

# WARP 3.0 Table of Contents

<b>Overview</b> .....	1
<b>Chapter 1: Initial Setup</b>	
Quick Install Instructions .....	4
<b>Chapter 2: Interfaces</b>	
LAN .....	6
WAN .....	8
<b>Chapter 3: Configuration</b>	
System Info .....	9
Load Balancing .....	10
Route Test .....	11
Unit Failover .....	11
Administration .....	19
<b>Chapter 4: Advanced Configuration</b>	
Pass-Through .....	20
Reverse Mapping .....	21
Static Routes .....	22
Policy Routing .....	23
SmartDNS .....	25
Session Timeouts .....	30
<b>Chapter 5: Tools</b>	
Speed Chart .....	31
Speed Meter .....	32
Diagnostics .....	33
SNMP .....	34
Reboot/Shutdown .....	43
<b>Chapter 6: Paging Software</b>	
Add New Pager Information .....	44
Change Existing Pager Information .....	46
Remove Pager Entry .....	47
<b>Chapter 7: Site Failover</b>	
Site Failover Configuration .....	48
<b>Technical Support</b> .....	54

# Overview

FatPipe® WARP is the next generation of high-speed router clustering devices from FatPipe Networks. It is the ultimate solution for companies that want the highest levels of WAN redundancy, reliability, and speed for Internet connections for data traffic directed from the network to the Internet as well as data traffic directed to servers hosted internally.

FatPipe WARP supports the hosting of large sets of internal servers including load balancing, firewall, e-mail, Citrix® and web servers. FatPipe WARP works with all existing hardware and applications. No BGP programming is required. FatPipe WARP is available in two versions: 50 Mbps and 155 Mbps, supporting more than three DS3 connections.

You can access the manual, FatPipe WARP configuration, and the FatPipe website from the configuration interface of WARP. The interface also has links to the feature set, sales and support contact information, and frequently asked questions.

## Chapter 1: Initial Setup

This chapter provides you with the information required to setup the cable connections and the initial configuration for FatPipe WARP. In this chapter you will learn how to:

- Install the WARP unit
- Connect WARP to your network

## Chapter 2: Interfaces

This chapter explains how to setup necessary networking parameters for FatPipe WARP to work with your existing networking environment. In this chapter you will learn how to:

- Setup the IP Address, Subnet Mask, and Default Gateway of each networking interface
- Use or disable access to functions and features of the WARP unit
- Check the status of each WAN connection

## Chapter 3: Configuration

WARP dynamically load balances inbound and outbound IP traffic for the highest levels of reliability and redundancy of WAN/Internet connections. Along with comprehensive load balancing algorithms, you can also choose failover recovery options using one or more standby WARP units either at your site, called Unit Failover, or at separate locations, called Site Failover. You can access and configure these options under the Configuration section of the menu. Information about Site Failover is described in detail in Chapter 7. In this chapter you will learn how to:

- Choose the most appropriate load balancing option for your IP traffic
- Specify external DNS servers the WARP box will use for name resolution
- Set Route Test configuration
- Setup Failover between two or more WARP units at the CPE
- Set Administrator and user privileges and passwords
- Reset default system settings
- Set system time

## **Chapter 4: Advanced Configuration**

Use the management interface to setup SmartDNS, Pass-Through, and Reverse Mapping for inbound data traffic. In this chapter you will learn how to:

- Configure Pass-Through for inbound traffic to servers in your network
- Configure Reverse Mapping for inbound data traffic to servers in your network
- Configure Static Routes for inbound traffic
- Utilize the Policy Routing feature to specify rules for outbound connections
- Configure SmartDNS for inbound load balancing and redundancy

## **Chapter 5: Tools**

Use FatPipe WARP's management interface to monitor the performance of your current network. You can check the status of routers and Internet connections using FatPipe WARP's Diagnostic Tools or check the speed of connections using the Speed Meter and Speed Chart views. In this chapter you will learn how to:

- View the WAN's performance by using the Speed Chart and Speed Meter
- Check status of routers and connections using WARP's Diagnostic Tools
- Analyze performance with System Statistics

## **Chapter 6: WARP Paging Configuration**

FatPipe WARP comes with monitoring tools that will continuously test the status of services going through the WARP unit as well as the unit itself. The Paging Software will send you an alert if a failure occurs on the WAN. In this chapter you will learn how to:

- Install the Paging Software
- Change settings, add and remove pager numbers and e-mail addresses

## **Chapter 7: Site Failover**

WARP units can be configured to automatically failover to one or more remote site units where inbound connectivity to Internet accessible servers is critical. This technology utilizes Site Failover, and is an optional feature available upon request. Please refer to the back of the manual for general contact information or contact your local FatPipe representative for purchasing information. In this chapter you will learn how to:

- Configure site failover between two or more units located at different sites

## Chapter 1: Initial Setup

FatPipe WARP is a 19" standard rack mountable 4U device. It has four Ethernet ports located at the back of the chassis (See Fig. 2.1). The LAN port is used to connect to your LAN. The other three ports are used to connect to your WAN routers. Each of the Ethernet ports must be configured to match the IP addresses of your network by using FatPipe WARP's management interface.

**A PRE-INSTALL WORKSHEET IS INCLUDED IN THE CUSTOMER PACKET THAT CAME WITH THIS PRODUCT.**

**IF YOU WANT A FATPIPE TECHNICAL SUPPORT ENGINEER TO ASSIST YOU WITH INSTALLATION, YOU WILL NEED TO FILL OUT THE PRE-INSTALL WORKSHEET AND FAX IT TO FATPIPE TECHNICAL SUPPORT.**



Fig. 1.1

1. Unpack FatPipe WARP from its shipping box.
2. You will receive a 19" rack mountable unit, a power cord, and a floppy disk containing the Paging Software.
3. To install FatPipe WARP you will need one CAT 5 Ethernet network cable for each interface you will use. You may also need a CAT 5 Ethernet crossover cable for use in between the FatPipe LAN port and a computer for initial configuration.

FatPipe WARP can be configured and managed remotely through a browser-based management application. You must use Internet Explorer 5.0 (or higher) with the Java Virtual Machine (JVM) installed to access the management tools from a remote location.

**Important:**

- *Internet Explorer 6.0 installs the JVM automatically. Other versions may not install the JVM by default. Please make sure your browser has the latest JVM installed. Visit [www.microsoft.com/java](http://www.microsoft.com/java) to find information on installing Microsoft's JVM.*
- *If you will be accessing the FatPipe management application through a firewall, make sure port 5001 is allowed for outbound connections. Also make sure Java applets are allowed through the firewall.*

## Quick Install Instructions

The following section is a quick overview of the installation process. We recommend that you refer to the rest of the manual for detailed descriptions of various menu items and screens.

Select a PC on your LAN to configure FatPipe WARP. This PC will be referred to as the Management PC. Any PC on the LAN can be used to manage WARP once initial configuration is complete.

1. Connect WARP to a UPS outlet. Power on WARP. WARP takes less than a minute to boot up.
2. Connect the LAN port to your Local Area Network and the WAN ports to your Wide Area Network routers. You need to at least connect the LAN port for initial configuration.
3. On the Management PC, go to the IP address configuration menu for the network card. (On a Windows client PC, go to Control Panel - Network - TCP/IP bound to network card - Properties). Important: Note the current IP settings so that you can reset your computer's IP information after configuration. Temporarily setup the Management PC with IP address 192.168.0.10, Subnet Mask 255.255.255.0, and Gateway 192.168.0.1.
4. If prompted, reboot Management PC and wait for it to boot back up.
5. Point the web browser on your Management PC to <http://192.168.0.1> This will bring up the Management page of WARP.
6. Click on FatPipe WARP's GO button. This will bring you to the Management Interface login page. At your first login, enter Administrator as the user name (it is case sensitive). There is no password for the first login. Simply click the Login button to access FatPipe WARP's Management Console.
7. Click Administration on the menu and select Administrator from the user list. Click Set Password to set the login password.
8. Configure all the active WAN ports at this time with IP Address, Subnet Mask, and Default Gateway settings. For more details, see Chapter 3: Interfaces, in this manual. If any of your WAN IPs are assigned using DHCP, you can select Obtain An IP Automatically Using DHCP option.
9. Configure the LAN port by clicking on LAN under Interfaces, then click the Aliases button to add an IP from your existing LAN Subnet. We recommend keeping the default 192.168.0.1 IP address as long as it does not conflict with any other IP on your network. Click Ok, then the Save button.
10. Set the TCP/IP settings of your Management PC back to the original values.

Your WARP unit will be set up for Internet access at this point.

**Helpful Tips**

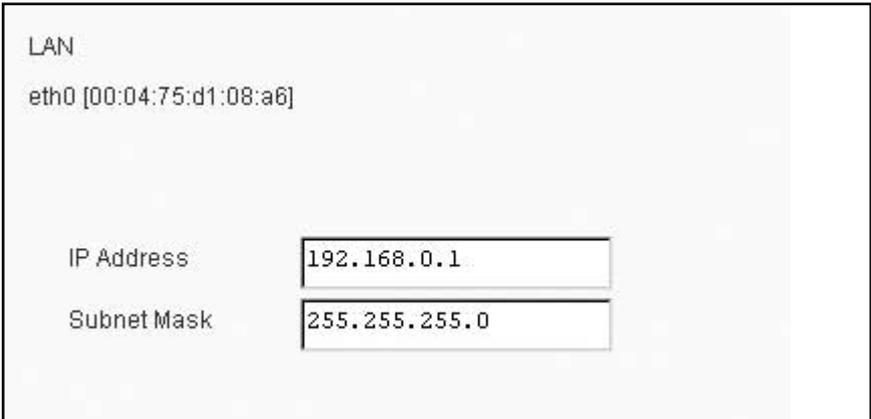
- *If you are using public IPs on the LAN side of WARP in a Pass-Through configuration, it may not be necessary to change the Default Gateway of your firewall or Default Gateway of your clients if you do not have a firewall. WARP's Proxy ARP will automatically forward packets destined for any of the WAN routers.*
- *If you are using a DHCP server on your LAN, then you may have to change the configuration of the DHCP server so that it provides the IP address of WARP's LAN port as the default gateway address.*
- *You should also reboot the routers and firewalls to clear all their ARP caches. This will assure proper network communication between network devices.*

## Chapter 2: Interfaces

Learn how to setup networking parameters to implement easy integration of WARP with your current environment by using the Interface menu on the FatPipe WARP Remote Configuration window. View and change IP Addresses, Subnet Masks, and Default Gateways in the Port Configuration screens. You can also view line status and enable or disable SSH, Remote Management, and DNS access for each WAN port.

### LAN

To set the LAN port configuration, click LAN on the port menu (See Fig. 2.1).



The screenshot displays the LAN configuration window. At the top, it shows 'LAN' and the interface identifier 'eth0 [00:04:75:d1:08:a6]'. Below this, there are two input fields: 'IP Address' with the value '192.168.0.1' and 'Subnet Mask' with the value '255.255.255.0'.

IP Address	192.168.0.1
Subnet Mask	255.255.255.0

Fig. 2.1

### LAN Port Advanced Parameters

When you have servers in your network that you want accessible from the Internet, you must setup Pass-Through or Reverse Mapping. If you set up Pass-Through instead of Reverse Mapping, you may need to assign multiple IP addresses to each server. This is required to access the servers over the multiple links to the Internet. For certain configurations, you may need to multi-home the LAN interface of the WARP unit (See Fig. 2.2). Click on Aliases to assign extra IP addresses on the LAN port.

IP Address	Subnet Mask
192.168.0.1	255.255.255.0
12.23.113.4	255.255.255.0
3.3.3.4	255.255.255.0

Fig. 2.2

### WAN

Click on WAN1, WAN2, and WAN3 icons to configure each WAN port in your network (See Fig. 2.3). This is where You can assign IP Address, Subnet Mask, and Default Gateway settings to each WAN interface (WAN1, WAN2, WAN3). To obtain the IP address automatically, check Obtain an IP Address Automatically Using DHCP. (The Default Gateway should be set to the Ethernet IP address of the router.

WAN1

eth1 [00:04:75:d1:08:57]

Obtain an IP address automatically using DHCP

Specify an IP address

IP Address

Subnet Mask

Default Gateway

Access Control:

Enable SSH

Enable Remote Management

Enable DNS

 Port Status: UP

Fig. 2.3

*Note: Port Status will read UP when the WAN connection is functioning and available for data communication. Port Status will read DOWN when the WAN connection is unavailable.*

### Access Control

FatPipe is a secure system with most services disabled except those needed to provide FatPipe Remote Management, SSH and SmartDNS. Although these services present minimal risk, this feature provides a way to limit or completely disable access. You can enable or disable access to these services by selecting or deselecting the corresponding boxes on the WAN Port Configuration pages.

## Chapter 3: Configuration

The Configuration section allows you to configure basic parameters of your WARP unit. Under the Configuration menu, You can choose a load balancing method for inbound and outbound IP traffic, set route test configurations, and setup Failover between two or more WARP units either at the same location or at separate locations. (Please refer to Chapter 7 for detailed information about Site Failover). The Configuration section is also where you can set user privileges and set user passwords.

### System Info

Click System Info to configure system settings. You can assign the host name and domain name for WARP using the corresponding fields (See Fig. 3.1). You can also access the Set System Time function to set the correct time and date for your system.



