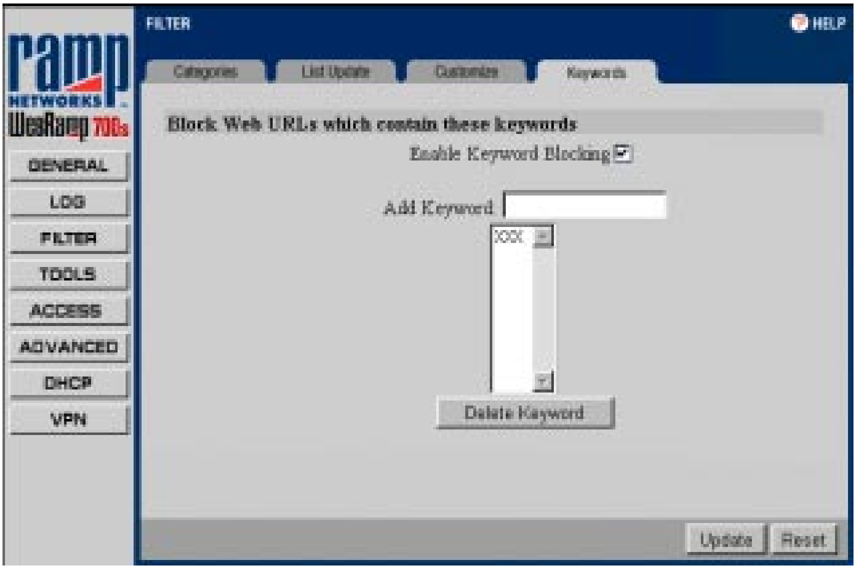
- **Disable all Web traffic except for Trusted Domains**. When the Disable all Web traffic except for Trusted Domains box is checked, the WebRamp 700s will only allow Web access to sites on the Trusted Domains list. With careful screening, this can be close to 100% effective at blocking pornography and other objectionable material.
- **Don’t block Java/ActiveX/Cookies to Trusted Domain Sites**. When this box is checked, the WebRamp 700s will permit Java, ActiveX and Cookies from sites on the **Trusted Domains** list to the LAN. In certain cases, it may be desirable to allow Java, ActiveX or Cookies from sites that are known and trusted. For example, blocking Cookies will require users to reconfigure My Yahoo, or any other site that uses Cookies to customize the content displayed according to the users preferences, each time they visit.
- **Message to display when a site is blocked**. When a user attempts to access a site that is blocked by the WebRamp 700s Content Filter List, a message is displayed on their screen. The default message is “Web Site Blocked by the WebRamp 700s Filter”. Any message, including embedded HTML, up to 255 characters long, may 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

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



Block Web URLs which contain these keywords

Enable Keyword Blocking ☑

Add Keyword

XXX

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

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, as well as those on breast cancer.

To enable this function, check the **Enable Keyword Blocking** checkbox and click the **Update** button. The operation will take a few seconds to complete. Once completed, a message confirming the update will be displayed at the bottom of the window.

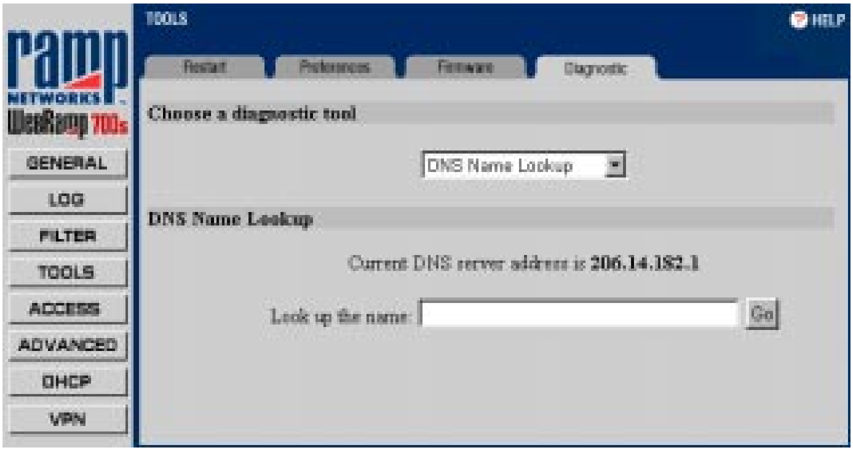
Enter the keyword to block in the **Add Keyword** field and click the **Update** button. The operation will take a few seconds to complete. Once completed, a message confirming the update will be displayed in the status line at the bottom of the window. The keyword will then appear in the keyword list.

To remove a keyword, select the keyword to be removed from the list and click the **Delete Keyword** button. The operation will take a few seconds to complete. Once completed, a message confirming the update will be displayed in the status line at the bottom of the window, and the keyword will no longer be displayed in the list.

DNS Name Lookup Tool

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 will return the numerical TCP/IP address of a host name.

Click the button labeled **Tools** on the left side of the browser window and then click the tab labeled **Diagnostic** at the top of the window. A window similar to the following will be displayed.



Choose a diagnostic tool

DNS Name Lookup

DNS Name Lookup

Current DNS server address is 206.14.182.1

Look up the name:

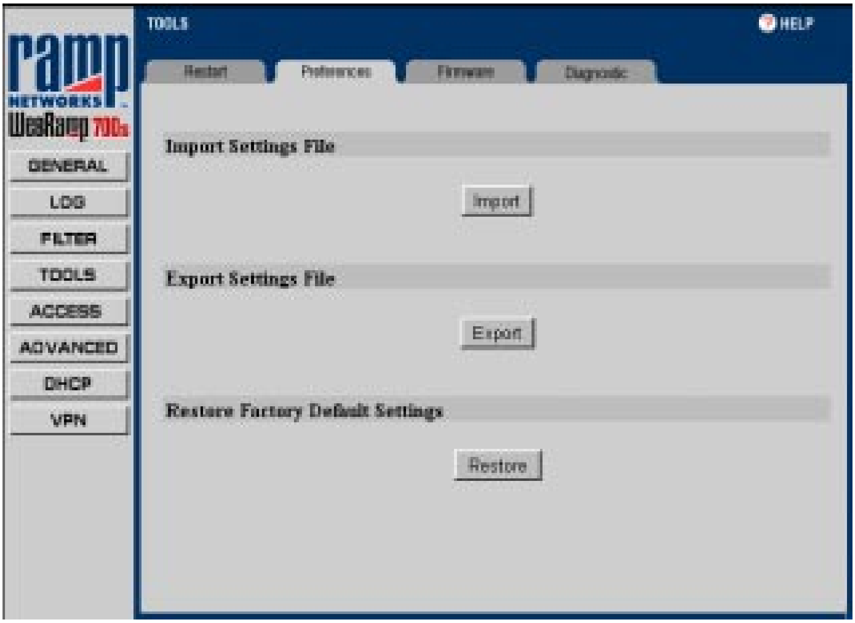
From the **Choose a Diagnostic Tool** popup menu, select **DNS Name Lookup**.

Enter the host name to lookup in the **Look up the Name** field and click **Go**. The WebRamp 700s will then query the DNS server and display the result at the bottom of the window.

NOTE – The IP address of the DNS server must be entered in the Network Settings tab in the General button for the Name Lookup feature to function.

Preferences

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

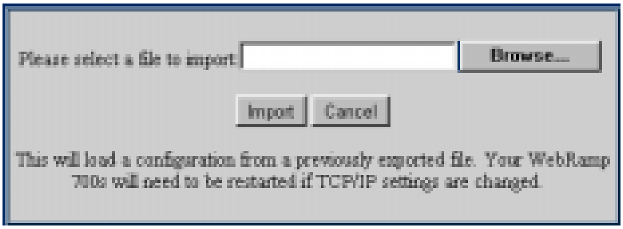


Settings for the WebRamp 700s can be saved and retrieved for backup purposes. This process is recommended when upgrading the WebRamp 700s software as well.

Import Settings File

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

Click the **Import** button. A window similar to the following will be displayed.



