ET/BWMGR Appliance User Manual

Getting Started

Unpacking and Setting up the system
Making the Connections

Power Supply Requirements & Plug Locations:

- 1U Case (ET/R1500, ET/R1700i)
- 1U/SM Case (ET/R1500SM, ET/R1700SM, ET/R1750D)
- 1U/SM Mini Case (ET/R1710SM, ET/R1750SM)
- ET/R1800G Case
- ET/R1800GO Case
- 3U Case (ET/R4400 Opteron)
- 4U Case (ET/R4000M)
- ET/D1200 Desktop Unit

Network Connections:

- Connecting a System with Failover Hardware
- Connecting a 2 (or more) Port System without Failover

Booting the System on the Console

Using a Serial Console

Initial System Setup

Using the Setup Script
Connecting to the ET/ADMIN Interface
Permenantly Setting IP Address(es)
Setting the Default Gateway
Setting up DNS
Setting the timezone
Setting the Time and Date

Registering Your ET/BWMGR License Key

Connecting a NAT System

NAT with a Failover Bridge
NAT with a 2-port system (without Failover)
NATd Configuration

Setting up a Web Cache Appliance

Default Settings and Important Notes
Step-by-Step Configuration
Security Notes

Accessing the System From a Network

SSH vs Telnet

Setting up the Hard Drive Backup System

Enabling/Configuring backup
When your main hard drive fails
Initializing a new backup hard drive

Other Configuration Settings

Configuring the Appliance as a Router
Changing the ET/Admin Password
Changing the System Passwords
Notes on the Failover Watchdog Timer
Notes on the Hardware Watchdog
Recovering Lost Passwords
Changing the MySQL password

Other Appliance Functions

Using SSL Encryption with the Graphical Interface
Using the Apache HTTP Server with the ET/ADMIN
Apache Redirects
Using Public Graphs
Setting up an extern mySQL Database
Enabling and disabling snmpd (and other services)
Checking System Processes
Rebooting the System
Configuring WAN Interfaces

Post-Configuration Security

System Updates

Updating Your System Over the Internet
Update Subscription Notes
Reverting to the previous version

Routine Maintenance

Monitoring System Status
Backup & Restore Overview
Backing up
Restoring from Backup
Maintaining the Statistics Database - Purging Old Data
Repairing a Broken Database
Using the Recover CD-ROM

Getting Support

Troubleshooting

Getting Started

Unpacking and Setting up the system

When you unpack your system you should see a ziplock bag which contains at least a power cord and some screws. Rackmount systems can be set up as a desktop unit or as a rackmount. Rackmount ears are already installed on rackmountable units when shipped. If your unit has a lockable front panel, the keys should also be included in the bag.

Making the Connections

This section describes each of the appliances available. Make sure you read the entire hardware section carefully before attempting to put your system online.

Power Supply Requirements & Plug Locations:

The power supply requirements and location of connectors are directly related to which enclosure you have ordered. Make sure you read the appropriate section for your case, as plugging in the unit before selecting the proper voltage can easily (and instantly) ruin your power supply. All of the cases have an ATX-style connector with keyboard, mouse, VGA, and at least one serial port in a group, usually coded by color. (VGA=blue, keyboard=purple, COM1 serial=green). For the location of network connections and power supply notes, please read the section below for your case.

1U Case (ET/R1500, ET/R1700i):

The 1U cases contains an auto-switching power supply that can accept both 115v and 230v AC input. The only switch on the power supply is an on/off switch. On the front panel there are two thumb-screws which can be used to release the front panel and access the power switch, reset switch, and floppy disk drive. Turn the thumbscrews counter-clockwise until they are free, and then swing the front panel down. On the back of the case, to the right of the ATX cluster, you will see two network connections (fxp0/fxp1 in FreeBSD, or eth0/eth1 in Linux). Ordering is from left to right. Additional ports may be located in the card slot to the right of the case, depending on options. If you have purchased an ET/R1X00-FO with the hardware failover, the failover ports (fxp2/fxp3, or eth2/eth3) will be in the card slot (again, ordered from left to right).