The screenshot displays a configuration interface with the following elements:

- WARP Host Name:** A text input field containing the value "warp".
- Domain Name:** A text input field containing the value "yourdomain.com".
- Current System Time:** A label indicating the current time is "3:25 PM".
- Set System Time:** A button located below the current system time label.

Fig. 3.1

## Load Balancing

FatPipe WARP provides four methods for load balancing: Round Robin (default), Response Time, Fastest Route, and On Failure. Click Load Balancing to choose a load balancing method (See Fig. 3.2).

Choose a method for load balancing

Round Robin

Response Time

Fastest Route

On Failure

Ports:	Status:
WAN1	PRIMARY
WAN2	BACK UP
WAN3	BACK UP

Fig. 3.2

**Round Robin** configures FatPipe WARP for sending IP connections sequentially over each connection to the Internet. This method is recommended for similar speed connections to the Internet, even if the connections are not of the same kind (e.g.: combining two same speed fractional T1s and a DSL line).

**Response Time** configures FatPipe WARP to balance your network's Internet traffic based on each line's average response time for Internet requests. This method is recommended for unequal speed connections. The fastest connection will be used more often with Response Time.

**Fastest Route** configures FatPipe WARP to balance load on a per destination basis. Each session will go over the fastest line for its destination. Choose this option when you want to make sure each session goes out the line with the fastest route for its destination.

**On Failure** configures FatPipe WARP to balance the network's load based on the primary line's current availability. All traffic will be directed in and out of the primary line(s). If the primary line(s) fails, all traffic will then be directed over the backup line(s). Choose this option when combining a primary and a stand-by communication line.

*Note: At least one primary line and one backup line must be selected if you choose the On Failure option (See Fig. 3.2).*

## Route Test

FatPipe WARP tests connections from the FatPipe WARP unit to the router, the router to the provider, and the WARP unit to three user-specified sites on the Internet.

To specify a test connection to an external site, enter the domain name or IP address of that site by clicking the Add button on the Route Test page (See Fig. 3.3).

Host Name/IP	Port
www.yahoo.com	80
64.124.237.148	80
64.4.50.7	25

Fig. 3.3

## Unit Failover

WARP is designed to provide a reliable and redundant connection to the Internet. WARP units can be configured to automatically failover. One would need at least two units (Active and Standby) to implement WARP Unit Failover. You can add as many standby units as you want, although one active unit and one standby unit is a typical scenario for most companies. Once configured, each unit's status will read as either Active, Up, or Down.

Completely configure, install, and test one of the WARP units connected to your network. Make sure that all of your lines are up and that the WARP is up and multiplexing traffic. Also make sure that your public servers are accessible from the Internet.

Attach the Standby WARP to a hub on the LAN side of the Active WARP. Both WARP units must have their LAN ports connected to the same hub. The Active unit will be the unit that is first online, so make sure the unit that you have initially configured is online before you bring up the Standby.

To configure failover, click Unit Failover on the menu. Select the Enable Failover check box on both units (See Fig. 3.4).

The Active unit is the live gateway for the LAN. A correctly configured Standby unit is capable of taking over for the Active unit should the Active unit experience a failure. A Standby unit will read Up in the failover cluster status page (See Fig. 3.4).

A unit in the Down state is a unit configured in the cluster, but is not functioning properly. It cannot come to a Standby state. Down units within the cluster are invisible in terms of service provided by the Active FatPipe.

Enable Failover

Cluster ID:  Port No.:

Unit List  User Specified Priority Local Unit ID:

Unit ID	Unit Name	Priority
1	Unit1	auto
2	Unit2	auto

Channel List

Interface	Source IP	Destination IPs
LAN	192.168.10.1	192.168.10.255

Fig. 3.4

Click on Failover to access the Unit Failover page (See Fig. 3.4). There you can set parameters to accomplish failover between two or more FatPipe units.

The Cluster ID is used to denote to which cluster a Unit belongs. (e.g., If you had four FatPipe WARP units, and each pair is the gateway for two dissimilar LANs, each pair would have to a different Cluster ID.)

The port number is the port used for communication between units.

Unit List specifies the FatPipe units in the current cluster.

Channel list specifies the IP addresses used for communication between the units in the cluster.

User Specified Priority: This setting allows the user to specify a priority level for each unit. Priorities are used to determine which units will be active or standby. If the field is left unchecked, it will default to the auto setting that dynamically manages unit priority.

Local Unit ID is the number assigned to a specific unit in a cluster.

### Creating or Deleting Unit Entries

Enable Failover

Cluster ID  Port No.

Unit List  User Specified Priority Local Unit ID

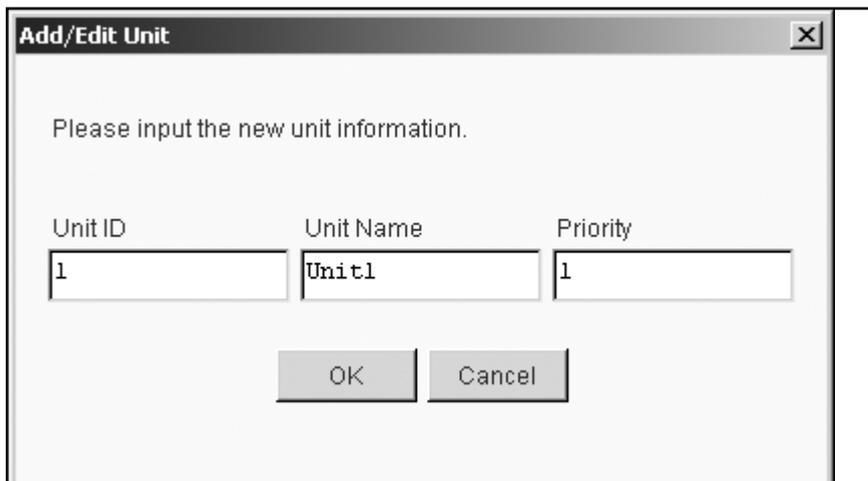
Unit ID	Unit Name	Priority
1	Unit1	auto
2	Unit2	auto

Channel List

Interface	Source IP	Destination IPs
LAN	192.168.10.1	192.168.10.255

Fig. 3.5

Click on the Add button next to the Unit List on the LAN Failover page. The Add/Edit Unit page allows you to input specific information about a unit (see Fig. 3.6).



The screenshot shows a dialog box titled "Add/Edit Unit" with a close button in the top right corner. The main text inside the dialog reads "Please input the new unit information." Below this text are three input fields arranged horizontally. The first field is labeled "Unit ID" and contains the value "1". The second field is labeled "Unit Name" and contains the value "Unit1". The third field is labeled "Priority" and contains the value "1". At the bottom of the dialog are two buttons: "OK" and "Cancel".

Fig. 3.6

The Unit ID must be specific to each FatPipe in the cluster, e.g.: 1, 2, etc.

The Unit Name should be something that corresponds to the Unit ID for easy reference.

The Priority field corresponds to the unit in the cluster that is designated as the active unit when the User Specified Priority box is enabled on the main Unit Failover page. Lower numbers are assigned the highest priority. Units within a cluster should be configured with different priorities.

## Cluster Status

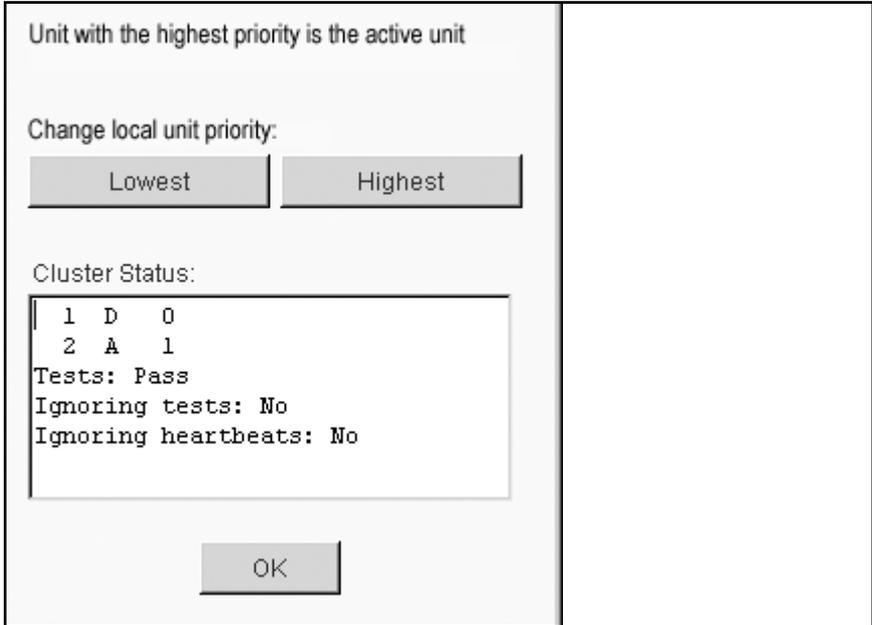


Fig. 3.7

To view the cluster status, click on Show Cluster Status (Fig.3.6) on the main Unit Failover page (see Fig. 3.7). Cluster status indicates the state of the units in the cluster.

**A** Stands for Active unit and indicates that the active unit is running properly.

**U** Stands for UP status, and that the Standby Unit is running properly.

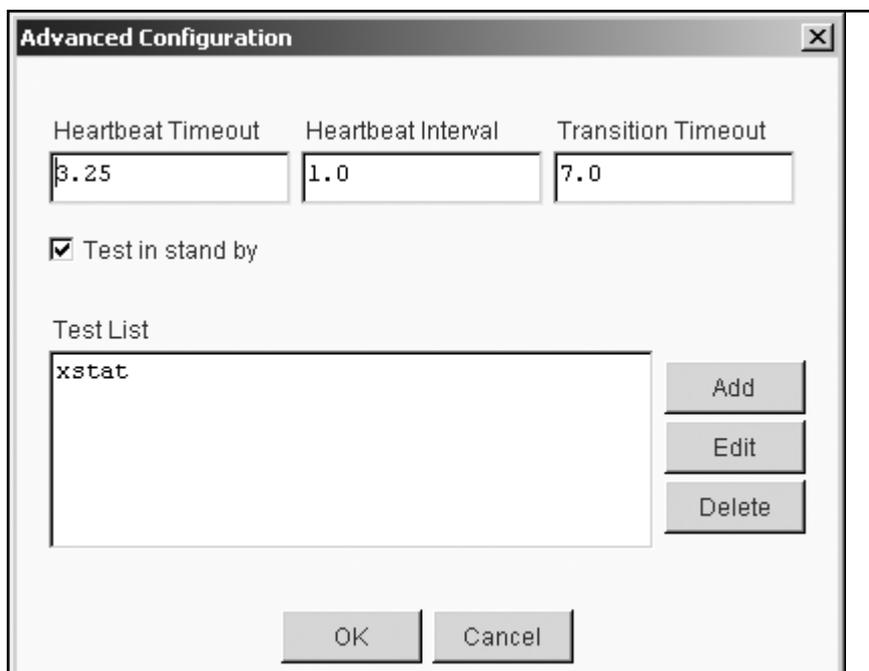
**D** Stands for Down status, and indicates the Unit is not functioning properly

The number designation listed after the cluster status (A, U, or D) shows the priority of the active and standby units.

**Please note:** If the User Specified Priority is disabled (this is default), number 1 always denotes the active unit and any number from 2 –100 denotes the standby units – numbers are dynamically assigned (see Fig. 3.7).

You can change the status of nodes by clicking on Lowest or Highest under the heading Change local unit priority on the Show Cluster Status page. Changing the local unit priority will alter the status of the unit you are observing. For example, you could choose to force the currently active unit to a Lowest unit priority, which would cause the unit to go into standby mode.

## Advanced Configuration



The screenshot shows a window titled "Advanced Configuration" with a close button (X) in the top right corner. The window contains three input fields: "Heartbeat Timeout" with the value "3.25", "Heartbeat Interval" with the value "1.0", and "Transition Timeout" with the value "7.0". Below these fields is a checkbox labeled "Test in stand by" which is checked. Underneath is a section titled "Test List" containing a text box with the value "xstat". To the right of the text box are three buttons: "Add", "Edit", and "Delete". At the bottom of the window are two buttons: "OK" and "Cancel".

Fig. 3.8

The Advanced Configuration window can be accessed by clicking on the Advanced button on the main configuration page. You can set time intervals and timeouts between active and standby units, and create a test list to test connectivity.

Heartbeat Timeout is the time parameter to wait for a heartbeat from the other FatPipe before determining that the unit in question has some trouble. Active and standby units send "heartbeats" to each other according to the heartbeat interval set by the administrator, under the Heartbeat Interval field in the Advanced Configuration page.

Transition Timeout creates a delay for testing any of the addresses listed in the Test List on the Advanced Configuration page. The unit changing to active state will ignore any scheduled tests during the transition time. This could be necessary should MAC and IP addresses change as a result of transition, and routers/switches need some time to relearn routes.

**Test List:** Configures the units to perform external tests in addition to the test connection between nodes.

The example listed in Figure x.4 shows: `xping 197.60.23.10`, used to check for Internet connectivity. This test can be made more specific by specifying a port number otherwise the test uses ICMP.

Should these tests fail regardless of the other tests, the unit in question will go into a standby state.

There can be multiple tests done so the changing in state of the unit isn't dependant on one test should the user decide to use this parameter.