This will load a configuration from a previously exported file. Your WebRamp 700s will need to be restarted if TCP/IP settings are changed.

Click the **Browse** button to select a file which was previously saved using the **Export Settings** button.

Once the file is selected, click the **Import** button.

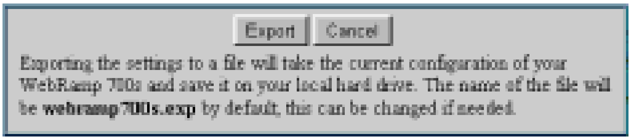
Restart the WebRamp 700s for the settings to take effect.

NOTE – The Web browser software being used for the Import Settings function must support HTTP uploads. As of the writing of this manual, only Netscape Navigator 3.0 and above has this feature. Netscape Communicator is available on the WebRamp 700s CD.

Export Settings File

It is possible to save the WebRamp 700s configuration information to a **preferences file** on a local system, and then to load it back into the WebRamp 700s later.

Click the **Export** button. A window similar to the following will be displayed.

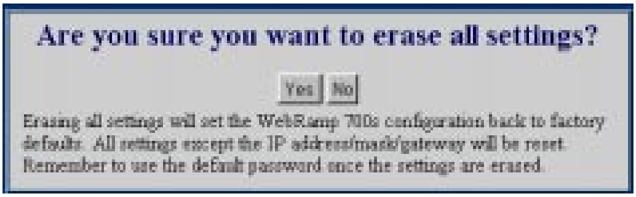


Exporting the settings to a file will take the current configuration of your WebRamp 700s and save it on your local hard drive. The name of the file will be **webramp700s.exp** by default, this can be changed if needed.

Choose the location to save the settings file, which is named **webramp700s.exp** by default, but may be renamed. This process may take up to a minute.

Restore Factory Defaults

The **Restore** button can be used to clear all configuration information and restore the WebRamp 700s to its factory state.



Are you sure you want to erase all settings?

Erasing all settings will set the WebRamp 700s configuration back to factory defaults. All settings except the IP address/mask/gateway will be reset. Remember to use the default password once the settings are erased.

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

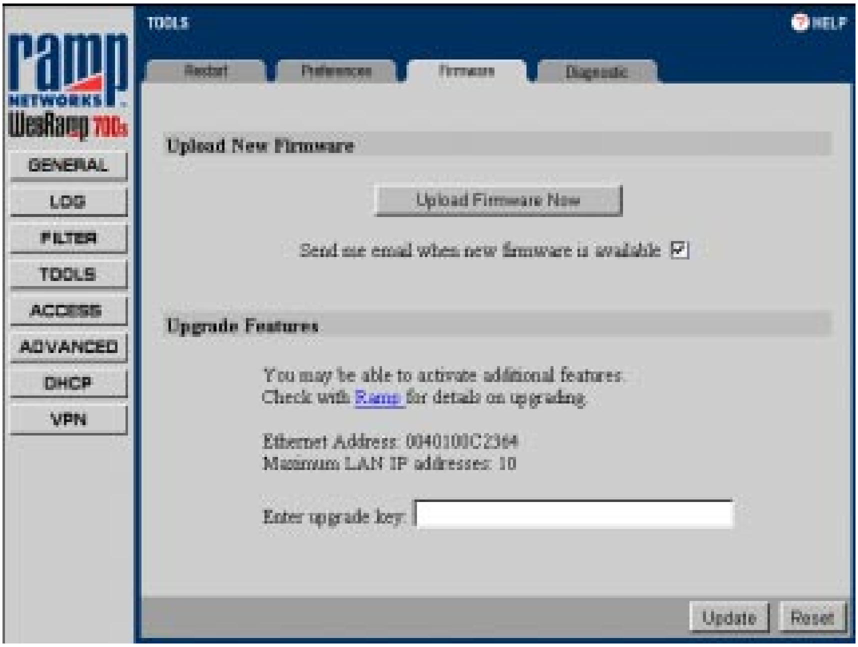
Update Software

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 factory default. It is advisable to export the WebRamp 700s settings before uploading new software and then import them after the upgrade has been completed.

The WebRamp 700s checks to see if new software is available for download from Ramp Networks’ FTP site on a weekly basis. If there is a new software release, an E-mail notification is sent to the address in the **Send log to** field located under the **Log Settings** tab.

Click the button labeled **Tools** on the left side of the browser window and then click the tab labeled **Firmware** at the top of the window. A window similar to the following will be displayed.



Upload New Firmware

Upload Firmware Now

Send me email when new firmware is available ☑

Upgrade Features

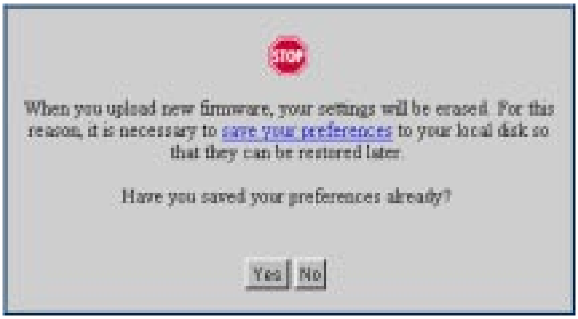
You may be able to activate additional features.
Check with Ramp for details on upgrading.

Ethernet Address: 0040100C2364
Maximum LAN IP addresses: 10

Enter upgrade key:

To be automatically notified when new firmware is available, check the **Send me email when new firmware is available** checkbox and click the **Update** button. When enabled, the WebRamp 700s will check the Ramp Networks FTP site for new firmware once a week. If new firmware is available, an E-mail message containing the new version's release notes will be sent to the administrator.

Click the **Upload Firmware Now** button. A window similar to the following will be displayed.

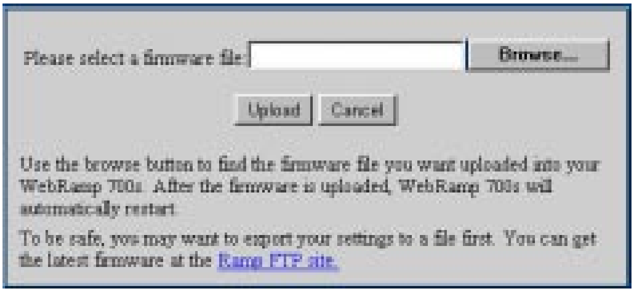


When you upload new firmware, your settings will be erased. For this reason, it is necessary to save your preferences to your local disk so that they can be restored later.

Have you saved your preferences already?

When new firmware is uploaded, all settings will be erased. For this reason, it is necessary to save the WebRamp 700s preferences to a local disk so that they can be restored later. Select **Save your preferences** to export settings to a file.

Once the settings have been saved to a file, click **Yes**. A window similar to the following will be displayed.



Please select a firmware file:

Use the browse button to find the firmware file you want uploaded into your WebRamp 700s. After the firmware is uploaded, WebRamp 700s will automatically restart.

To be safe, you may want to export your settings to a file first. You can get the latest firmware at the Ramp FTP site.

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

The WebRamp 700s must be restarted for the changes to take effect.

NOTE – The Web browser software being used to load new software into the WebRamp 700s must support HTTP uploads. As of the writing of this manual, only Netscape Navigator 3.0 and above has this feature. Netscape Communicator is available 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 **Ramp**.