1U/SM Cases: (ET/R1500SM, ET/R1700SM, ET/R1750D)

The SuperMicro 1U case contains an auto-switching power supply that can accept both 115v and 230v AC input. Viewing the front panel, you will see the CD-ROM and floppy drives on your left, and the power and reset buttons on the right, next to the indicator lights. The primary ethernet ports are located immediately to the right of the ATX cluster, and are labelled port 1 and 2. If your appliance has hardware bypass/failover the 2 failover ports are located in the card slot. Also note that in the box you should find sliding rails for mounting this unit on racks, if needed.

1U/SM Mini Cases : (ET/R1710SM, ET/R1750SM)

The 1U mini cases have an auto-switching power supply that can accept both 115v and 230v AC input. The layout is the same for both the ET/R1710SM and the ET/R1750SM. Viewing the front panel, you will see the CD-ROM and floppy drives on the left, and the powr button on the right, next to the indicator lights. The 1U mini cases are much smaller and lighter than our other appliances, and do not ship with the sliding rail attachments. These appliances ship standard with the FreeBSD OS installed.

ET/R1710SM

Viewing the rear of the case, the primary and secondary ethernet ports (em0 and em1) are located immediately to the right of the ATX cluster, and are labelled LAN1 and LAN2. If your appliance has hardware bypass/failover, the 2 failover ports (fxp0 and fxp1) will be located in the card slot on the right.

ET/R1750SM, ET/R1750D

Viewing the rear of the case, the primary and secondary ethernet ports (bge0 and bge1) are located immediately to the right of the

ATX cluster, and are labelled LAN1 and LAN2. The failover ports (em0 and em1) are located in the card slot on the right.

Notes on the ET/R1800G:

The ET/R1800G case contains an auto-switching power supply that can accept both 115v and 230v AC input. Viewing the front panel, you will see the CD-ROM and floppy drives on your left, and the power and reset buttons on the right, next to the indicator lights. Viewing the rear of the case, the primary ethernet ports are located immediately to the right of the ATX cluster, and are labelled "LAN1" and "LAN2". These ports are identified as em0 and em1. The failover ports are located in the card slot and are ordered from right to left (em2 and em3). The ET/R1800G ships with only the FreeBSD Operating System installed. Also note that there is a separate on/off switch for the power supply, located just to the right of the AC input.

Notes on the ET/R1800GO:

The ET/R1800GO case contains an auto-switching power supply that can accept both 115v and 230v AC input. Viewing the front panel, you will see the CD-ROM and floppy drives on the left, and the two SATA drive bays on the right. The power and reset buttons are located above the drive bays, along with the indicator lights. Viewing the rear of the case, the primary ethernet ports are as follows: (left to right) fxp0 , bge1 and bge0, and the failover ports em1 and em0. By default, fxp0 is used as the administrative port, and em0 and em1 are used as the two-port bridge. bge0 and bge1 are left unused, but can be used as a non-failover bridge or as regular ethernet ports.

3U Case (ET/R4400 Opteron):

The redundant power supply in the 3U case automatically switches between 115v and 230v AC input. Each power supply module has a green light indicating that the module is receiving and providing power properly. If one of these modu les should fail, an alarm will sound, and the light will indicate which unit has failed. The modules can be hot-swapped, and replaced while the unit is running. The alarm can be cancelled by pushing the small button at the top of the module bay. On the front of the case, you will see two bays with doors. These bay doors share the lockable knob in the center of the case. The right-hand bay holds the CD-ROM drive, as well as the power and reset switches, while the left-hand bay holds the floppy drive. Viewing the rear of the case, the primary ethernet ports are as follows: (left to right) fxp0 , bge1 and bge0. Any cards ordered with the appliance will be located in the card slots to the right. Assuming you have purchased two ET/GigFailover cards, they will be ordered (from left to right, top to bottom) em2, em3, and em0, em1. By default, fxp0 is used as the administrative port, and the em devices are used as bridge ports. bge0 and bge1 are left unused, but can be used as a non-failover bridge or as regular ethernet ports.