### Creating LAN Channel

A Channel is a combination of Ethernet interface (or alias), and IP addresses of other units in the cluster. Each unit in the cluster uses channels to communicate with other units in a cluster. You can configure a Channel by clicking on the Add/Edit Channel button (see Fig. 3.7).

**Add/Edit Channel**

Please input the new channel information.

Source Interface: LAN

Destination IPs: 197.60.23.21

Source IP: 197.60.23.22

Source Mask: 255.255.255.0

Source Gateway: 0.0.0.0

OK Cancel

Fig. 3.9

The following fields are listed in the Add/Edit Channel configuration page (See Fig. 3.9):

**Source Interface:** This drop down menu allows you to choose which interface of the FatPipe unit you are creating the communication channel for.

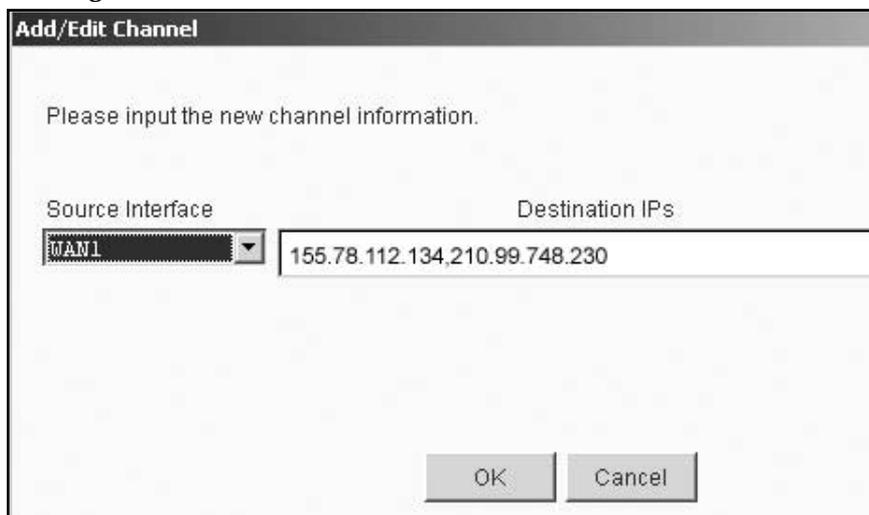
**Source IP:** This is the alias IP address that the observed unit has for its LAN interface, which is used for communication with other FatPipe units in the cluster on the LAN side.

**Destination IP:** The Destination IP is the configured alias on the LAN port of another FatPipe unit in the cluster.

**Source Mask:** This is where the administrator enters the subnet mask of the source IP.

**Source Gateway:** Always configure 0.0.0.0 in the Unit Failover to indicate that there is no gateway to utilize.

### Creating WAN Channels



The screenshot shows a dialog box titled "Add/Edit Channel". Inside the dialog, there is a text prompt: "Please input the new channel information." Below this, there are two main input areas. The first is labeled "Source Interface" and contains a dropdown menu with "WAN1" selected. The second is labeled "Destination IPs" and contains a text box with the IP addresses "155.78.112.134,210.99.748.230". At the bottom right of the dialog, there are two buttons: "OK" and "Cancel".

Fig. 3.10

### Add/Edit Channel Configuration for WAN Interfaces

**Source Interface:** This drop down menu allows you to choose which interface of the FatPipe you are creating the communication channel for. The example listed in Figure 3.10 shows that WAN1 is being configured.

**Source IP:** This is the alias IP address that the observed unit has for its WAN 1 interface, which is the IP address that is used for communication with other FatPipe units on WAN1.

**Destination IP:** The destination IP is the configured alias(es) on WAN 1 of another FatPipe in the cluster.

**Source Gateway:** the Source Gateway is where you enter the router's IP address that is attached to WAN1 of the FatPipe unit.

## Administration

Add or remove users by clicking Administration and then Add User or Delete User. You can change User Privileges and Passwords in this menu. Only an Administrator can set privileges, add or remove users, and change passwords (See Fig. 3.11).

This is also where you can import and export configuration files from this page by clicking Administration and then Import WARP Settings or Export WARP Settings.

You can also restore system defaults by clicking on the Restore System Default Setting button in the Administration menu.

The screenshot displays a web interface for user administration. It features two columns: 'User Name:' and 'Privilege:'. The 'User Name:' column lists 'Administrator', 'Jason', and 'T-bone'. The 'Privilege:' column lists 'ADMINISTRATOR', 'ADMINISTRATOR', and 'USER'. To the right of these columns are four buttons: 'Add User', 'Delete User', 'Set Privilege', and 'Set Password'. Below these columns are four buttons arranged in a 2x2 grid: 'Restore WARP Settings', 'Set Login Banner', 'Backup WARP Settings', and 'Restore Defaults'.

User Name:	Privilege:	
Administrator	ADMINISTRATOR	Add User
Jason	ADMINISTRATOR	Delete User
T-bone	USER	Set Privilege
		Set Password

Restore WARP Settings	Set Login Banner
Backup WARP Settings	Restore Defaults

Fig. 3.11

## Chapter 4: Advanced Configuration

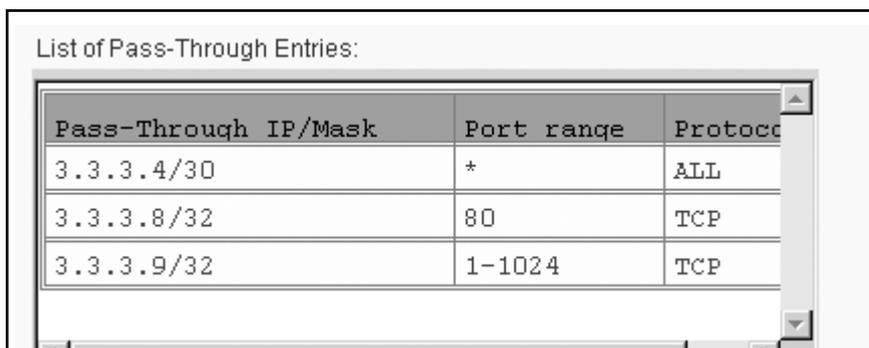
FatPipe WARP provides dynamic load balancing algorithms for inbound as well as outbound IP traffic. WARP supports the hosting of internal servers including web, e-mail, firewall, and load balancing servers. WARP features FatPipe's SmartDNS™, Pass-Through, and Reverse Mapping technologies for inbound load balancing. To allow inbound traffic, you must setup Pass-Through or Reverse Mapping.

### Pass-Through

Pass-Through allows public IPs to be used internally. You must use a smaller subnet, typically a /30 (255.255.255.252) subnet, on WARP's WAN port. The router, firewall, and any other device with a public IP will be assigned the full subnet mask. WARP's LAN port will also be assigned the full subnet mask. WARP will use Proxy ARP to route traffic back to the LAN for the IPs you specify under Pass-Through. You can specify single IPs using a /32 mask or an entire IP subnet using other masks (e.g., /24 for a block of 256 IPs).

You may need to make changes to your router, firewall, or other network devices to setup WARP in a Pass-Through configuration. For the router to communicate with WARP, it must have an IP address that is in the /30 subnet, even though it is assigned the full subnet mask. Also, the network and broadcast IPs of the /30 subnet are unusable because they cannot be routed back to the LAN.

To use Pass-Through, click Pass-Through under the Advanced Configuration section of the menu. Click Add, Edit, or Delete to complete your task (See Fig. 4.1).



The screenshot shows a window titled "List of Pass-Through Entries:" containing a table with three columns: "Pass-Through IP/Mask", "Port range", and "Protocol". The table lists three entries:

Pass-Through IP/Mask	Port range	Protocol
3.3.3.4/30	*	ALL
3.3.3.8/32	80	TCP
3.3.3.9/32	1-1024	TCP

Fig. 4.1

## Reverse Mapping

Reverse Mapping uses NAT (Network Address Translation) and PAT (Port Address Translation) to map public IPs to internal IPs for a single port or all ports. This allows public access to internal servers. You can map a public IP to an internal private IP or if Pass-Through is used with another WAN line, you can map a public IP from one line to a public IP from the Pass-Through line.

Multiple public IP addresses can be mapped to one or more internal IP addresses. This means that if you use Reverse Mapping on two of your WAN lines, you can map two different public IP addresses to a single internal server and not have to multi-home the internal server. Reverse Mapping is also useful for conserving public IP space by allowing a single public IP address to be mapped to one or more internal servers based on port numbers.

To use Reverse Mapping, click on Reverse Mapping under the Advanced Configuration section of the menu.

Enter the external IP addresses and port numbers in the corresponding boxes as well as the internal IP addresses and port numbers you would like to map them to, one set at a time. Click on the Save button to save changes (see Fig. 4.2).

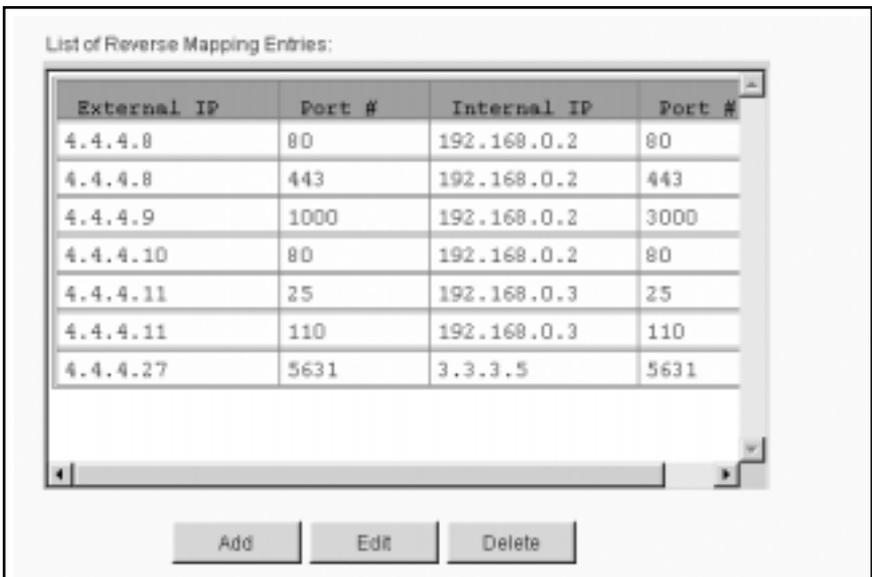


Fig. 4.2

## Static Routes

When you have servers in your network that need to be accessible from the Internet, you may need to setup static routes to these servers. This section describes how to configure FatPipe WARP to direct Internet traffic in large networks with multiple sub-networks.

Click on Static Routes to add or remove static route configurations (See Fig. 4.3). Static Routes are used to direct packets to their specified destination through the user-defined gateway. The Metric defines the number of hops between WARP and the gateway (minimum 2). A Destination IP Address, a Network Subnet Mask, a Gateway IP Address, and a Metric Parameter form one static route. The Add, Edit, and Delete buttons are used to add, edit, or delete a static route.

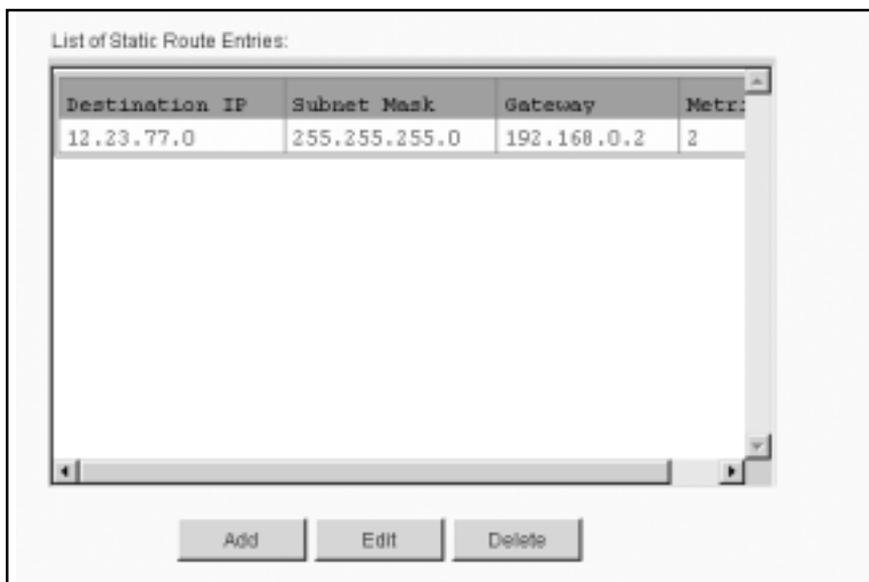


Fig. 4.3

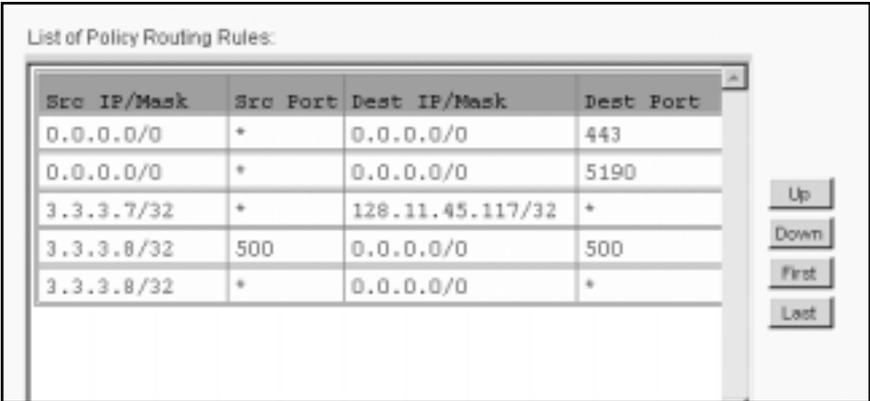
## Policy Routing

Policy Routing allows you to direct outbound traffic based on specific criteria. It uses prioritized rules that define the criteria and the traffic mode used when a data stream matches the criteria (See Fig. 4.5).