Network Access Rules

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:

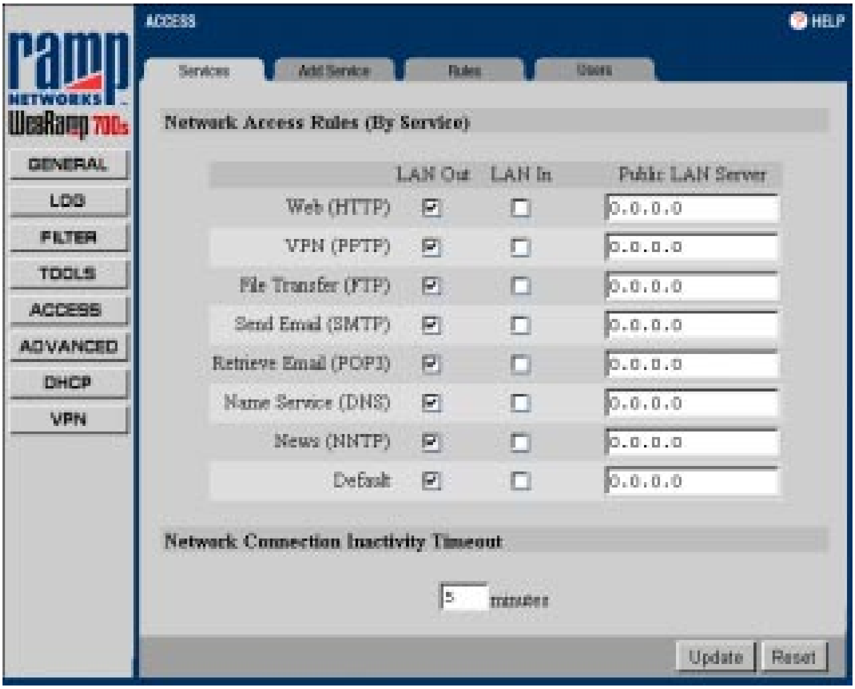
- Block all traffic of a certain type, such as IRC (Internet Chat), from the LAN to the Internet.
- Allow certain types of traffic, such as Lotus Notes database synchronization, from the Internet to a specific host on the LAN.
- Allow access to a Web server to everyone but competitors.
- Restrict use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

Viewing Rules

Click the button labeled **Access** on the left side of the browser window and then click the tab labeled **Services** at the top of the window. A window similar to the following will be displayed.



Network Access Rules (By Service)

	LAN Out	LAN In	Public LAN Server
Web (HTTP)	☑	□	0.0.0.0
VPN (PPTP)	☑	□	0.0.0.0
File Transfer (FTP)	☑	□	0.0.0.0
Send Email (SMTP)	☑	□	0.0.0.0
Retrieve Email (POP3)	☑	□	0.0.0.0
Name Service (DNS)	☑	□	0.0.0.0
News (NNTP)	☑	□	0.0.0.0
Default	☑	□	0.0.0.0

Network Connection Inactivity Timeout

5 minutes

The **Services** window contains a table showing the defined **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. However, LAN access to NNTP may be blocked by nucleating the **LAN Out** box corresponding to the NNTP News service.

- **LAN Out**. When enabled (checked) for a specific protocol, users on the LAN will be able to access servers of that type on the Internet. When the box is disabled (unchecked), users on the LAN will not be able to access servers of that type on the Internet. Default value is enabled. 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 the service is enabled (checked), users on the Internet will be able to access all hosts on the LAN via that protocol. When disabled (unchecked), access to the protocol is not permitted from the Internet to the LAN. Default value is disabled, use caution when enabling. 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.
- **Public LAN Server**. A Public LAN Server is a single host on the LAN that is defined to handle all traffic originating from the Internet to the LAN of a specific protocol, such as HTTP. A Public LAN Server may be defined 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. This is done for security purposes. Without this timeout, it is possible that connections could stay open indefinitely, creating potential security holes. This Inactivity Timeout may be increased if users frequently complain of dropped connections in applications such as Telnet and FTP.

NOTE – If there is an SMTP 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 this is not done, users on the LAN will not be able to receive Internet E-mail.

Click the **Update** button to send the configuration data to the WebRamp 700s. The operation will take a few seconds to complete. Once completed, a message confirming the update will be displayed at the bottom of the window. It is necessary to 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, its IP address would be entered in both the “http” and “ftp” fields.

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

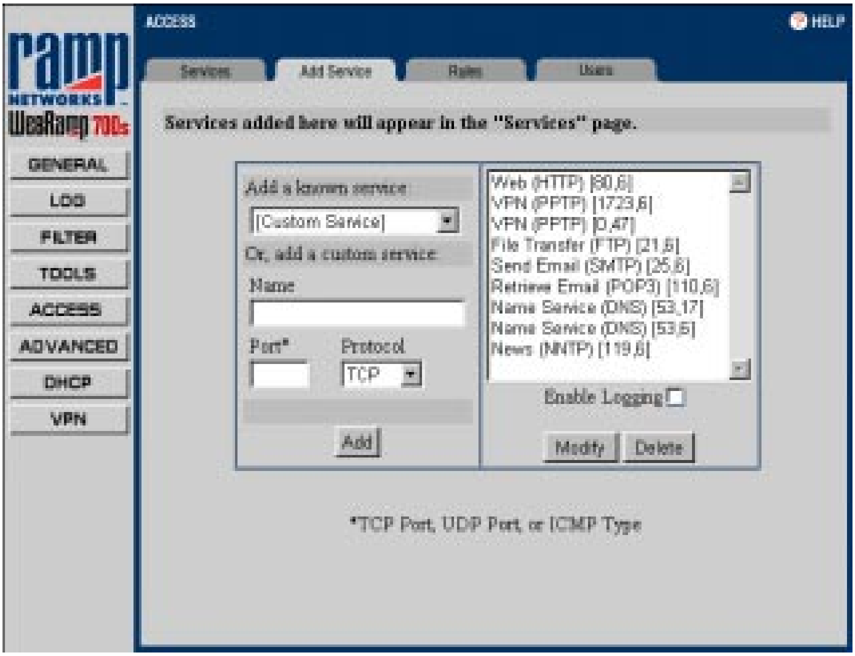
NOTE – PPTP will allow a remote user access to any resource on the LAN. As such, it is critical to maintain the security of the PPTP server, ensure that all security patches are installed, and that users are careful with their account information.

NOTE – If NAT is enabled, then the address of the LAN server will be translated. For example, if the Web server on the LAN with the address 192.168.168.10 is entered in the Public LAN Server's “http” field, and the NAT Public IP Address is 200.200.200.200, then users on the Internet will need to access 200.200.200.200.

Add Service

If a protocol is not listed in the **Services** window, support for it may be added.

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



Services added here will appear in the "Services" page.

Add a known service: [Custom Service]

Or, add a custom service

Name

Port*

Protocol: TCP

Web (HTTP) [80,6]
VPN (PPTP) [1723,6]
VPN (PPTP) [0,47]
File Transfer (FTP) [21,6]
Send Email (SMTP) [25,6]
Retrieve Email (POP3) [110,6]
Name Service (DNS) [53,17]
Name Service (DNS) [53,6]
News (NNTP) [119,6]

Enable Logging □

*TCP Port, UDP Port, or ICMP Type

The scrolling list on the right side of the screen displays all IP protocols which are currently defined and will appear in the **Add 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. Any entries with identical names will be grouped together, and will be treated as a single service. Up to 128 entries are supported.

To add support for a well-known service by name, select the name of the service from the **Add a known service** popup menu and click **Add**. The new service will appear 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.

To add a custom service, 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** popup menu. Click **Add**, and the new service appears in the list box.

NOTE – To add custom services, the **Protocol** popup must be set to “Custom Service”.

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

It is possible to disable logging of 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, all activity for this service may be configured to be ignored by the screen log. To disable screen logs for a specific service, highlight its name in the listbox, uncheck the **Enable Logging** check box, and click **Modify**.

To delete a service, highlight its name in the listbox, and click **Delete**. For services with multiple entries, it is possible to delete only a single Port/Protocol combination from the list. For example, deleting the entry marked “Name Service (DNS) [53,6]” would delete just the TCP portion of the service.