4U Case (ET/R4000M):

The power supply in the non-redundant 4U case is NOT automatically switched. You must select the proper input voltage before plugging in this unit. The power supply is located in the rear of the case. There should be a small red switch with two positions. Make sure the switch reads the proper voltage before connecting.
If you have the redundant power supply, then the voltage is automatically switched by the power supply. Each power supply module has a green light indicating that the module is receiving and providing power properly. If one of these modules should fail, an alarm will sound, and the lights will indicate which unit has failed. The modules can be hot-swapped, and replaced while the unit is running.
The front panel of the 4U case is hinged at the bottom. The lockable knob at the top can be turned clockwise to open the panel. Behind the panel you will find the floppy drive, CD-ROM drive, power switch, reset switch, and the power and HDD activity lights. On the rear of the unit, you will find the ATX cluster in the middle. Immediately to the right of the video output is the primary ethernet port em0. The card slots to the right will hold additional ports, depending on the configuration you have ordered.

ET/D1200 Desktop Unit (discontinued)

The ET/D1200 is a compact desktop chassis, with a power supply that is NOT automatically switched. You **must** select the proper input voltage before plugging in this unit. The power supply is located in the back of the case, on the left side. You will see a small red switch with two positions: 115 and 230. Select the voltage appropriate for your outlets before plugging in the unit.

Viewing the front panel, you will see the CD-ROM drive (optional) on your right, and the floppy drive on your left. Underneath the CD-ROM drive is the power switch and indicator lights. On the rear of the case, from left to right, are the AC input, COM1 serial port (blue), and then the ATX cluster. The ATX cluster includes mouse, keyboard, VGA, and the primary ethernet (fxp0, located just above the USB ports, which are not active). Above the ATX cluster are the expansion card slots where you will find the secondary ethernet port (fxp1), or the optional failover ports fxp1 and fxp2. The D1200 is available only with the FreeBSD Operating System.

Network Connections:

Once you have read the above section, you should be aware of how many ports are on your machine and their names. The sections below refer generally to ports 0, 1 (2, 3.. etc). The method for connecting each system is generic, you simply need to correlate the interface name to the port number. You also need to be aware that any bridged ports on the bandwidth manager act like a 2 (or more) port hub, and therefore care must be taken not to plug any two bridged ports into the same network. Plugging two bridged ports into the same switch or hub will most likely bring down both your network segment and your bandwidth manager. If the machine is running while this happens and the console is connected, you will see LOOP messages if this condition occurs. Note on the use of crossover cables: If you are connecting the system directly to another router or server, you can use a crossover cable instead of plugging both units into a hub or switch (you CANNOT connect the system directly to a router or server with a regular ethernet cable). However, be aware that some devices do not "negotiate" the link speed and duplex correctly, so you may have to force one or both of the devices into the correct setting. If you see sluggish system performance or the unit won't pass data, see the troubleshooting section for more info.

Connecting a System with Failover Hardware:

Units equipped with the hardware Failover option will have 3 or more ethernet connectors. Port 0 is the administrative port. This port is assigned an IP address for remote configuration, and is NOT configured as a bridge. Note that if you have a cache system the setup procedure is different, and is described in a separate section below.

3 port system: Port 0 = administrative, Port 1 = failover port 1, Port 2 = failover port 2
4 port system: Port 0 = administrative, Port 1 = unused, Port 2= failover port 1, Port 3 = failover port 2

On 4 port systems, port 1 is located immediately to the right of port 0, but is not used. Three port systems use ports 1 and 2 as the "failover" ports as described above.

Failover port 1 should be connected to your internal network (the same hub or switch as your administrative port), while failover port 2 should be connected to your upstream provider (usually via a router). Both of these failover ports are bridged, in bridge group 1. You can plug the administrative port into the same network as failover port 1 or 2, but failover port 1 and 2 MUST be on physically separate networks or you will create a LOOP.

By default, the failover ports are physically connected together, also known as the "closed" state. In this state, the two ethernet ports are connected as if they were one wire. This means traffic will flow across the ports, even when the machine is powered off. In fact, that is the easiest way to test your unit - place the unit in between two switches, or plug an individual computer via a crossover into one of the bridged ports and try to access a remote host. Even with the unit powered down, the warning about plugging both ports into the same network applies. In this case it won't affect the machine, but can adversely affect your network for the duration.