Each rule has the following criteria:

- Source IP/Mask: Single IP, whole IP subnet, or all IPs
- Source Port(s): Single port, port range, or all ports
- Destination IP/Mask: Single IP, whole IP subnet, or all IPs
- Destination Port(s): Single port, port range, or all ports
- Protocol(s): Specific protocol or all protocols

Source IP/Mask and Destination IP/Mask can use an asterisk (\*) to indicate all IPs. Source and Destination Port(s) can use a hyphen to specify port ranges (e.g., 1-1024) or use an asterisk (\*) to specify all ports.



List of Policy Routing Rules:

Src IP/Mask	Src Port	Dest IP/Mask	Dest Port
0.0.0.0/0	*	0.0.0.0/0	443
0.0.0.0/0	*	0.0.0.0/0	5190
3.3.3.7/32	*	128.11.45.117/32	*
3.3.3.8/32	500	0.0.0.0/0	500
3.3.3.8/32	*	0.0.0.0/0	*

Buttons: Up, Down, First, Last

Fig. 4.4

Each rule has two possible traffic modes: Interface Priority and Interface Specific.

- Interface Priority directs traffic out the first live line, using a user-specified WAN port order. NAT can be enabled or disabled per port in the port order.
- Interface Specific directs traffic out only the specified line(s). NAT can be enabled or disabled per selected port.

The rules are prioritized, which means that the first rule that matches is applied. If the top rule is not matched, the next rule is checked, and on down the rule-set until the bottom is reached. If no rules are matched, the default rule is applied. The default rule is to mask (NAT) and multiplex (send out all live ports) outbound traffic.

---

To use Policy Routing, click on Policy Routing under Advanced Configuration on the menu. On the Policy Routing page, click Add, Edit, or Delete to add, edit delete a new Policy Routing rule.

## Policy Routing Examples

### FTP Example

Src IP/Mask: 207.88.121.10/32 Src Port: \*

Dest IP/Mask: 166.70.117.245/32 Dest Port: 20-21

Protocol: TCP

Traffic Mode: Interface Specific

- WAN1: Enabled (checked) with NAT Disabled (unchecked)
- WAN2: Disabled (unchecked)
- WAN3: Disabled (unchecked)

Details: This policy states that when the device with address 207.88.121.10 goes to connect to 166.70.117.245 on ports 20-21 (FTP), to send traffic only out WAN1 and not to use NAT.

### HTTP Example

Src IP/Mask: 207.88.121.10/32 Src Port: \*

Dest IP/Mask: 167.80.119.10/32 Dest Port: 80

Protocol: TCP

Traffic Mode: Interface Specific

- WAN1: Disabled (unchecked)
- WAN2: Enabled (checked) with NAT Disabled (unchecked)
- WAN3: Disabled (unchecked)

Details: This policy states that when the device with address 207.88.121.10 connects to 167.80.119.10 on port 80 (HTTP), to send traffic only out WAN2 and not to use NAT.

### HTTPS Example

Src IP/Mask: \* Src Port: \*

Dest IP/Mask: \* Dest Port: 443

Protocol: TCP

Traffic Mode: Interface Priority with port order: WAN1, WAN2, WAN3

- WAN1: NAT Enabled (checked)
- WAN2: NAT Enabled (checked)
- WAN3: NAT Enabled (checked)

Details: This policy states that any connection going to any IP for HTTPS (SSL Secure website), to send traffic out WAN1, unless it's down then use WAN2, unless both are down then use WAN3. You must enable (check) NAT on each of these ports for this to work.

**VPN Example (Part 1)**

Src IP/Mask: \* Src Port: \*  
Dest IP/Mask: 500 Dest Port: 500  
Protocol: UDP

Traffic Mode: Interface Specific

- WAN1: Enabled (checked) with NAT Disabled (unchecked)
- WAN2: Disabled (unchecked)
- WAN3: Disabled (unchecked)

Details: This policy states that any connection that has source UDP port 500 destined for UDP Port 500 (IKE, Internet Key Exchange), to send traffic only out WAN1 and not to use NAT.

**VPN Example (Part 2)**

Src IP/Mask: \* Src Port: \*  
Dest IP/Mask: \* Dest Port: \*  
Protocol: ESP

Traffic Mode: Interface Specific

- WAN1: Enabled (checked) with NAT Disabled (unchecked)
- WAN2: Disabled (unchecked)
- WAN3: Disabled (unchecked)

Details: This policy states that any connection using the ESP protocol (used with IPSEC), to send traffic only out WAN1 and not to use NAT.

**Legend:**

\* = All Ports or All IPs  
Src Port = Source Port  
Dest Port = Destination Port

**SmartDNS**

SmartDNS provides inbound load balancing and inbound redundancy to internal servers.

**The benefits of FatPipe's SmartDNS feature are:**

- Load Balancing: SmartDNS balances load by advertising the different paths into a host on a LAN. The host appears to be a different IP address at different times, thus using all available lines. The IP addresses are resolved based on the selected load-balancing algorithm (See Chapter 3: Load Balancing).
- Speed: Through load balancing, FatPipe SmartDNS speeds up the delivery of inbound traffic according to the currently selected load-balancing algorithm.
- Failover: SmartDNS will dynamically sense when a failure occurs and will make adjustments to the DNS replies so it will not hand out IP addresses that are associated with the connection that is down.

SmartDNS allows hosts on a network to have multiple IP addresses associated with them from different providers, and will hand out the IP addresses for these hosts using the load-balancing algorithm selected in the Load Balancing configuration. SmartDNS tests the different connections and can detect when connections fail.

### **Setup Steps for Moving DNS to WARP**

1. Register a new domain with a registrar, or if you have an existing domain, get all current domain information from current DNS provider (the group managing your DNS, typically one of your ISPs).
2. Register new name server names with the registrar using your domain name (e.g., ns1.yourdomain.com and ns2.yourdomain.com).
3. Setup DNS Zone (domain information) on FatPipe WARP.
4. Initiate a transfer of your domain name with the registrar and point it to your newly registered name server names (e.g., ns1.yourdomain.com and ns2.yourdomain.com).

### **Registering a New Domain Name**

You must contact a domain registrar to register a domain name. You can get a full list of ICANN-accredited registrars from InterNIC.com. Directnic.com and Networksolutions.com are two of the competing ICANN-accredited registrars you can use. In the course of registering the new domain, you may be required to provide two name servers that will handle your domain name. If the registrar provides default name servers, you can use them. Otherwise, just specify any existing name servers (perhaps just put in ns.yahoo.com and ns1.yahoo.com and their corresponding IP addresses). Selecting a domain is really not significant at the point of registration. You will transfer these domains to your name server names in a future step.

### **Registering Name Servers**

Contact your registrar to initiate the creation of your new name servers using your domain name (e.g., ns1.yourdomain.com and ns2.yourdomain.com). Each name server name will map to its own WAN port IP address on WARP. As far as the registrar knows, your domain name is handled on multiple physical name servers, but in reality you're simply mapping a different name server name to each of the WAN port IP addresses.

### **Setting Up DNS Zone (Domain Information)**

To achieve inbound redundancy, each domain name record (e.g., www) will have multiple IP addresses assigned to it -- one from each WAN IP block. SmartDNS will hand out these IP addresses based on the type of load balancing you have set WARP to use. If you choose Round Robin, the IP addresses are handed out in a round-robin fashion. If you choose Response Time, packets will be handed out based on the response time of each WAN line. If you use On Failure, only IP addresses from the designated primary WAN lines are handed out. If you specify two primary WAN lines, then the two IP addresses associated with those lines are handed out in a round-robin fashion.

**Basic SmartDNS Example**

1st WAN IP Block	7.0.0.0 – 7.0.0.255
2nd WAN IP Block	8.0.0.0 – 8.0.0.255
3rd WAN IP Block	9.0.0.0 – 9.0.0.255

**IP Addresses on FatPipe WAN Ports**

WAN1	7.0.0.2
WAN2	8.0.0.2
WAN3	9.0.0.2

**Registered Name Servers**

ns1.yourdomain.com	7.0.0.2
ns2.yourdomain.com	8.0.0.2
ns3.yourdomain.com	9.0.0.2

**SmartDNS Name Server Entries (NS records)**

Name	Name Server
@	ns1.yourdomain.com
@	ns2.yourdomain.com
@	ns3.yourdomain.com

**SmartDNS Host Name Entries (A records)**

Name	IP Address
@	7.0.0.5
@	8.0.0.9
@	9.0.0.44
www	7.0.0.5
www	8.0.0.9
www	9.0.0.44
ftp	7.0.0.7
ftp	8.0.0.35
ftp	9.0.0.19

**Transferring the Domain to Your New Name Server Names**

Contact your existing registrar to initiate the transfer to your new name server names. This is usually done online by logging into your account at the registrar's website and filling out the proper request for transfer.

**A Quick Note About Time to Live (TTL)**

SmartDNS uses a short TTL to ensure the information about the IP addresses for the hosts it serves are accurate and up-to-date. This means that the machines on the Internet will always connect to the host using a route that is available instead of trying to access the host using an IP address that is not accessible due to a line failure.

The TTL value informs all DNS servers on the Internet how long they should store information about your domain. For example, a name server caches your domain information following a request for a website that uses your domain. Until the TTL value is exceeded, that name server will continue using the information supplied by the first request each time your domain is requested. When

your domain is requested after the TTL period, the name server will conduct a new query for updated information about your domain. The TTL value is measured in seconds.

WARP ensures that DNS information is up-to-date. You can change the TTL to your own preferences, along with Refresh, Expire, and Retry entry settings.

Set TTL, Refresh, Expire, and Retry settings by entering the corresponding information in the Master Zone Defaults by clicking through the SmartDNS, Create Master, and Create Master Zone configuration pages. You must click on SAVE to activate all changes made to the SmartDNS settings.

### SmartDNS Setup

Click on SmartDNS to access the SmartDNS page (See Fig. 4.5). Click on the Create Master button to input Domain Name, Master Server, e-Mail address, and Records File information (see Fig. 4.5).

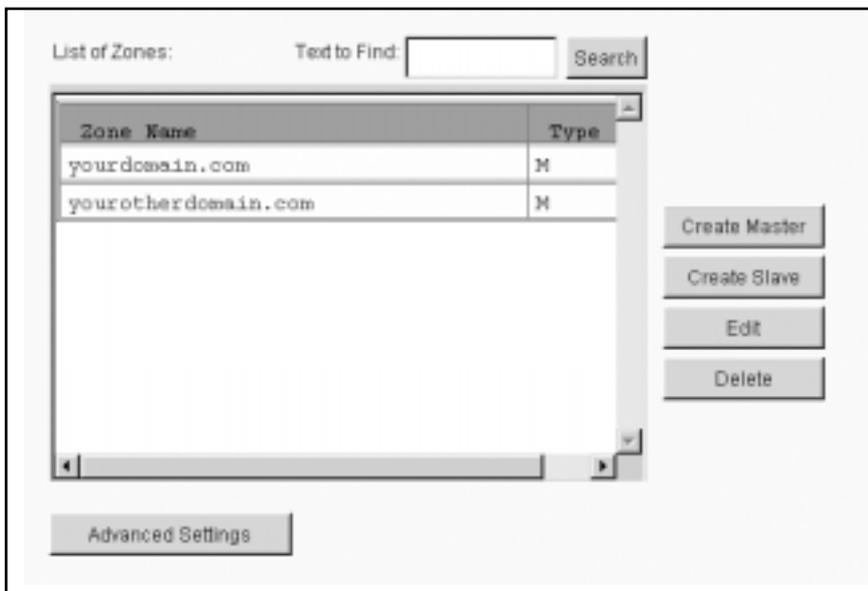


Fig. 4.5

To set default values for the Master Zone, enter Refresh, Retry, Expire, and TTL information under Zone Parameters (See Fig. 4.6).

The screenshot displays the configuration interface for a Master Zone. At the top, under the heading "Records:", there are five buttons for record types: A, NS, MX, CNAME, and PTR. Below this, the "Master Server" field is set to "ns.yourdomain.com.", the "Email Address" field is set to "admin.yourdomain.com.", and the "Records File" field is set to "yourdomain.com" with an "or" option and an unchecked "None" checkbox. The "Zone Parameters:" section contains four input fields: "Refresh" (28800), "Retry" (7200), "Expire" (604800), and "TTL" (10).

Records:				
A	NS	MX	CNAME	PTR
Master Server	ns.yourdomain.com.			
Email Address	admin.yourdomain.com.			
Records File	yourdomain.com	or	<input type="checkbox"/> None	
Zone Parameters:				
Refresh	28800	Retry	7200	
Expire	604800	TTL	10	

Fig. 4.6

To continue configuration of the master zone, highlight the zone under the List of Zones and click on Edit, which will take you to the Edit Master Zone window. This is where you setup Zone Parameters. Zone Parameters are measured in seconds.