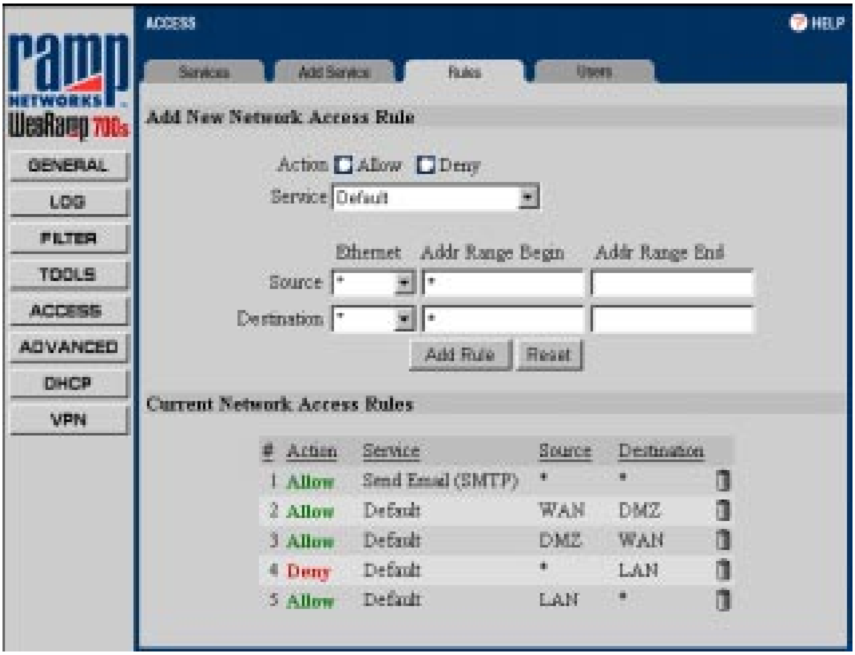
Defining Network Access Rules

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, etc. However, it is possible to create vulnerabilities to attacks that exploit vulnerabilities in applications, such as WinNuke.

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



Add New Network Access Rule

Action □ Allow □ Deny

Service: Default

	Ethernet	Addr Range Begin	Addr Range End
Source	*	*	
Destination	*	*	

Current Network Access Rules

#	Action	Service	Source	Destination
1	Allow	Send Email (SMTP)	*	*
2	Allow	Default	WAN	DMZ
3	Allow	Default	DMZ	WAN
4	Deny	Default	*	LAN
5	Allow	Default	LAN	*

It is important to fully consider logic behind the new rule before it is added. The following list will help.

Network Access Rule Logic List

1. 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.”
2. Is the intent of the rule to allow or deny traffic?
3. What is the flow of the traffic: from the LAN to the Internet, or from the Internet to the LAN?
4. List which IP services will be affected.
5. List which computers on the LAN are to be affected.
6. 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 created by 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?

Once these questions have been answered, adding rules is simply a matter of plugging the information into the correct fields in the **Rules** window.

- **Action**. Select the **Allow** or **Deny** radio button depending on the intent of the rule, as defined by item 2 in the “Network Access Rule Logic List”.
- **Service**. Select the IP protocol as defined by item 4 in the “Network Access Rule Logic List” from the **Service** menu. If the protocol is not listed, it will be necessary to first define it in the **Add Service** window.

- **Source**. There are two parameters that are configured for the **Source** item. Select the Network Access Rule's source port, **LAN** or **WAN** from the **Ethernet** pull-down menu.

NOTE – The DMZ option is currently unavailable.

- 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**, respectively. If all IP addresses are to be affected, enter * in the **Addr Range Begin** field.
- **Destination**. There are two parameters that are configured for the Destination item. Select the Network Access Rule's destination port, **LAN** or **WAN** from the **Ethernet** menu.
- 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** icon in the far right row of the table rule.

Understanding the Network Access Rule Hierarchy

The rule hierarchy has two basic concepts:

1. Specific rules override general rules.
2. 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 the least specific, and rules at the top of the window override the rules listed at the bottom of the window.

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 button labeled **Access** on the left side of the browser window, then click the **Rules** tab.
2. Click the **Deny** radio button in the **Action** field.
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 button labeled **Access** on the left side of the browser window, then click the **Rules** tab.
2. Click the **Deny** radio button in the **Action** field.
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 button labeled **Access** on the left side of the browser window, then click the **Rules** tab.
2. Click the **Allow** radio button in the **Action** field.
3. From the **Service** menu, choose **Ping**. Select **WAN** from the **Source Ethernet** menu. If the service is not listed in the menu, add it in the **Add Service** window.
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.

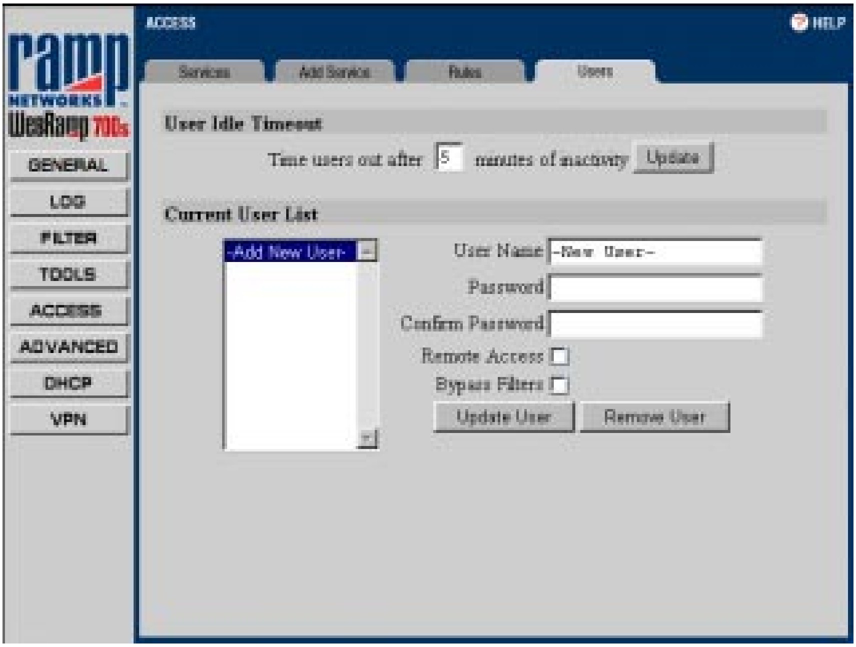
7. Click the **Add Rule** button.

User Authentication

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.

User Settings

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



User Idle Timeout

Time users out after 5 minutes of inactivity

Current User List

-Add New User-

User Name -New User-

Password

Confirm Password

Remote Access □

Bypass Filters □

- **Idle Timeout**. This sets the maximum period of inactivity, in minutes, before a user will be required to re-establish an Authenticated Session. Enter the desired number of idle time minutes and click **Update**. **Idle Timeout** applies to **Remote Access** and **Bypass Filters**.
- **Current User List**. The user list is a scrollable box which contains a list of all currently defined users. In addition, there is an entry at the top of the list labeled -**Add New User-**.

To add a new user:

1. Highlight the **-Add New User-** entry.
2. Enter the user’s login name in the **User Name** field.
3. Enter the user’s password in the **Password** and **Confirm Password** fields. It is important to use a password that could not be guessed by someone else. Avoid using names of friends, family, pets, places, etc. 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 “so#n&c”. Passwords are case sensitive.
4. Choose the privileges to be enabled for the user by selecting one or both checkboxes. Two options are available:
   - **Remote Access**. Unrestricted access to the LAN from a remote location on the Internet.
   - **Bypass Filters**. Unrestricted access to the Internet from the LAN, bypassing Web, News, Java, and ActiveX blocking.
5. Click the button marked **Update User.**

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”).

The WebRamp 700s supports a list of up to 100 users.

To change a user’s password or privileges, highlight the name in the scrollable box, make the changes and click the **Update User** button. To delete a user, highlight the name and click the **Remove User** button.

Establishing an Authenticated session

Authenticated sessions are used to allow a user on the Internet to access the LAN without restrictions, or to allow a user on the LAN to access the Internet without restrictions, bypassing the Content Filter Lists.

NOTE – The Web Browser software being used to establish an authenticated session must support Java, JavaScript or ActiveX scripting. As of the writing of this manual, only Netscape Navigator 3.0 and above has the necessary features. Netscape Communicator is available on the WebRamp 700s CD.