Once the machine is powered up and the ET/BWMGR is running, the software watchdog routine will "open" the failover ports. If you are close to the unit, you may hear a "click" as the ports open. When the ports are opened, the ET/BWMGR bridge will pass traffic from one interface to the other. When the failover ports are in the "closed" state traffic should pass as if there is a single wire and the machine is not present. Once you determine that you are passing traffic correctly and the machine is bridging, you can start creating some rules.

Connecting a 2 (or more) Port System without a Failover card:

Note: If you are using NAT, please follow the instructions in the NAT section and not this section.

If you have a 2-port machine without the hardware failover option, such as the ET/R1710SM, you should have a default configuration in which port 0 is assigned an IP address, and is the primary port for bridge group 1. Port 1 must also be assigned to bridge group one, and must not be set to primary. The machine in the default configuration acts just like a 2 port switch. As a test, you should plug port 0 into your network, and port 1 via a hub or switch to your upstream network. Or, you can plug an individual computer into one of the ports via a crossover cable. Once you have determined that you are passing packets through the bridged ports and are not looping, then you can start creating and testing rules.

If you have more than 2 ports and want to create a large bridge group, you just need to assign all of the other ports (other than the primary) to be in bridge group 1. So if you have a 4 port card, assign ports fxp1 through fxp4 to bridge group 1. The appliance will then act like a 5 port switch.

Booting the System on the Console

The ET/R1700 (SM) systems (now discontinued) are shipped dual boot so that you can either run FreeBSD or LINUX, your choice. The system default is FreeBSD, so if you want to run LINUX you will have to first boot the system with a monitor and keyboard attached to override the default. If you don't have strong preconceptions about LINUX, we recommend that you use FreeBSD. All other appliances are shipped with FreeBSD only, and you will not see the boot menu.

When the system first boots, you should see a screen such as the following:

F1: FreeBSD
F2: Linux

Pressing F1 will boot FreeBSD,and pressing F2 will boot LINUX. Once you make a choice, that becomes the default system boot for subsequent boot-ups. So, once you chose an OS and set up the network, you won't have to put a monitor and keyboard on the system again unless you want to change to a different OS. As mentioned above, those using Web Cache or Gigabit systems should not change the boot default from FreeBSD.

Your system should boot to a login prompt. Log in with the user name "root" and the default passwd "saturn5". You should then see a shell prompt similar to the following:

ET/R1710#

Using A Serial Console

A serial console is available on all ET/R series units. The 9 pin serial connector on the back of the machine unit is a DTE serial port and can be connected to a terminal with a null modem cable. Default configuration of the port is 9600 baud, 8 bits, No parity, and 1 stop bit. The port is located towards the center of the rear of the unit, and is usually green in color if the plugs are color-coded.

The following describes the default boot behavior in FreeBSD and LINUX. Note that console (without the word "serial") implies using the monitor and keyboard.

FreeBSD:
The default behavior is to send the boot messages to both the console and the serial console. Once a kernel has been selected (either by hitting enter, selecting an alternate kernel, or waiting a few seconds), then the kernel messages are printed on the console. If you do not have a monitor or are working from the serial console and wish to see the kernel messages, type

boot: -h <enter>

this will change the default to the serial console for this boot only, and continue with the boot process. If you find yourself using the serial console more than you do the regular console, you may change the default by editing the file /boot.config . Options are as follows:

-D This is the default. Dual boot, meaning the boot loader prompt is sent to both consoles. Boot messages are displayed on the monitor unless overridden by input at boot time (this can be done at either the keyboard attached to the system, or via the serial console, and affects only the current boot).

-h -D Change the default console to be serial. Boot messages are now displayed by default on the serial console and not the console. This can be temporarily overridden by typing -h <enter> at the boot prompt. The -h option is a toggle, so in this case selecting it twice (once in /boot.config, once again at the boot prompt), is the same as simply using the -D option in the /boot.config file.

-h This will also change the default console to be serial, but also has the effect of not displaying the boot prompt on the regular console (meaning there is no way to override this setting from the regular console.) It is recommended that you leave the -D setting unless using -P as shown below.

-P This will automatically change the default console by detecting whether or not you have a keyboard attached to the machine. If a keyboard is present, a normal console boot is peformed. If no keyboard is present, the boot switches to the serial console.

Once the system is up and running, you will get a login prompt on the serial console, regardless of any settings changed above.