Enter and edit basic data and records in the Edit Master Zone window. There are five types of records: A, NS, CNAME, MX, and PTR. You can create, edit, or delete existing records by clicking on the corresponding buttons (See Fig. 4.7).

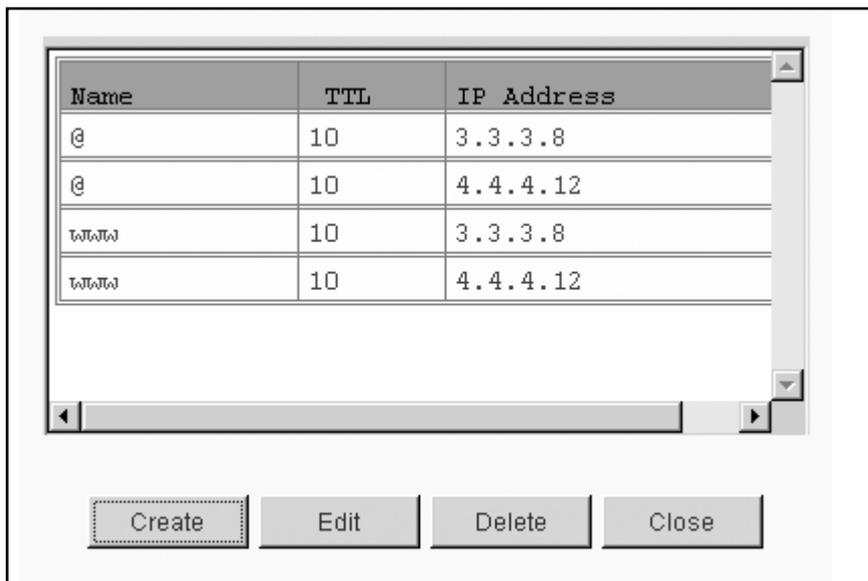


Fig. 4.7

To create a slave zone, click on the Create Slave button and enter the Domain Name, Master Server IP address, and Records File information.

### Session Timeouts

Set TCP and UDP idle timeouts on the Sessions Timeouts page under Advanced Configuration on the menu. The defaults are 120 minutes for TCP and 3 minutes for UDP (See Fig. 4.8).



Fig. 4.8

## Chapter 5: Tools

FatPipe WARP provides graphical monitoring tools to aid you in monitoring the speed and performance of your Internet connections. This chapter describes the methods to view the Speed Chart and the Speed Meter.

### Speed Chart

Monitor the upload and download or combined speeds of each of the WAN lines independently or in combination. To view the chart, click Speed Chart (See Fig. 5.1).

There are five views to choose from:

- WAN1 - Displays Total Speed, Upload Speed, and Download Speed for WAN1
- WAN2 - Displays Total Speed, Upload Speed, and Download Speed for WAN2
- WAN3 - Displays Total Speed, Upload Speed, and Download Speed for WAN3
- ALL PORTS TOGETHER - Displays Total Speed, Total Upload Speed, and Total Download Speed of all WAN ports
- ALL PORTS - Displays Total Speed for each of the WAN ports on the same graph

The Speed Chart is a dynamic, real-time chart that updates every second. The scale dynamically changes based on the current bandwidth.

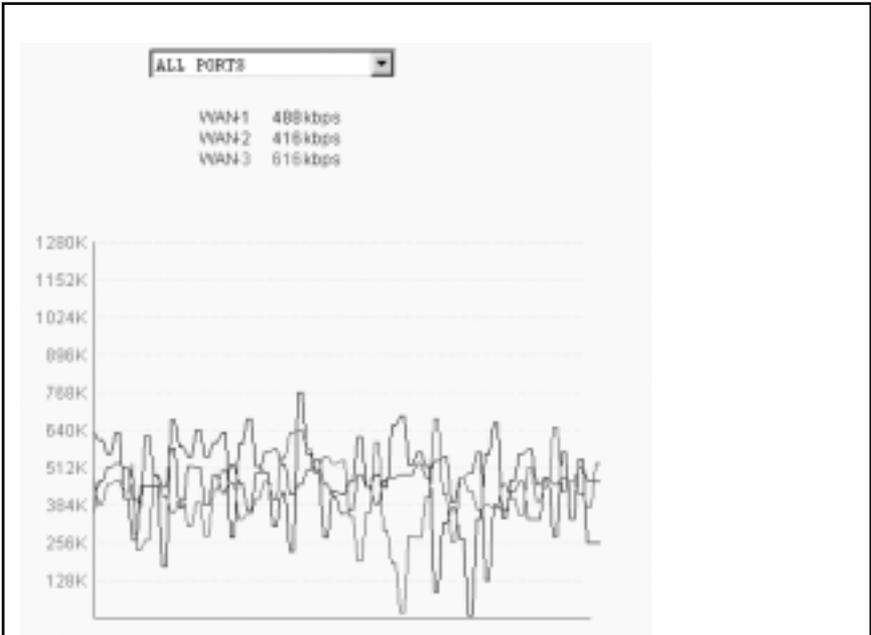


Fig. 5.1

## Speed Meter

Monitor the upload and download or combined speeds of each of the WAN lines independently or in combination. To view the meter, click Speed Meter (See Fig. 5.2).

There are four views to choose from:

- WAN1 - Displays Total Speed, Upload Speed, and Download Speed for WAN1
- WAN2 - Displays Total Speed, Upload Speed, and Download Speed for WAN2
- WAN3 - Displays Total Speed, Upload Speed, and Download Speed for WAN3
- ALL PORTS TOGETHER - Displays Total Speed, Total Upload Speed, and Total Download Speed of all WAN ports

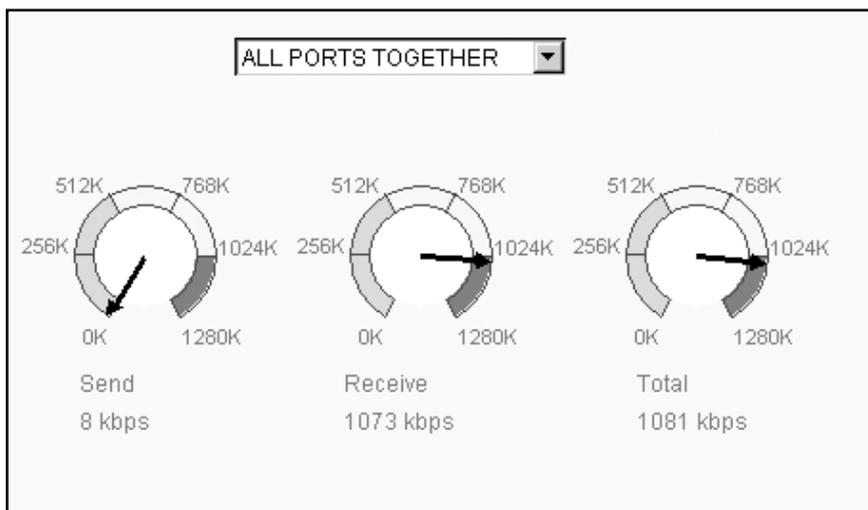


Fig. 5.2

## Diagnostics

FatPipe WARP can test both physical and Internet service connections for availability. Select the Diagnostics page to run various tests.

Ping a host or Trace Route to a host to test connectivity (See Fig. 5.3). Enter the IP address or domain name of the host, which can be a router, server, or any other IP enabled device. You can also select which port to run these tests from.

Click Show System Statistics to view information about WARP including system uptime and port statistics (e.g., packets received, packets transmitted, and any packet errors).

Host:  Port:

Display Results:

```
port 1:
  RX pkts: 12622969 err:0 drop: 0 coll: 0
  TX pkts: 331001 err:0 drop: 0
port 2: up: 90.8% down: 9.2%
  RX pkts: 2443762 err: 0 drop: 0 coll: 136
  TX pkts: 1182366 err: 0 drop: 0
port 3: up: 99.8% down: 0.2%
  RX pkts: 2401683 err: 3 drop: 0 coll: 277
  TX pkts: 1037322 err: 0 drop: 0
port 4: up: 99.0% down: 1.0%
  RX pkts: 1011213 err: 0 drop: 0 coll: 69
  TX pkts: 1098127 err: 0 drop: 0
```

Fig. 5.3

Click Show Route Test Display to view a graphical display of current line status (See Fig. 5.4).

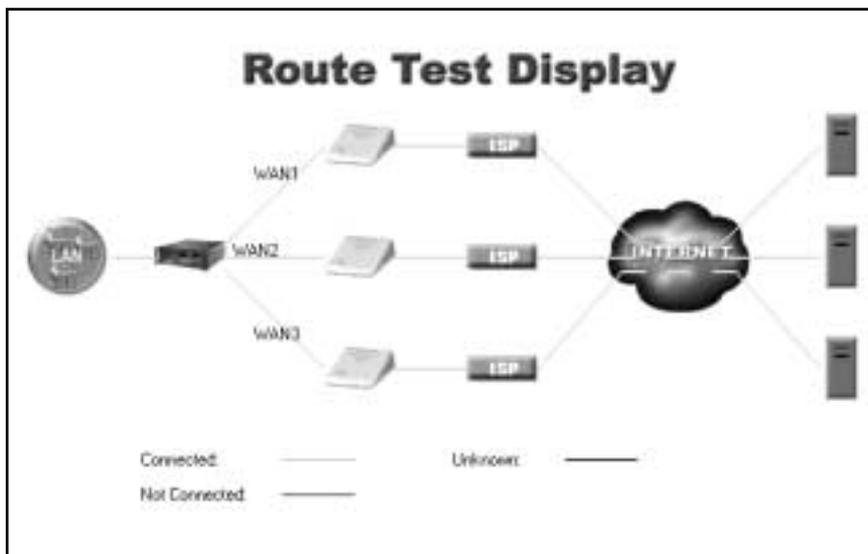


Fig. 5.4

## SNMP

FatPipe WARP supports SNMPv2 (Simple Network Management Protocol version 2) with MIB-II (Management Information Base II) compliance, to accommodate SNMP queries in addition to sending out SNMP traps. This allows you to use SNMP management software to monitor and gather statistics from WARP and view and monitor system parameters of your WARP unit without opening the FatPipe GUI. However, currently Fatpipe products do not support any write access via SNMP managers. (You can also configure WARP to send an SNMP trap to alert you when a line goes down or comes back up).

**Most Users will not need to change the default settings because the FatPipe SNMP default settings will allow you to query all the same MIBs with in SNMPv2. You only change the default settings if you want to create groups and user permissions.**

Note: Visit <http://community.roxen.com/developers/idocs/rfc/rfc2575.html> for detailed information on SNMP terminology and technology concepts outlined in RFC 2575 and RFC 2571.

**Configuring SNMP**

Click on SNMP on the Remote Configuration menu to view the main SNMP configuration page, where you can view the SNMP menu to setup SNMP community names, group names, securities, user permissions, and traps (see Fig. 5.5).

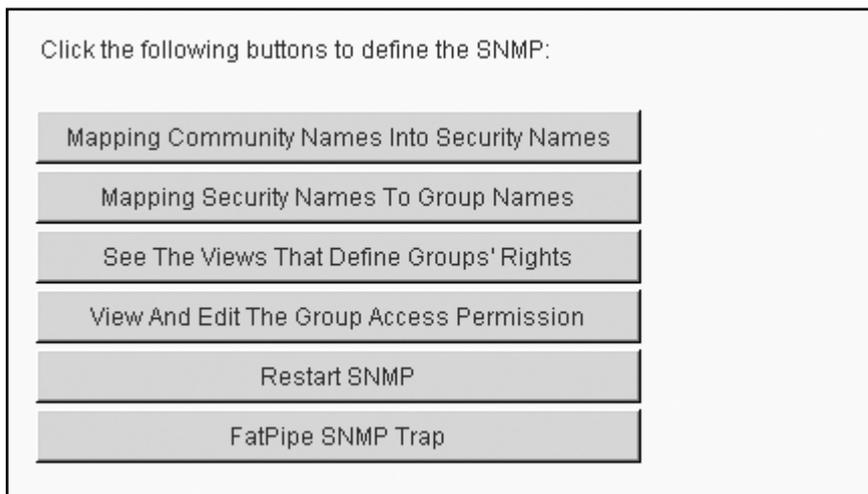


Fig. 5.5

To add or edit communities, click on the Mapping Community Names Into Security Names button located on the main SNMP configuration page (see Fig. 5.5). You will view the Security Mapping page, where you can add, edit, or delete a map (see Fig. 5.6).