In order to establish an Authenticated Session, a user points their Web browser at the Web Address of the WebRamp 700s. This process is identical to the administrator login.

The user will see a dialog asking them for their user name and password. After filling in these fields and clicking the **Login** button, their password will be verified using MD5 authentication. The password is never sent “in the clear” over the Internet, preventing password theft and replay attacks.

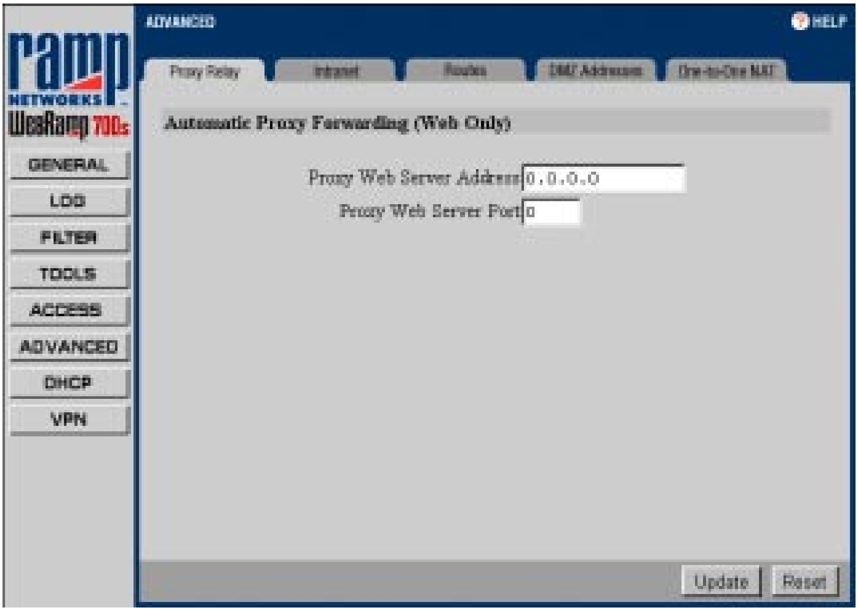
Once authenticated, remote users will be able to access all IP resources on the LAN, and users on the LAN will be able to bypass the Content Filter Lists. The connection will close if user inactivity on the connection exceeds the configured time-out period. In that case, the remote user will need to reauthenticate.

NOTE – All user names are case insensitive (“john” is equivalent to “JOHN” or “John”), but all passwords are case sensitive (“password” is not the same as “Password”). If it seems like authentication is failing for no reason, check the “caps lock” key on your keyboard to make sure that it is not on.

NOTE – Authenticated Sessions create a log entry when established. However, no user activity is logged.

Advanced Window

Click the button labeled **Advanced** at the left side of the browser window. A window similar to the following will be displayed.



Automatic Proxy Forwarding (Web Only)

Proxy Web Server Address 0.0.0.0

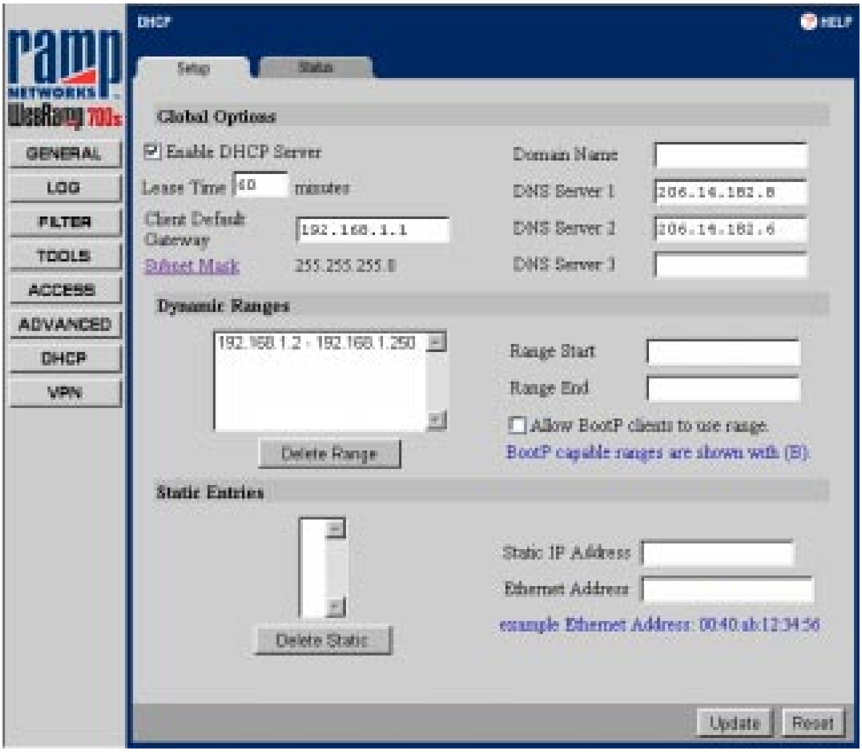
Proxy Web Server Port 0

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

Additional features may be available. See the Ramp Networks Web site located at www.rampnet.com for upgrade pricing and availability.

DHCP Server

Click the button labeled **DHCP** at the left side of the browser window. A window similar to the following will be displayed.



Global Options

☑ Enable DHCP Server

Lease Time 60 minutes

Client Default Gateway 192.168.1.1

Subnet Mask 255.255.255.0

Domain Name

DNS Server 1 206.14.182.8

DNS Server 2 206.14.182.6

DNS Server 3

Dynamic Ranges

192.168.1.2 - 192.168.1.250

Range Start

Range End

☐ Allow BootP clients to use range.

BootP capable ranges are shown with (B).

Static Entries

Static IP Address

Ethernet Address

example Ethernet Address: 00:40:ab:12:34:56

DHCP, which stands for “Dynamic Host Configuration Protocol”, is a means for computers on a network to get their TCP/IP settings from a centralized server.

DHCP Setup

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

Global Options

- **Enable DHCP Server**. This option allows you to enable or disable the DHCP server. Enabled by default. The DHCP server should remain disabled if there is already a DHCP server on the LAN or if manual addressing is used on the LAN computers.
- **Lease Time.** The Lease Time is the amount of time that the TCP/IP address is leased, or given to the client machine before the DHCP server will attempt to renew that address. If the client still requires the use of the TCP/IP address, the DHCP Server grants 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 returned to the pool of available addresses to be used again. Default value is 60 minutes.
- **Client Default Gateway**. Enter the IP address of the WAN router used by LAN clients to access the Internet.
- **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, consider the IP address 192.168.228.17. Assuming a Class C subnet mask of 255.255.255.0 is used, the first three numbers (192.168.228.) represent the Class C network address, and the last number (17) identifies a particular host on this network. This value is set in the **General** section's **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 human readable host names into the numeric IP addresses used by computers to route information to the correct machine. Multiple DNS servers may be used to improve performance and reliability. Enter the TCP/IP address of the DNS Server(s) in these fields.

Dynamic Ranges

When a client makes a request for a TCP/IP address, and the requester is a DHCP client, the WebRamp 700s DHCP server leases an address from the Dynamic Ranges.

NOTE – Prior to offering an address from the Dynamic Range to a requesting client, the WebRamp 700s first verifies that the address is not already in use by another machine on the LAN.

- **Range**. To create a range of dynamic IP addresses to be assigned to requesting clients, enter the starting number in the **Range Start** field, and the ending address in the **Range End** field and then click the **Update** button. Theoperation will take a few seconds to complete. Once completed, a message confirming the update will be displayed at the bottom of the window.
- **Allow BootP clients to use range**. If the Allow BootP clients to use range check box is selected, Dynamic BootP clients will be configured when they boot. Dynamic BootP clients are BootP clients that do not have an IP address assigned to their MAC address. They are similar to DHCP clients with the exception that leases are not supported.
- **Delete Range**. To remove a range of addresses from the dynamic pool, select it from the scrolling list of Dynamic Ranges, and click the **Delete Range** button. The operation will take a few seconds to complete. Once completed, a message confirming the update will be displayed at the bottom of the window.