NOTE: If you wish to use a serial console and boot into single user mode, you must set either the -h -D or the -h option, or set -P and make sure there is no keyboard attached to the unit. Otherwise, selecting single user mode will bring up the shell prompt

using the monitor and keyboard.

LINUX:

In LINUX you will see the LILO prompt on both the console (monitor) and serial console. You may select an alternate kernel to load at this prompt. Boot messages are displayed on the serial console via syslog. As such, there will be no messages until syslog is started a bit later in the boot process. However, all messages from the current boot will be displayed on the serial console once syslog starts. Boot messages are always displayed on the monitor as well. Once the system is up and multiuser is active, you will get a login prompt on the serial console. You may select single user mode (-s) on either console, but the shell prompt will be displayed on the monitor only. This implies that you must use a monitor and keyboard to do emergency maintenance if you are using LINUX.

Initial System Setup

In order for your system to function properly on your network you will need to do some basic set up so that you can properly access, start and register your license key. At a minimum, you must set up the IP address, DNS client information, and a default gateway before registration.

Using the Setup Script:

Next you will have to configure your ethernet address, default router and DNS server information. If you are setting up the box as a router, then both of your ethernet adapters will probably have addresses. If you are setting up a bridge, then only one should be given an address. On a system with failover hardware, your first port (fxp0 or eth0) must be assigned the address. To fully realize the benefits of the failover hardware, you must use a bridged configuration.

The simplest way to do initial IP configuration is to run the "etip" command after logging in as root. This will prompt you for the interface (enter fxp0 or eth0), IP address, netmask, default gateway, and DNS server IP address. The settings made will be immediately applied to the system configuration, and also saved so that they will take effect on subsequent boots. The example below shows the usage of "etip". Commands typed by the user are shown in italics.

etip

Which interface would you like to assign an IP address? Select from the following list of detected interfaces. fxp0 fxp1 fxp2 fxp3
Interface: *fxp0*
Please enter the IP address for fxp0: *a.b.c.d*
Enter your netmask (or hit enter for default of 255.255.255.0):
Enter your default gateway: a.b.c.d? *a.b.c.d*
Enter your primary DNS server (or hit enter to skip): *y.y.y.y*

Using the following values for interface fxp0:
IP Address: a.b.c.d, Netmask x.x.x.x
Default Gateway: a.b.c.?
Primary DNS Server: y.y.y.y

OK to use these settings? (y/n) *y*

Answering "y" will apply and save the changes. You can now access the machine remotely.

Assuming that all went well with the etip script, your next step should be to connect to the ET/Admin GUI interface.

Connecting to the ET/ADMIN Interface:

Once you have assigned the ethernet address, you should be able to access the graphical administration interface (ET/ADMIN), which is running on port 10000. Use your favorite web browser to access the following URL:

http://a.b.c.d:10000

Where a.b.c.d is the address that you assigned the system. You will be prompted for a username and password. The default username is "admin" and the password is "saturn5". (see "Changing the ET/ADMIN password"). Once you have setup up the address and can connect to the ET/Admin GUI, you can skip the "manual system setup" section, but do take a look at the "setting

the time zone" section below:

The following indented section is for reference only, in case you need to fix something manually.

Manual System Setup:

If you need to manually set up your system, the following section describes the steps required to make your initial settings and store them so they will be activated whenever your system is restarted. If you have used the etip setup script then you should skip to the section titled "Setting The Time Zone".

Log in as root, and run the following command (where a.b.c.d is the IP address you wish to assign the bandwidth manager, and x.x.x.x is the netmask). You should replace the interface name with whatever port 0 is on your machine, if necessary.

For FreeBSD:

ifconfig fxp0 a.b.c.d netmask x.x.x.x

For LINUX:

ifconfig eth0 a.b.c.d netmask x.x.x.x

After doing this, your machine should be accessable from the network with the address you specified. Note that the address you give the system must be an address that is accessable locally on the wire that you have attached to the first ethernet port.
Also note that using "ifconfig" to set/change IP addresses is a temporary change and will not be saved if the machine is rebooted. See the section on connecting to the ET/ADMIN interface and permanently setting IP addresses below.