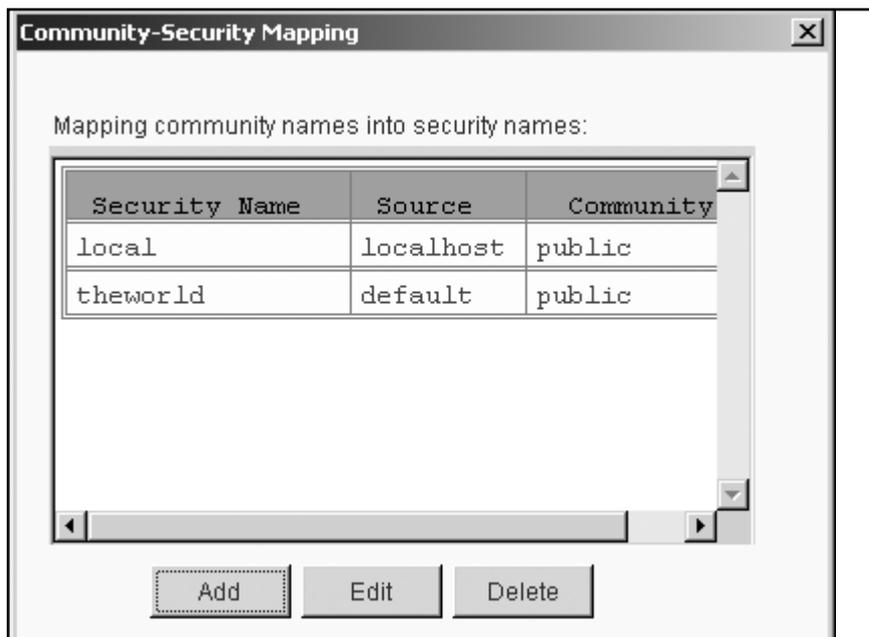


Fig. 5.6

Clicking on Add or Edit button will bring you to the Add/Edit Community Security Mapping page, where you can input or change the security name, source, or community settings (see Fig. 5.7).

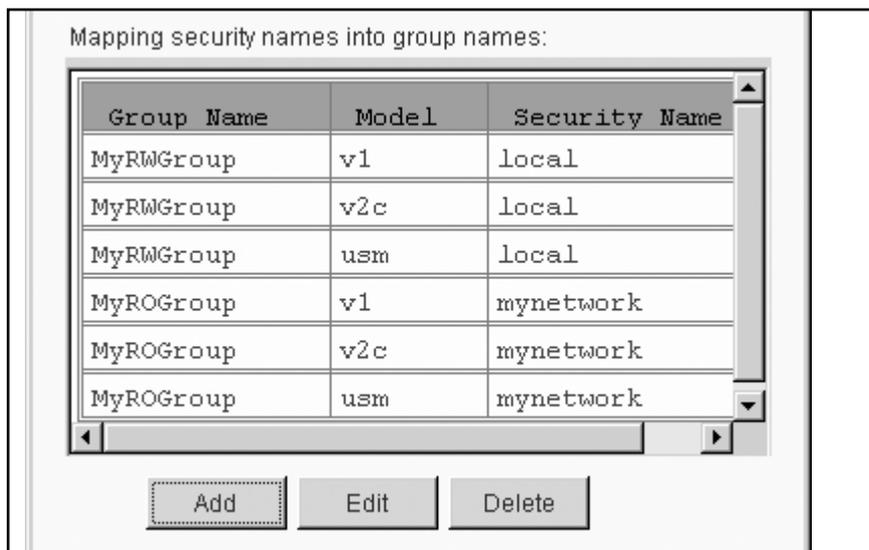


Fig. 5.7

To add or edit groups, click on Mapping Security Names to Group Names located on the main SNMP configuration page (see Fig. 5.8).

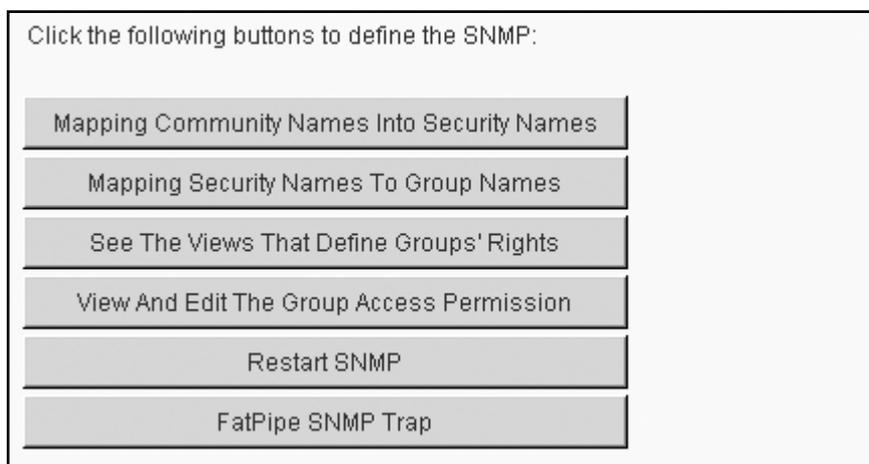


Fig. 5.8

Clicking on the Add or Edit buttons will open another window where you can input or modify group names, models, and security names (see Fig. 5.9).

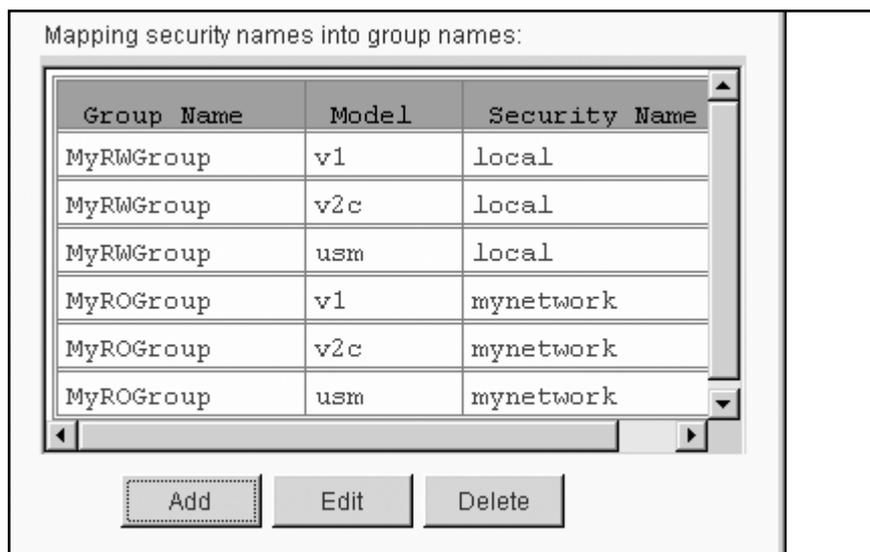


Fig. 5.9

To add or edit views, click on the See The Views That Define Groups' Rights button located on the main SNMP configuration page (see Fig. 5.10).

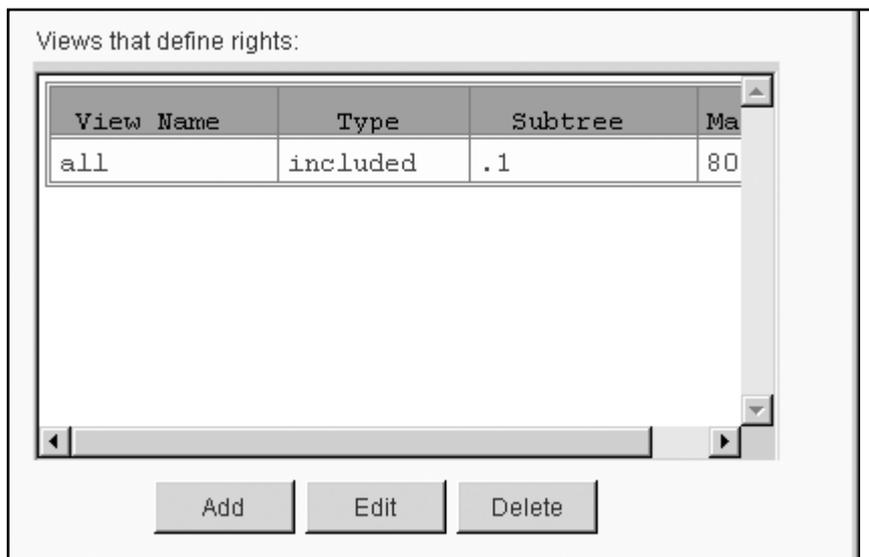


Fig. 5.10

Clicking on the Add or Edit buttons will open window box where you can input or modify view name, type, subtree, and mask (see Fig. 5.11).

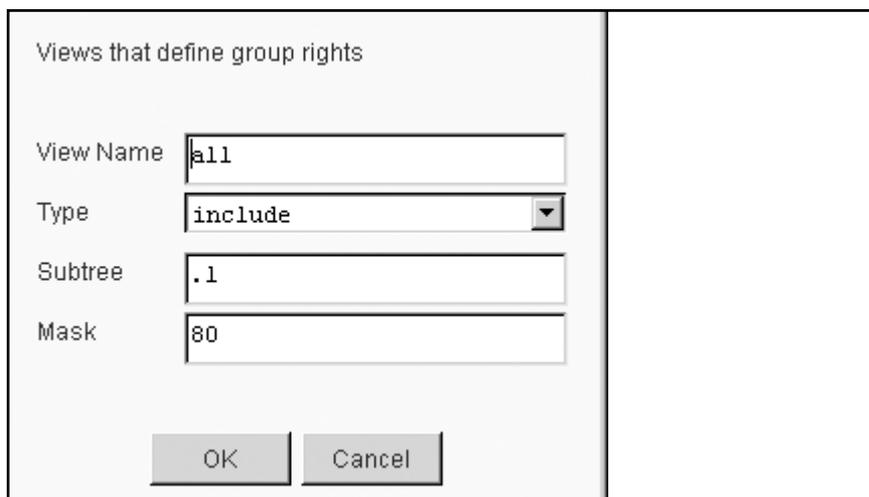


Fig. 5.11

To add, edit, or delete group access permissions, click on View And Edit The Group Access Permission button located on the main SNMP configuration page (See Fig. 5.12).

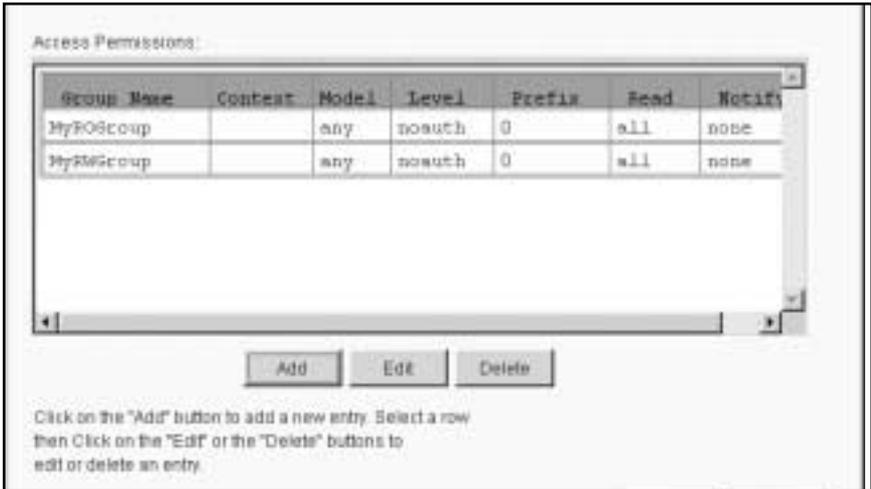


Fig. 5.12

Access Permission

Group Name	MyR06Egroup	Context	
Model	any	Level	noauth
Read	all	Notify	none
Prefix	exact		

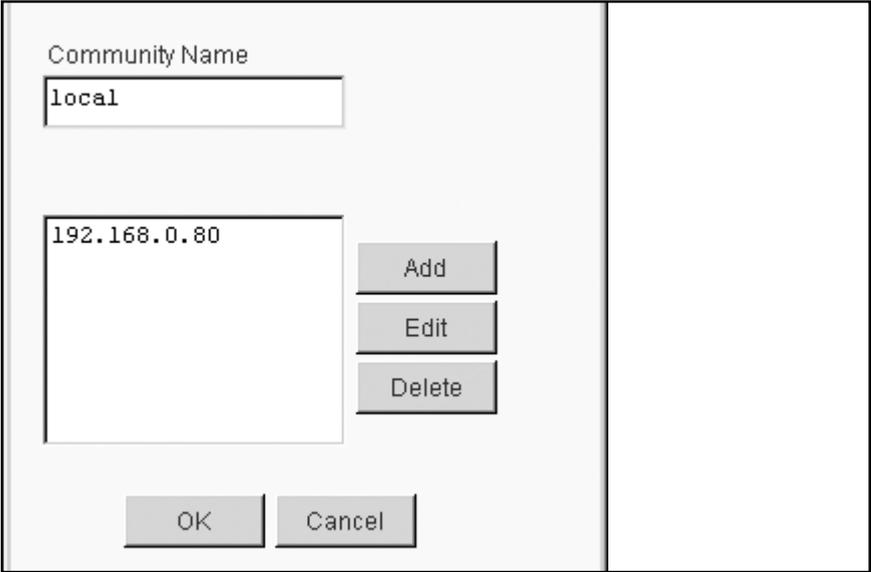
OK Cancel

Fig. 5.13

Clicking on the Add or Edit buttons will open another dialog box where you can input or modify group names, context, model, level, prefix, read, and prefix status.

Click on Restart SNMP, located on the main SNMP configuration page, to activate the SNMP agent configuration parameters you have setup.