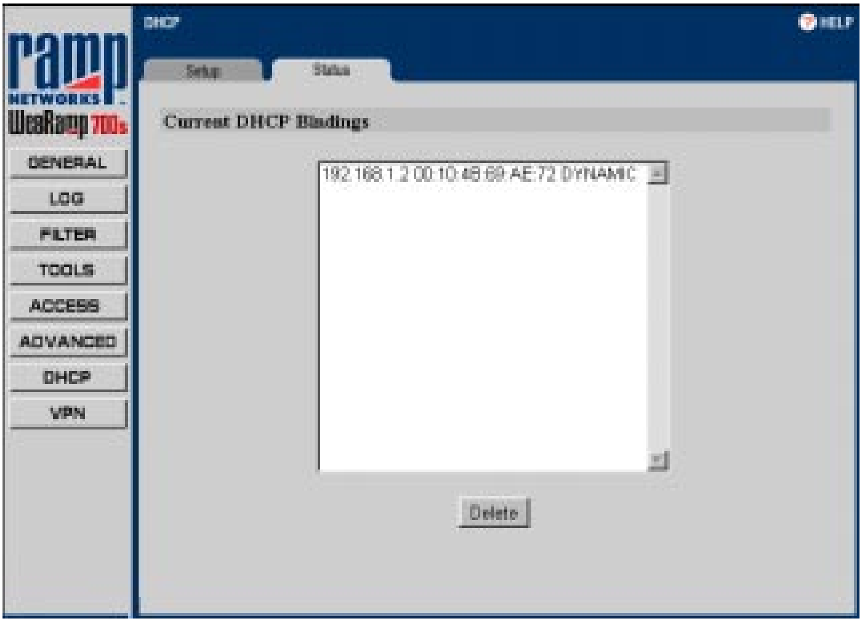
Static Entries

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 would require static addresses. If a static address is assigned, then that machine will always get 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 to be assigned to a requesting client, enter an IP address and the Ethernet (MAC) address of the client machine in the appropriate fields and then click the **Update** button. The operation will take a few seconds to complete. Once completed, a message confirming the update will be displayed at the bottom of the window.
- **Delete Static**. To remove a static address, select it from the scrolling list of Static Addresses and click the **Delete Static** button. The operation will take a few seconds to complete. Once completed, a message confirming the update will be displayed at the bottom of the window.

DHCP Status

Click the tab labeled **Status** at the top of the browser window. A window similar to the following will be displayed.



```
192.168.1.2 00:10:4B:69:AE:72 DYNAMIC
```

The scrolling window shows the details on the current bindings: IP and MAC address of the bindings, along with the type of binding (Dynamic, Dynamic BootP, or Static BootP).

To delete a binding, which frees the IP address in the DHCP server, select the binding from the list and then click **Delete**. The operation will take a few seconds to complete. Once completed, a message confirming the update will be displayed at the bottom of the Web browser window.

Click the **Refresh** or **Reload** button on your browser 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 first loaded.

Chapter

2

Configuration and Function of the Advanced Features

This chapter describes the configuration and function of the advanced features of the WebRamp 700s.

If the WebRamp 700s doesn't have the plus features loaded, contact Ramp Networks' sales for upgrade pricing and availability.

Automatic Proxy Forwarding

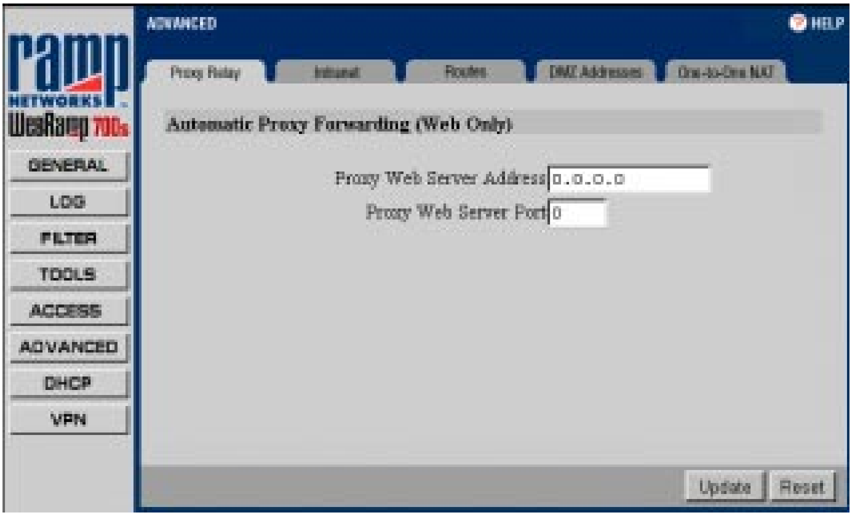
A proxy server intercepts all requests to the Web server to see if it can fulfill the requests by returning a locally stored copy of the requested information. If not, the proxy completes the request to the server and returns the requested information to the user and also saves it locally to fulfill future requests. Because of this, a proxy can improve Internet response and lessen the load on the Internet link. For example, suppose a school is using the Internet for a research project. A student requests a certain Web page, and then sometime later, a second student requests the same page. Instead of forwarding the request to the Web server where the page resides, the proxy server returns the local copy of the page that it already fetched for the first student.

The problem with a proxy server is that each client must be configured to support the proxy, making them an administrative problem.

If a proxy server is already installed on the LAN, instead of configuring each client to point to the proxy server, move it to the WAN and enable Automatic Proxy Forwarding. The WebRamp 700s is able to automatically forward all Web proxy requests to the proxy server without client configuration. As a result, no client configuration is required when a Web Proxy is used.

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

Click the button labeled **Advanced** at the left side of the browser window. Then, click the tab labeled **Proxy Relay**. A window similar to the following will be displayed.



Automatic Proxy Forwarding (Web Only)

Proxy Web Server Address 0.0.0.0

Proxy Web Server Port 0

Enter the IP address of the proxy in the **Proxy Web Server Address** field, and the proxy’s IP port in the **Proxy Web Server Port** field.

Click the **Update** button to send the configuration data to the WebRamp 700s. The operation will take a few seconds to complete. Once completed, a message confirming the update will be displayed at the bottom of the Web browser window.

Installing a Proxy to Improve Web Access

Consider installing a proxy server to improve the speed of Web access on the LAN, as well as lessen the load on the Internet connection.

Much of the difficulties involved with installing a proxy server revolve around the need to configure all clients on the LAN to point to the proxy. The WebRamp 700s Automatic Proxy Relay eliminates that problem, greatly easing the installation, configuration, and ongoing maintenance associated with a proxy server.

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. Links to download commercial demos of proxy servers, as well as shareware and freeware proxy servers are at www.rampnet.com/support/700s/faq.html.

Example

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

Installing a proxy on the WAN

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

2. **Configure Intranet settings**
   Click the button labeled **Advanced** on the left side of the browser window and then click the tab labeled **Intranet** at the top of the window. Enter the proxy server's IP address in the **Add Range** field, select the **Specified address ranges are attached to the WAN link** radio button, and click the **Update** button.

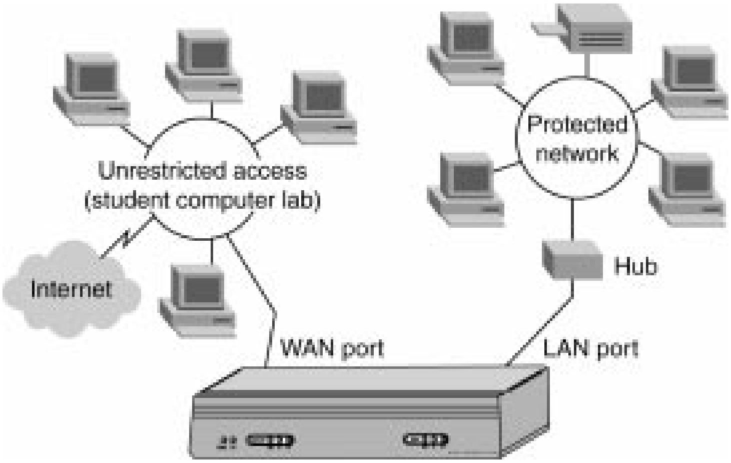
3. **Configure Web Proxy Relay**
   Click the button labeled **Advanced** at the left side of the browser window. Then, click the tab labeled **Proxy Relay**. Configure the Web proxy relay as described in this Reference. Web traffic will be directed to the proxy, which will fulfill all requests, without reconfiguring all Web browsers on the LAN.