Permanently Setting the IP Address

If you have just set up your system for the first time, you must now use the adminstration tools to permanently change the IP of your bandwidth manager. If you have an machine that's already in use, this is the correct method to change/add IP addresses as well. To tell the system to set the IP address you've assigned at each reboot, click on the Network tab from the left-hand menu and then select the Network Configuration link. This will bring up some additional icons:

Select -> Network Interfaces:

Within the table below Interfaces Activated at Boot Time , click on port 0, which will bring up a screen with information about this interface. Set your IP address to a.b.c.d (make sure the button next to the text box is selected) and verify IP and netmask settings. Make sure "Activate at boot?" is 'Yes', then click on save and apply . Make certain that you modify the interface on the bottom section of the page (under the "Interfaces Activated at Boot Time" label), as these changes are carried over to future boots. Changes made from the "Active Interfaces" table will only be temporary. Note that if you are planning to use the appliance as a router, you will want to assign an IP address to each interface that will be active. To return to the menu, Click on <- Return to Network Configuration at the bottom of the page.

Setting the Default Gateway:

Next you need to set the default gateway for the system if you want the machine to be able to access outside networks. If you DON'T want the machine to be accessable or to have access to the internet, skip this step. Note that in order to register the BWMGR software or use the web update facility you will have to be able to access the internet. To set the default gateway:

Select->Routing and Gateways:

Select the button next to the text box and enter the IP address of your default router, Note that the address must be accessable (typically on the same network as your IP address and network mask entered previously). Click save to save the settings. To return to the Network Configuration menu, click <- Return to Network Configuration.

Setting up DNS:

In order to access the bandwidth manager by name, or to be able to access other systems by name (required for the web update procedure), you must set up your DNS (Domain Name Service) client. You will also be able to set the hostname of this machine. From the menu:

Select-> DNS Client:

Set the hostname of this machine, and add your namerserver(s) IP address(es) in the DNS Servers box. Click save .

If you don't have a real DNS entry in your server for this system, you can use the "Host Addresses" table to alias names with IP addresses. The host address table will also be looked at before DNS is attempted, so it is a bit faster. Its also useful for aliases that are not real DNS entries. For example, if you wanted to access a machine at 211.14.18.12 with the name "MySunWorkstation", you could add an entry in the host addresses table as such and that name would be translated to the correct address.

Setting the Time Zone:

Making sure the time is correct is fairly important for users who are interested in storing statistics for rules. There are different utilities for selecting the proper time zone depending on which Operating System you are using. For either OS, you must log in to the console as "root" and run the correct program. For FreeBSD, use 'tzsetup'. This will bring up a series of text dialog boxes, which can be navigated by the arrow keys. For Linux, use 'tzselect'. Both programs are fairly self-explanatory and require that you choose the proper geographic area to narrow down the selection list. After confirming the time zone is correct for your location, check the time and adjust it if necessary.

Setting the Time and Date:

Click on the "System" tab from the main ET/Admin menu, then select the "System Time" link. You will see several fields where you can select the current Date, Month, Year, Hour, Minute, and even seconds. Make sure the date and time are current and click the "Apply" button to change the system time.

You are now finished with the basic configuration of the bandwidth manager. You may now want to read the section regarding using SSL encryption with the ET/ADMIN interface, as well as the section on enabling Apache and Apache redirects.

Configuring a NAT System

NAT (Network Address Translation) allows a private network connected to the appliance to share the public IP address assigned to the administrative interface. NAT is only supported on appliances with the FreeBSD Operating System.

NAT with a Failover Bridge:

Failover appliances should have 4 ports. Depending on your appliance, the port names will be:

fxp0, fxp1, fxp2, and fxp3 (ET/R1700SM-BW-FO)
em0, em1, em2, and em3 (ET/R1750SM, ET/R1800G, ET/R1710-SM with the Failover option.)

Port 0 is your administrative port.
Port 1 is the NAT port.

Before setting up NAT, you should first configure and connect your appliance as detailed in Initial System Setup. Configure your administrative port with an IP address (which is also referred to here as the "public" address) and connect your failover ports. Once you have the appliance connected and have tested that bridging works, then continue with the NAT configuration.