To add, edit, or delete trap destinations, click on the FatPipe SNMP Trap button on the main SNMP configuration page. (See Fig. 5.14)

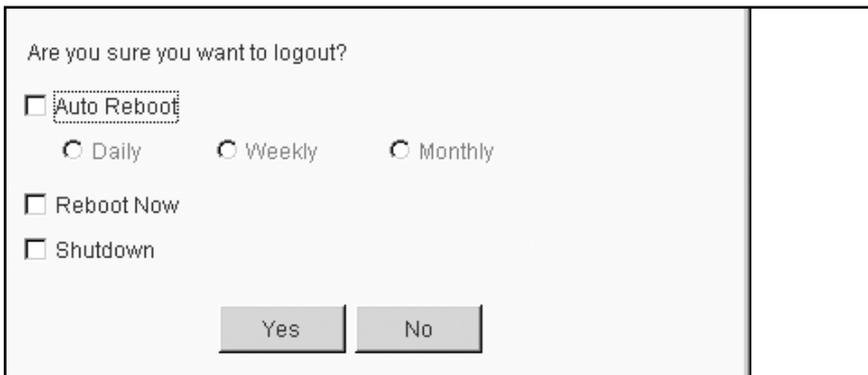


The image shows a configuration dialog box for SNMP traps. It is divided into two main sections. The left section contains a 'Community Name' field with the text 'local' entered. Below this is a larger text area containing the IP address '192.168.0.80'. To the right of this text area are three vertically stacked buttons: 'Add', 'Edit', and 'Delete'. At the bottom of the left section are two buttons: 'OK' and 'Cancel'. The right section of the dialog box is currently empty.

Fig. 5.14

## Reboot/Shutdown

Reboot or shutdown WARP safely by choosing the corresponding option.



Are you sure you want to logout?

Auto Reboot

Daily     Weekly     Monthly

Reboot Now

Shutdown

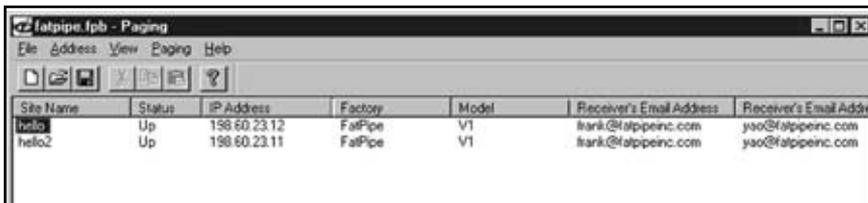
Fig. 5.15

## Chapter 6: Paging Software

FatPipe WARP comes with monitoring software, which will continuously test the status of the services going through the WARP unit, as well as the unit itself. The software alerts you if a failure occurs on the WAN. The Paging Software is provided on a floppy disk.

The Paging Software installs on any Windows® PC on the network (See Fig. 6.1). To use the Paging Software, you should have a text mode pager/cell phone and have e-mail paging capability.

If the status of WARP is normal, the status entry in the list will display Up, otherwise it will display Down. FatPipe WARP Paging Software will start monitoring by default. To stop the monitoring, click Paging on the menu and then choose Stop.

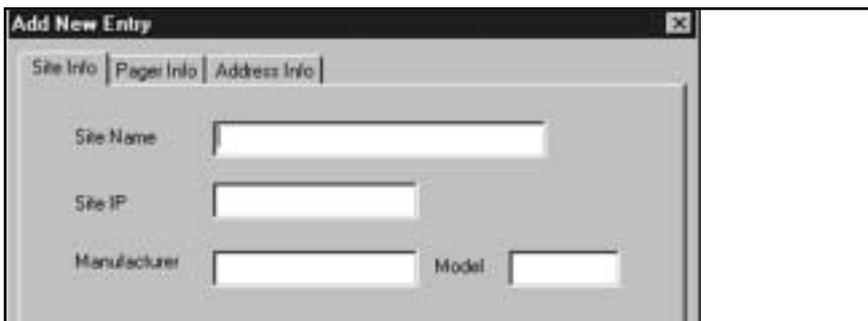


Site Name	Status	IP Address	Factory	Model	Receiver's Email Address	Receiver's Email Address
hello	Up	198.60.23.12	FatPipe	V1	frank@fatpipeinc.com	yao@fatpipeinc.com
hello2	Up	198.60.23.11	FatPipe	V1	frank@fatpipeinc.com	yao@fatpipeinc.com

Fig. 6.1

### Add New Pager Information

To add new site information to the database, you can press the Insert key on the keyboard or go to Address on the menu and click Add. This will bring up a dialog box as Figure 6.2 illustrates. The Site Name is the place where WARP resides; it can be any user defined unique name. The IP Address will be any valid IP address of the FatPipe WARP. The Manufacturer and Model are optional.



The dialog box titled "Add New Entry" has three tabs: "Site Info", "Pager Info", and "Address Info". The "Site Info" tab is selected. It contains four input fields:

- Site Name:
- Site IP:
- Manufacturer:
- Model:

Fig. 6.2

Click on Pager Info tab to bring up a window as shown in Figure 6.3. The Receiver's E-mail Address1 is the destination e-mail address where information should be sent. A send receiver (Administrator) can be entered on the Receiver's E-mail Address2 (optional). The Sender's E-mail Address is the e-mail address of the sender. The user must enter the SMTP server name or IP address for the page to be sent. The fields Area Code and Pager Number also have to be entered for paging.

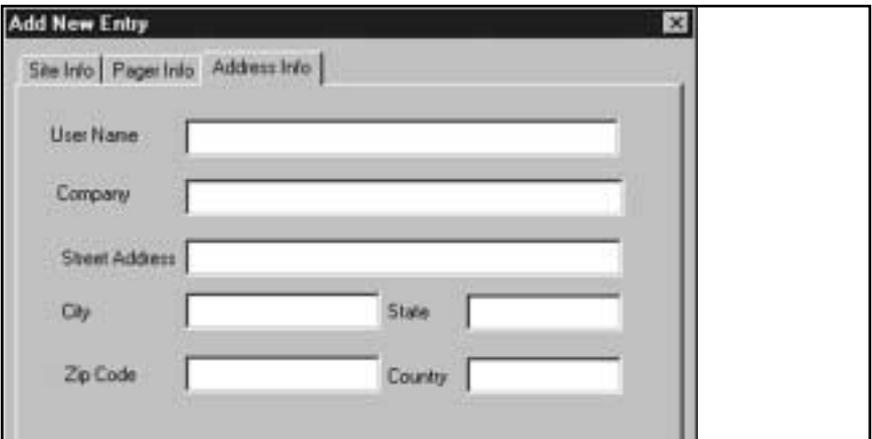


The screenshot shows a dialog box titled "Add New Entry" with a close button in the top right corner. It has three tabs: "Site Info", "Pager Info", and "Address Info". The "Pager Info" tab is selected. The form contains the following fields:

- Receiver's Email Address1:
- Receiver's Email Address2:
- Sender's Email Address:
- Sender's SMTP Server:
- Area Code:
- Pager Number:

Fig. 6.3

Click on Address Info tab to bring up the window shown in Figure 6.4. All fields in this window are optional. The user can enter this information for additional detail.



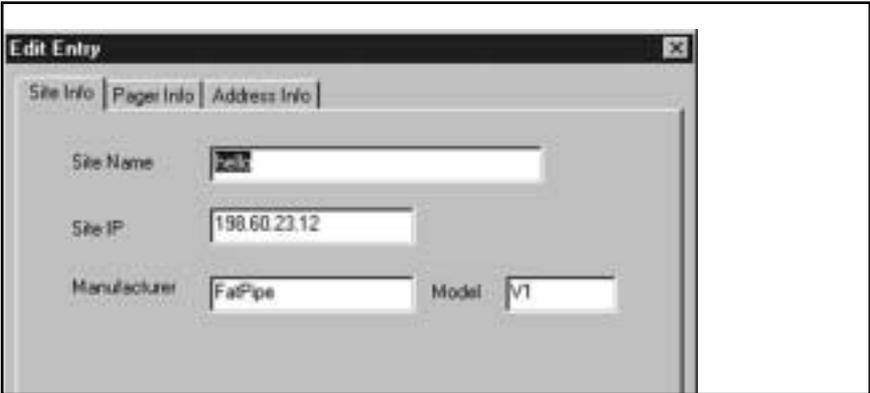
The screenshot shows the same "Add New Entry" dialog box, but with the "Address Info" tab selected. The form contains the following fields:

- User Name:
- Company:
- Street Address:
- City:  State:
- Zip Code:  Country:

Fig. 6.4

## Change Existing Pager Information

To change existing site information in the database, select site and the Enter key on the keyboard. Double-click the entry in the list, or go to Address on the menu and click Edit. This will bring up the dialog box as shown in Figure 6.5. All the fields can be modified in this window.



The screenshot shows a dialog box titled "Edit Entry" with a close button (X) in the top right corner. It has three tabs: "Site Info", "Pager Info", and "Address Info". The "Site Info" tab is selected. The form contains the following fields:

Site Name	<input type="text" value="2012"/>		
Site IP	<input type="text" value="198.60.23.12"/>		
Manufacturer	<input type="text" value="FatPipe"/>	Model	<input type="text" value="V1"/>

Fig. 6.5

Click on Pager Info tab to bring up the window shown in Figure 6.6. You can modify all the fields in this window.

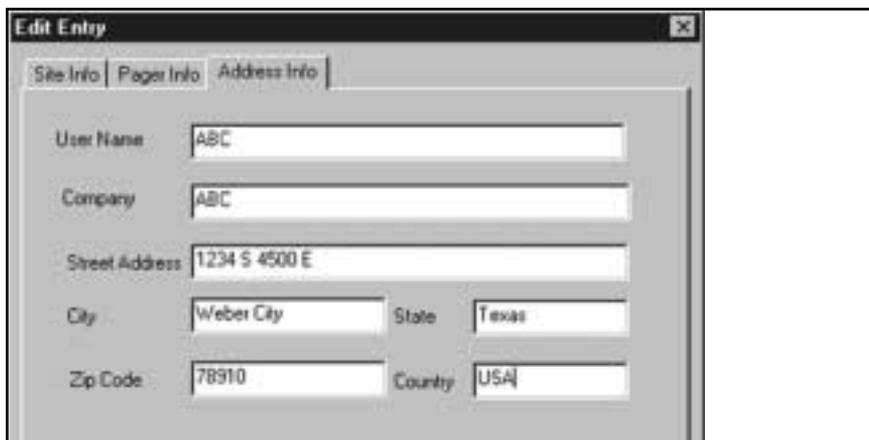


The screenshot shows the same "Edit Entry" dialog box, but with the "Pager Info" tab selected. The form contains the following fields:

Receiver's Email Address1	<input type="text" value="frank@fatpipeinc.com"/>		
Receiver's Email Address2	<input type="text" value="yao@fatpipeinc.com"/>		
Sender's Email Address	<input type="text" value="frank@fatpipeinc.com"/>		
Sender's SMTP Server	<input type="text" value="198.60.23.11"/>		
Area Code	<input type="text" value="123"/>	Pager Number	<input type="text" value="1234567"/>

Fig. 6.6

Click on Address Info tab to bring up the window shown in Figure 6.7. You can modify all the fields in this window.



The screenshot shows a window titled "Edit Entry" with three tabs: "Site Info", "Pager Info", and "Address Info". The "Address Info" tab is selected. The form contains the following fields:

User Name	ABC		
Company	ABC		
Street Address	1234 S 4500 E		
City	Weber City	State	Texas
Zip Code	78910	Country	USA

Fig. 6.7

### Remove Pager Entry

To remove an existing entry from the database, select the entry and press the Delete key on the keyboard. You may also go to Address on the menu and click Delete. It will bring up the dialog box, shown in figure 6.8. Click Yes to delete the entry or click No to cancel the operation.

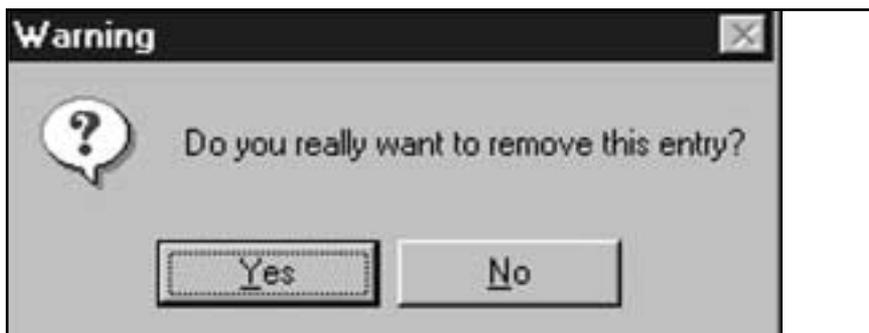


Fig. 6.8

## Chaper 7: Site Failover

WARP units can be configured to automatically failover to one or more remote site units where inbound connectivity to Internet accessible servers is critical. This technology, utilizes Site Failover, and is an optional feature available upon request. Please refer to the back of the manual for general contact information or contact your local FatPipe representative for purchasing information.

### Site Failover Configuration

You can setup two or more standby for Site Failover. You can add as many standby units as you want, although one active unit and one standby unit is a typical scenario for most companies. Once configured, each unit's status will read as either Active, Up, or Down.

A unit in the Down state is a unit configured in the cluster, but is not functioning properly. It cannot come to a Standby state. Down nodes within the cluster are invisible in terms of service provided by the active FatPipe.

Click on Site Failover to access the Site Failover page (See Fig. 7.1). Here you can set parameters to accomplish failover between two or more sites.

Enable Failover

Cluster ID: 103 Port No.: 5003 Show Cluster Status Advanced

Unit List  User Specified Priority Local Unit ID: 1

Unit ID	Unit Name	Priority
1	Unit1	auto
2	Unit2	auto

Add Edit Delete

Channel List

Interface	Destination IPs
WAN1	1.1.1.1
WAN2	2.2.2.2

Add Edit Delete

Fig. 7.1

The Cluster ID is used to denote to which cluster a Unit belongs.