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 no other devices between the WAN port of the WebRamp 700s and the Internet. To enable access to the area between the WAN port and the Internet (a.k.a. Intranet), additional configuration must be done.

The following describes how to install and configure the WebRamp 700s to provide Intranet firewalling.

Intranet firewalling is achieved by connecting the WebRamp 700s between the free and the restricted segments on the LAN, as shown below.



Installation

1. Connect the Ethernet port labeled LAN on the back of the WebRamp 700s to the network segment that will be protected against unauthorized access.

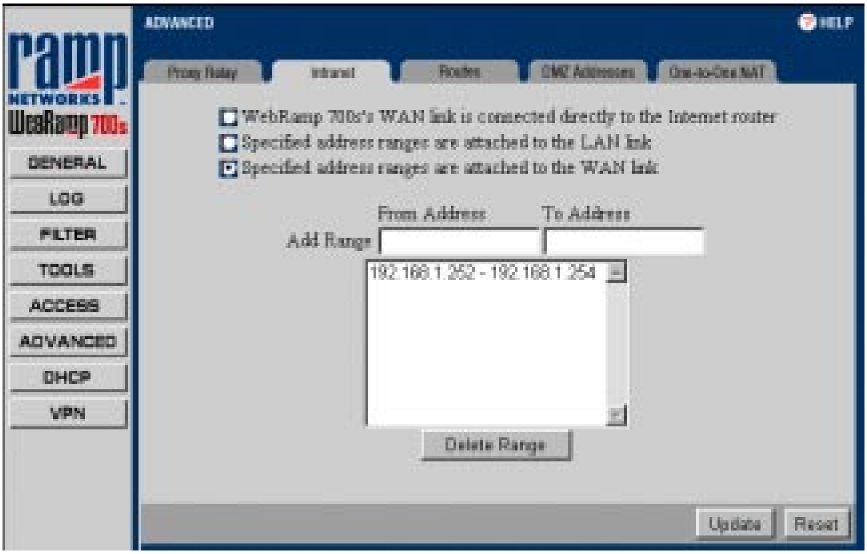
2. Connect the Ethernet port labeled WAN on the back of the WebRamp 700s to the rest of the network.

NOTE – Devices connected to the WAN port do not have firewall or content filter protection. It is advised that another webRamp 700s 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 port on the back of the WebRamp 700s labeled “5VDC/1.5A”.

Configuration

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



□ WebRamp 700s's WAN link is connected directly to the Internet router
□ Specified address ranges are attached to the LAN link
☑ Specified address ranges are attached to the WAN link

	From Address	To Address
Add Range		

192.168.1.252 - 192.168.1.254

To enable Intranet firewalling, it is necessary to identify which machines are protected against unauthorized access by specifying the IP addresses of these machines. This can be done in one of two ways: inclusively by specifying which machines are members of the segment with restricted access, or exclusively by specifying which machines are not.

When done inclusively, the IP addresses of the machines which are connected to the LAN port of the WebRamp 700s 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 done exclusively, the IP addresses of the machines connected to the WAN port of the WebRamp 700s 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.

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.

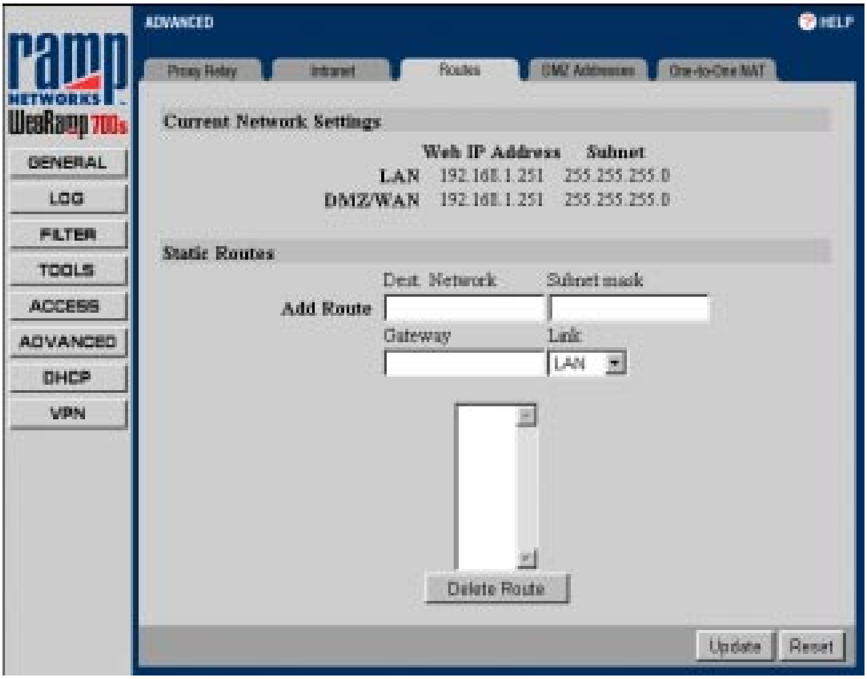
- **WebRamp 700s WAN link is connected directly to the Internet router**. Use this setting if the WebRamp 700s is protecting the entire network. This is the default setting.
- **Specified address ranges are attached to the LAN link**. Select this button when it is easier to specify which devices are on the LAN. If a machine's IP address is not specified, all communications through the WebRamp 700s for that machine will be blocked.
- **Specified address ranges are attached to the WAN link**. Select this button 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. Up to 64 address ranges may be entered.

Click the **Update** button to send the configuration data to the WebRamp 700s. The operation will take a few seconds to complete. Once completed, a message confirming the update will be displayed at the bottom of the window.

Routes

If the LAN has internal routers, their addresses and network information will need to be entered into the WebRamp 700s.

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



Current Network Settings

	Web IP Address	Subnet
LAN	192.168.1.251	255.255.255.0
DMZ/WAN	192.168.1.251	255.255.255.0

Static Routes

Add Route: Dest. Network, Subnet mask, Gateway, Link: LAN

Static routes are used if the LAN or WAN are segmented into subnets, either for size or practical considerations. For example, a subnet can be created which only 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 LAN port of the WebRamp 700s are shown at the top of the window. These are configured in the General section's Network tab.
- **WAN**. The IP address of the WAN port is shown. This will differ from that of the LAN port if NAT is enabled. This address is in the General section's Network tab. The Subnet Mask, if different from the default, may be entered.
- **Add Route**. Enter the destination network of the router in the **Dest. Network** field, the IP address of the router as it appears on the subnet of the WebRamp 700s in the **Gateway** field, and select which port on the WebRamp 700s, LAN or WAN, that the router is connected to from the **Link** popup menu. It may be necessary to check the configuration of the LAN routers in order to find this information.

Click the **Update** button to send the configuration data to the WebRamp 700s. The operation will take a few seconds to complete. Once completed, a message confirming the update will be displayed at the bottom of the window.

Chapter

3

Introduction to Networking

Overview

This chapter provides a non-technical overview of LANs and the network protocols supported by the WebRamp 700s. This chapter also includes a discussion of Internet Protocol (IP) addressing.

It may be helpful to review a book on TCP/IP for an overview of protocols such as TCP (Transmission Control Protocol), UDP (User Datagram Protocol), and ICMP (Internet Control Message Protocol). The following book is recommended for beginner and intermediate network administrators:

Teach Yourself TCP/IP in 14 Days Second Edition
Timothy Parker, Ph.D
SAMS Publishing
ISBN # 0-672-30885-1

What is a LAN?