Connect to the ET/Admin GUI, and Assign the private IP address and netmask to port 1. (eg, 10.0.1.1)

Configure your test machine with an address on the private network (eg, 10.0.1.30, with default gateway 10.0.1.1). Make sure that the test machine can ping 10.0.1.1. At this point, the appliance should be able to access external networks, but not the test machine.

Start NATd:

sh /etc/rc.natd

Once NATd is started, you should confirm that the test machine can now access external networks. If necessary during testing, the correct way to stop NATd is:

sh /etc/rc.natd stop

Once you have verified that NAT is working, you can enable it at boot time. From the main ET/Admin menu, select the "System Functions" link on the left side, then select "Boot Startup Tasks" below it. Find the line that starts NATd, and uncomment it by removing the "#" character from the start of the line, then clicking "Save" at the bottom of the screen.

Failover Notes:

Ports 2 and 3 are your bridged failover ports, and do not need IP addresses. Do not change the default bridge configuration. NAT will co-exist with your bridge, and will continue to operate even if the appliance is put into manual bypass mode; however, if the machine goes down or is powered off, the private network will be isolated.

NAT with a 2-port system (without Failover):

The first step is to configure the IP addresses. The primary address on em0 should be set first, using the 'etip' command as outlined in Initial System Setup. The default gateway, netmask, and primary DNS server are also configured at this time. Also see the Registration section, as you will need to enter your licens e key to start the ET/BWMGR software if you haven't already.

Connect to the ET/Admin GUI, and disable bridging on em0 and em1.

Assign the private IP address to em1. (eg, 10.0.1.1). You must use the ET/Admin GUI to assign this address, not 'etip'. At this point, you should be able to reach external networks directly from the appliance, and our test machine (with IP 10.0.1.30 and default gateway of 10.0.1.1) should only be able to reach its default gateway address.

Start NATd:

sh /etc/rc.natd

Once NATd is started, you should confirm that the test machine can now access external networks. If necessary during testing, the correct way to stop NATd is:

sh /etc/rc.natd stop

Once you have verified that NAT is working, you can enable it at boot time. From the main ET/Admin menu, select the "System Functions" link on the left side, then select "Boot Startup Tasks" below it. Find the line that starts NATd, and uncomment it by removing the "#" character from the start of the line, then clicking "Save" at the bottom of the screen.

NATd configuration:

The configuration for NATd is stored in "/etc/natd.conf". The basic configuration consists of two options, and can likely be used as-is.
interface defines the ethernet port with the public address.
unregistered_only will restrict NAT to only allowing private, unroutable addresses to be translated. This is enabled by default.
If you wish to use a more advanced configuration, please read the man page for 'natd'. As usual, we recommend testing with the default setup before changing anything.

Transparent Web Cache (Squid) FreeBSD ONLY

The following documentation applies only to units sold with the web cache hardware option. For a variety of support and performance reasons, the cache should only be used with the FreeBSD operating system, even though your system may have LINUX capability. The default configuration is a transparent proxy. All web traffic requests from your internal network will be transparently cached.

Default Configuration: (NOTE: This is new in v3.23)

Systems shipped with the cache option have the cache disabled by default. The cache option can make it difficult to debug a basic setup problem, so we recommend that you first get the system running without the cache, so that you are sure that you have it wired correctly, and that your basic shaping rules work properly. Once you have familiarized yourself with the system, you can enable the web cache and make any adjustments to your ruleset.

Step by Step Configuration:

1: Verify the Wiring

Make sure you have the correct bridge configuration. The cache system should ship from the factory with the correct setup, but we list them here as customers often change the defaults during testing. Make sure that the interface marked "(Inside)" is connected to your internal network.

ET/R1700SM-BW-FO-Cache:

fxp0: Bridge Group 1, Fallback enabled
fxp2: Bridge Group 1, Set as Primary (IP address) (Inside)
fxp3: Bridge Group 1

ET/R1710SM:

em0: Bridge Group 1, Primary (IP address)
em1: Bridge Group 1 (Inside)

ET/D1200

fxp0: Bridge Group 1, Primary (IP address)
fxp1: Bridge Group 1 (Inside)

ET/D1200 with optional Failover hardware

fxp0: Bridge Group 1, Fallback enabled
fxp1: Bridge Group 1, Set as Primary (IP address) (Inside)
fxp2: Bridge Group 1

2: Check your rules

Starting the cache will add a firewall rule to your ET/BWMGR ruleset on the inside bridge interface. Leave firewall indices 100-200 open for cache use. If you already have rules in this index range in the firewall, please move them before starting the cache.