The port number is the port used for communication between units.

Unit List specifies the FatPipe units in the current cluster.

Channel list specifies the IP addresses used for communication between the units in the cluster.

**User Specified Priority:** This setting allows the user to specify a priority level for each unit. Priorities are used to determine which unit will be active or stand-by. If the field is left unchecked, it will default to the auto setting that dynamically chooses unit priority.

Local Unit ID is the number assigned to the current unit.

### Creating or Deleting Unit Entries

The screenshot displays the configuration interface for Site Failover. At the top, there is a checkbox for "Enable Failover" which is checked. Below this, there are input fields for "Cluster ID" (103) and "Port No." (5003), along with "Show Cluster Status" and "Advanced" buttons. The "Unit List" section includes a "User Specified Priority" checkbox (unchecked) and a "Local Unit ID" field (1). Below this is a table with columns "Unit ID", "Unit Name", and "Priority". The table contains two entries: Unit 1 (Unit1, auto) and Unit 2 (Unit2, auto). To the right of the table are "Add", "Edit", and "Delete" buttons. The "Channel List" section below it has a table with columns "Interface" and "Destination IPs". It contains two entries: WAN1 (1.1.1.1) and WAN2 (2.2.2.2). To the right of this table are also "Add", "Edit", and "Delete" buttons.

Enable Failover

Cluster ID: 103 Port No.: 5003

Unit List  User Specified Priority Local Unit ID: 1

Unit ID	Unit Name	Priority
1	Unit1	auto
2	Unit2	auto

Channel List

Interface	Destination IPs
WAN1	1.1.1.1
WAN2	2.2.2.2

Fig. 7.2

Click on the Add button next to the Unit List on the Site Failover page. The Add/Edit Unit page allows you to input specific information about a unit (see Fig. 7.2).

The unit ID must be unique to each FatPipe in the cluster, e.g.: 1, 2, etc.

The Unit name should be something that corresponds to the Unit ID for easy reference.

The Priority field corresponds to the unit in the cluster that is designated as the active unit when the User Specified Priority box is enabled on the main Site Failover page (Fig. 7.1). Lower numbers are assigned the highest priority. Nodes within a cluster should be configured with unique priority values.

### Cluster Status

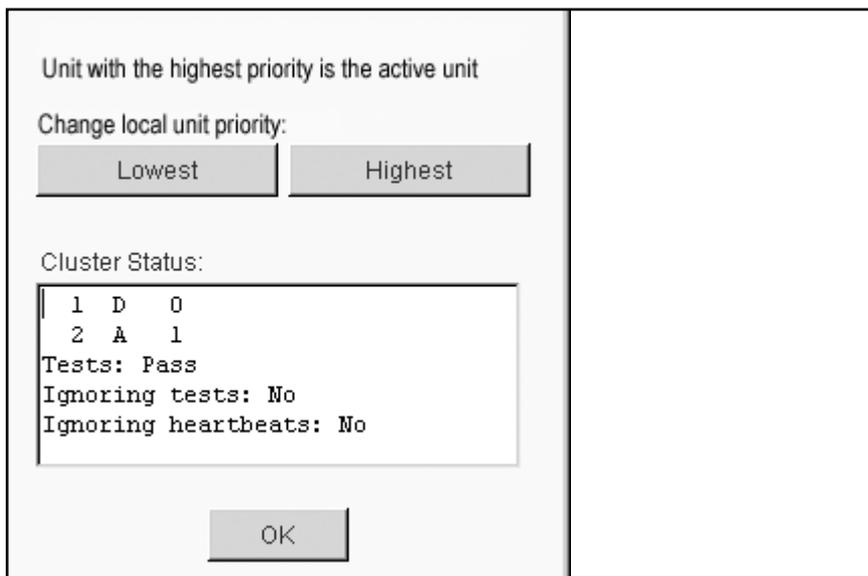


Fig. 7.3

To view the cluster status, click on Show Cluster Status (Fig. 7.3) on the main Site Failover page (see Fig. 7.1). Cluster status indicates the state of the nodes in the cluster.

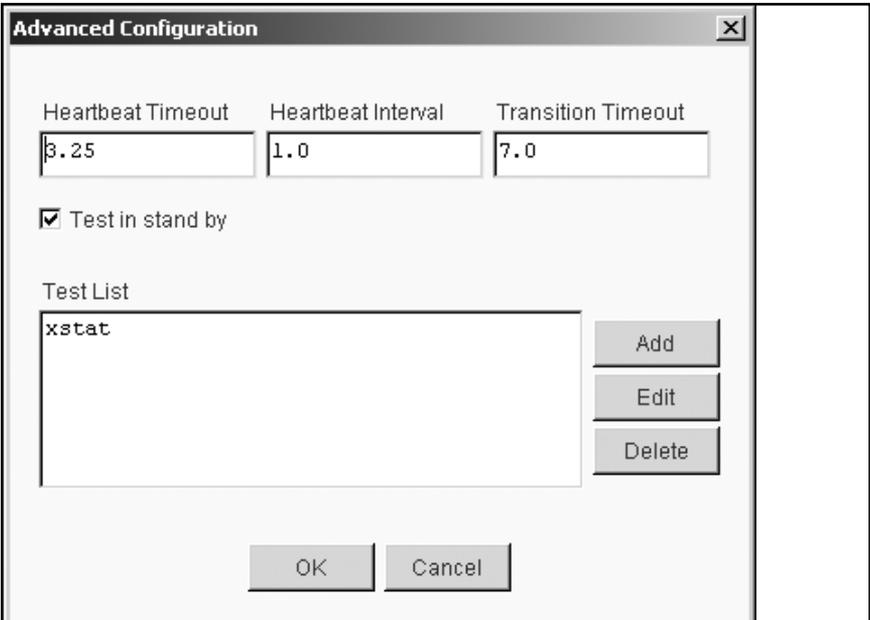
**A** Stands for Active unit and indicates that the active unit is running properly.  
**U** Stands for UP status, and that the Standby Unit is running properly.  
**D** Stands for Down status, and indicates the Unit is not functioning properly

The number designation listed after the cluster status (A, U, or D) shows the priority of the active and standby units.

**Please note:** If User Specified Priority is disabled (this is default), number 1 always denotes the active unit and any number from 2 –100 denotes the standby nodes – numbers are dynamically assigned (see Fig. 7.3).

You can change the status of nodes by clicking on Lowest or Highest under the heading Change local unit priority on the Show Cluster Status page. Changing the local unit priority will alter the status of the unit you are observing. For example, you could choose to force the currently active unit to a Lowest unit priority, which would cause the unit to go into standby mode.

### Advanced Configuration



The screenshot shows a dialog box titled "Advanced Configuration". It features three input fields at the top: "Heartbeat Timeout" (value: 3.25), "Heartbeat Interval" (value: 1.0), and "Transition Timeout" (value: 7.0). Below these is a checked checkbox labeled "Test in stand by". A "Test List" text area contains the text "xstat". To the right of the text area are three buttons: "Add", "Edit", and "Delete". At the bottom of the dialog are "OK" and "Cancel" buttons.

Fig. 7.4

The Advanced Configuration window can be accessed by clicking on the Advanced button on the main configuration page (see Fig. 7.1). You can set time intervals and timeouts between active and standby units, and create a test list to test connectivity.

Heartbeat Timeout is the time parameter to wait for a heartbeat from the other FatPipe before determining that the unit in question has some trouble. Active and standby units send "heartbeats" to each other according to the heartbeat interval set by the administrator, under the Heartbeat Interval field. (See Fig. 7.4).

Transition Timeout creates a delay for testing any of the addresses listed in the Test List on the Advanced Configuration page. The unit changing to active state will ignore any scheduled tests during the transition time. This could be necessary should MAC and IP addresses change as a result of transition, and routers/switches need some time to relearn routes.

**Test List:** Configures the nodes to perform external tests in addition to the test connection between nodes.

The example listed in Figure x.4 shows: `xping 197.60.23.10` is used to check for Internet connectivity. This test can be made more specific by specifying a port number otherwise the test uses ICMP.

Should these tests fail regardless of the other tests, the unit in question will go into a standby state.

There can be multiple tests done so the changing in state of the unit isn't dependant on one test should the user decide to use this parameter.

The following fields are listed in the Add/Edit Channel configuration page (See Fig. X.5 and Fig. 7.6):

**Source Interface:** This drop down menu allows you to choose which interface of the FatPipe unit you are creating the communication channel for.

#### **Add/Edit Channel Configuration for LAN Interface**

**Source IP:** This is the alias IP address that the observed unit has for its LAN interface, which is used for communication with other FatPipe units in the cluster on the LAN side.

**Destination IP:** The Destination IP is the configured alias on the LAN port of another FatPipe in the cluster.

**Source Mask:** This is where the administrator enters the subnet mask of the source IP.

**Source Gateway:** Always configure 0.0.0.0 in the Unit Failover to indicate that there is no gateway to utilize.



## Technical Support

For technical support on FatPipe products, please contact FatPipe Networks directly by calling (800) 724-8521 or (801) 281-3434, Ext. 2237, Monday through Friday, 7:00am to 6:00pm MST. Press number three (3) for Technical Support. You can schedule installations and upgrades outside the normal Technical Support hours with the FatPipe Technical Support team. You may also visit our website for answers to the most Frequently Asked Questions (FAQs). Our website is located at <http://www.fatpipeinc.com>. Send us an e-mail by writing to [support@fatpipeinc.com](mailto:support@fatpipeinc.com).

Contact FatPipe Networks' Technical Support team for more detailed information regarding Support options. FatPipe Networks does not charge for standard Technical Support for the first 90 days from the purchase date and never imposes a charge for current version updates. Feature enhancements and version upgrades are available with a support agreement package.

### **FatPipe Networks**

4455 South 700 East, First Floor  
Salt Lake City, UT 84107

**Telephone:** (800) 724-8521 or (801) 281-3434

**Fax:** (801) 281-0317

**e-Mail:** [support@fatpipeinc.com](mailto:support@fatpipeinc.com)

**Web Page:** <http://www.fatpipeinc.com>

**FatPipe Product Warranty**

©2000 - 2002 FatPipe Networks, Inc. All rights reserved. Patents existing and patents pending in the U.S.A. and elsewhere. FatPipe® is a registered trademark of FatPipe Networks. Windows® is a registered trademark of Microsoft Corporation. All other companies and products names are trademarks of their respective companies. All specifications are subject to change without notice.

FatPipe Networks makes no warranty, either expressed or implied for the hardware enclosed herein UNLESS the Warranty Registration Card which accompanies this product has been filled out and returned to FatPipe Networks. With the return of the Warranty Registration Card, FatPipe Networks warrants its hardware products to the original purchaser against defects in materials and workmanship for one year, as long as the product is used in its original installation.

If you discover a defect, FatPipe Networks will at its option repair, replace or refund the purchase price of the product at no charge to you, provided it is returned during the warranty period. Transportation charges will be prepaid to FatPipe Networks. (You can obtain additional information directly from FatPipe Networks, 4455 South 700 East, First Floor, Salt Lake City UT 84107). For each product returned for warranty service, please attach your name, address, telephone number, a description of the problem and a copy of the bill of sale bearing the appropriate serial numbers as proof of the date of the original retail purchase.

**Returns**

To return the unit to FatPipe Networks for repairs, please contact the Customer Service Department at FatPipe Networks to get a Return Merchandise Authorization Number (RMA # ). You must write this number on the outside of the package where it can be easily seen. No unit will be accepted without an RMA #. For help, call toll free: 800-724-8521 or (801)-281-3434.

The warranty applies only to the hardware products and is not transferable. The warranty does not apply if: (1) the product has been damaged by accident, abuse, misuse or misapplication, or has not been operated in accordance with the procedures described in this and/or accompanying manuals; (2) the product has been altered or repaired by someone other than FatPipe Networks Customer Service personnel; or (3) any serial number has been removed, defaced or in any way altered. FatPipe Networks may use re-manufactured, refurbished or used parts and modules in making warranty repairs.

ALL IMPLIED WARRANTIES, INCLUDING IMPLIED WARRANTIES MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ARE LIMITED IN DURATION TO THE ORIGINAL PURCHASER, USING THE PRODUCT IN ITS ORIGINAL INSTALLATION. THE WARRANTY AND REMEDIES SET FORTH ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHERS, ORAL OR WRITTEN, EXPRESS OR IMPLIED. NO FATPIPE NETWORKS DEALER, AGENT OR EMPLOYEE IS AUTHORIZED TO MAKE ANY MODIFICATION, EXTENSION, OR ADDITION TO THIS WARRANTY. FATPIPE NETWORKS, IS NOT RESPONSIBLE FOR SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM ANY BREACH OF WARRANTY, OR UNDER ANY LEGAL THEORY, INCLUDING LOST PROFITS DOWNTIME, GOODWILL, DAMAGE TO OR REPLACEMENT OF EQUIPMENT AND PROPERTY, ANY COST OF RECOVERING, REPROGRAMMING OR REPRODUCING ANY PROGRAM OR DATA STORED IN OR USED WITH FATPIPE NETWORKS PRODUCTS.

Specific States do not allow the exclusion or limitation of implied warranties liabilities for incidental or consequential damages, so the above limitation or exclusion may not apply to you. This warranty gives you specific legal rights that may vary from State to State.