LAN stands for Local Area Network. Local area refers to a network in one location, such as one floor, one building, or a campus.

What is a Firewall?

A firewall is a software or hardware system that prevents unauthorized outside access, theft, deletion, or modification of information stored on a local network. Typically, this unauthorized access would be via an organization’s Internet connection.

Network Protocols

Protocols are rules that networking hardware and software follow to communicate with one another. The WebRamp 700s uses the TCP/IP protocol.

IP, TCP

IP stands for Internet Protocol. This protocol provides connectionless data transfer over a TCP/IP network. Since IP alone does not provide end-to-end data reliability as well as some other services, other protocols such as TCP can be added to provide these services. TCP stands for Transmission Control Protocol. In TCP/IP, TCP works with IP to ensure the integrity of the data traveling over the network. TCP/IP is the protocol of the Internet.

IP Addressing

To become part of an IP network, a network device must have an IP address. An IP address is a unique number that differentiates one device from another on the network to avoid confusion during communication. To help illustrate IP addresses, the following sections compare an IP address to the telephone numbering system, a system that is used every day.

Like a phone number with its long distance “1” and area code, an IP address contains a set of four numbers. While we separate phone number components with dashes, for example 1-408-555-1212, IP address number components are separated by decimal points or dots (called dotted decimal notation), for example 123.45.67.89. Because computers use a binary number system, each number in the set must be less than 255.

There are three components that contribute to an IP address:

- IP address itself
- Subnet mask
- Default gateway

The following sections discuss each of these components in detail.

IP Address

Just as each household or business requires a unique phone number, a networked device (such as a computer, printer, file server, or router) must have a unique IP address. Unlike phone numbers, in IP addressing it is necessary to always use the entire number when communicating with other devices.

There are three classes of IP addresses: A, B, and C. Like a main business phone number that one can call and then be transferred through interchange numbers to an individual's extension number, the different classes of IP addresses provide for varying levels of "interchanges" or subnetworks and "extensions" or device numbers. The classes are based on estimated network size:

- Class A — used for very large networks with hundreds of subnetworks and thousands of devices. Class A networks use IP addresses between 0.0.0.0 and 127.0.0.0.
- Class B — used for medium to large networks with 10–100 subnetworks and hundreds of devices. Class B networks use IP addresses between 128.0.0.0 and 191.0.0.0.
- Class C — used for small to medium networks, usually with only a few subnetworks and less than 200 devices. Class C networks use IP addresses between 192.0.0.0 and 223.0.0.0.

Just as one would go to the phone company for their phone number, there are controlling bodies for IP addresses. The overall controlling body for IP addresses worldwide is InterNIC. Businesses or individuals can request one or many IP addresses from InterNIC; it's a good idea to estimate the network's future growth in the class and number of IP addresses requested.

Most large centralized companies have a network manager in charge of all IP address numbers. Other companies have a distributed administration scheme that allows the local network manager to set local IP addresses. In this case, the local manager gets a sub network or "interchange" number from the company's central network manager and then assigns local IP address numbers.

Subnet Mask

As mentioned previously, the IP addressing system allows creation of subnetworks or “interchanges” and device numbers or “extensions” within those subnetworks. These numbers are created using a mathematical device called a subnet mask. A subnet mask, like the IP address, is a set of four numbers in dotted decimal notation. Subnet masks typically take three forms:

- 255.0.0.0
- 255.255.0.0
- 255.255.255.0

The number 255 “masks” out the corresponding number of the IP address, resulting in IP address numbers that are valid for the network. For example, an IP address of 123.45.67.89 and a subnet mask of 255.255.255.0 results in a sub network number of 123.45.67.0 and a device number of 89. The IP address numbers that are actually valid to use are those assigned by InterNIC; otherwise, anyone could set up IP addresses that are duplicates of those at another company.

The subnet mask used for the network typically corresponds to the class of IP address assigned. If the IP address is Class A, use a subnet mask of 255.0.0.0. Class B addresses use a subnet mask of 255.255.0.0, and Class C IP addresses use a subnet mask of 255.255.255.0.

Default Gateway

A default gateway is like a long distance operator - users can dial the operator to get assistance connecting to the end party. In complex networks with many subnetworks, gateways keep traffic from traveling between different subnetworks unless addressed to travel there. While this helps to keep overall network traffic more manageable, it also introduces another level of complexity.

To communicate with a device on another network, one must go through a gateway that connects the two networks. Therefore, users need to know the default gateway’s IP address. If there is no gateway in the network, use an IP address of 0.0.0.0 in fields that apply to a default gateway.

Appendix A

Cable Specifications and Pinout Diagram

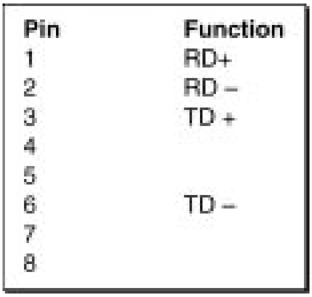
This appendix lists cable requirements and provides pinout diagrams for the WebRamp 700s.

Cable Specifications

The WebRamp 700s supports the following cable types and maximum lengths.

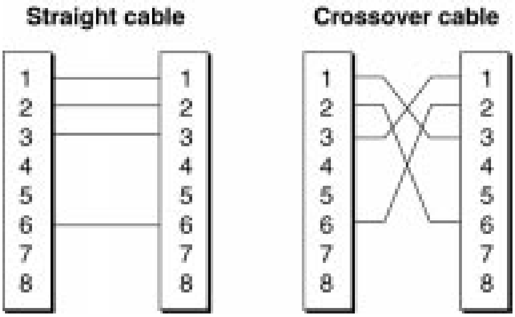
- Maximum 10Base-T Twisted Pair cable length of 100 meters.

Figure A-1 Pinout diagram



Pin	Function
1	RD+
2	RD –
3	TD +
4	
5	
6	TD –
7	
8	

Figure A-2 Twisted pair cable pinout diagram



Appendix B

Technical Specifications

The WebRamp 700s Firewall has the following specifications:

Hardware Specifications

- CPU: MC 68360 @ 25mHz
- RAM: 4MB
- ROM: 128KB
- Flash: 2MB
- Real time clock (Year 2000 compliant)
- Convection cooled: no internal fan needed

Interfaces

- (2) 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

C

Optional Direct Connection

The security of the WebRamp 700s is ensured by the use of a secret Administrator Password. Once the password is set, it is used to authenticate the administrator's identity as well as to conceal any important information exchanged with the Web Management Interface. For example, when the administrator's password is changed, the old password is used to conceal the new one.

The WebRamp 700s comes pre-configured from the factory with a default password. It is critical to change this password during the initial configuration of the firewall. Unfortunately, the default password can only provide limited protection the first time the administrator's password is set. In principle, an individual inside the network could capture all network transmissions and then perform mathematical analyses to discover the new Administrator Password. Though this is more academic than a practical issue, using the **Direct Connection** option to set the password for the first time may be advisable if this is a concern.

Direct Connection Instructions:

1. Disconnect the Management Station from the local Ethernet network.

2. Attach the WebRamp 700s directly to your Management Station. This is done by connecting a Twisted Pair “reverse” cable from the Management Station's Ethernet port to the LAN Port of the WebRamp 700s.

3. Turn on the WebRamp 700s by connecting the supplied power cable to the port on the back labeled **5VDC/1.5A**. Do not use a power supply other than the one supplied with the WebRamp 700s.

4. Wait for the **Test** LED to turn off, which is lit while the WebRamp 700s initializes itself. This should take about 90 seconds.

5. Perform the Initial Configuration steps as described in the *WebRamp 700s Installation Guide*.

6. Disconnect the Management Station from the WebRamp 700s and reconnect it to the main Ethernet network. Note that in some cases it may be necessary to restart the Management Station after reconnecting it.

7. Attach the WebRamp 700s to the LAN as described in the *WebRamp 700s Installation Guide* and continue with configuration.

Appendix

D

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, etc. 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 can not 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.