3: Start the cache

Find the "Squid Proxy Server" module in the "Servers" section of the ET/Admin GUI. Once you have opened the module, you will see a link at the top right of the screen "Start Squid". Click on "Start Squid". After a few seconds the page will reload and you should now see "Apply Changes" and "Stop Squid". This indicates that the cache has started.

NOTE Stopping/Starting Squid from the GUI will also change whether the cache is started at boot time.

3: Test the cache

Connect to an external web site from a browser connected to the inside bridge interface. Generally, if you have started the cache and you can reach external web sites, the cache is working. Look for hits on firewall rule #150 on your inside interface. You can also use the Cache Manager link in the Squid module to check that you are caching web requests. Click on "Cache Manager Statistics" and login as user "Manager", default password of "saturn5". Click on "General Runtime Information" or "Cache Utilization" and see if you are getting cache hits.

For more information on the many functions available in Squid, visit the Squid web site: http://www.squid-cache.org , where you will find manuals and examples. The "Help" link at the top of the ET/Admin Squid GUI also goes to this page.

4: Security and Advanced Usage

The default configuration of the web cache is to transparently cache ALL http requests from your internal network, while disallowing direct access to the cache (to prevent unauthorized outside usage of your cache).

In some situations, you may want to limit the cache usage to individual users or specific subnets. If you wish to exclude a subnet or IP address range from being cached, simply add a firewall allow rule with an index < 100 that matches http requests from the IPs in question. You can also use the Squid ACL (if you are familiar with the syntax) to exclude certain clients or URLs from being cached.

If you need to modify the default rule, or need additional rules to control who gets cached, this MUST be done by editing files in "/usr/local/squid/etc". "cache.config" defines the inside interface, where all your cache rules must be applied. "cachestart" and "cachestop" control the adding and removing of rules when the cache is started and stopped. There are instructions within these files on where to add or modify rules. Use existing rules as examples. Changes made to the rule in the ET/Admin BWMGR GUI will be lost after the next reboot, unless you also change cachestart. Note that if you add any rules to cachestart, you should also add a line to remove that rule in cachestop, otherwise they will not be removed if you stop the cache.

Also note that if you are allowing your customers to view their usage graphs, you will likely want to edit cachestart to avoid caching these requests. Find the line that reads:

#/sbin/ipfw -q add 2500 pass tcp from any to MY.IP.ADDR.HERE 80 in

Change "MY.IP.ADDR.HERE" to be the IP address you are using for customer graph access. Remove the "#" symbol. Then save the file. Changes to /etc/rc.cache will be applied at the next boot, or you can apply them immediately by clicking "Stop Squid" then "Start Squid" in the ET/Admin GUI.

Registering Your ET/BWMGR License Key

Appliances ship with a demo key installed. You must install the license key issued to the appliance, as the demo is time-limited. When an appliance is shipped, a license key is generated and sent by email to the contact on the purchase order. Additionally, the license key should also be printed on your invoice. You can also find a listing of all of your current license keys by logging into your account on our web site. If you have multiple licenses or appliances, you can view all your keys, and match the serial number of the license to the serial number of the primary ethernet interface on your appliance.
Initially, you should start the ET/BWMGR with your license key to ensure that it works, this will also eliminate the demo time limit. Once you have the unit installed in the final location, you should then register your license. **Registration is required** in order to access the update server, whether you have the included 30 days of support and updates, or you have purchased the 1-year subscription. If you have the free 30-day subscription, you should make sure to check for any updates or bug fixes that have been added since your system was built before the subscription expires. You can see the expiration date of your keys when viewing them in your account on the ET web site.

When you access the ET/Admin GUI, you will see the main ET/BWMGR configuration on the right side of the screen. If not, click on Bandwidth Manager on the left hand side on the top of the menu. Click on the "Setup BWMGR" button. Make sure your primary interface is selected as the "key interface" (either fxp0 or em0). To double check, display the pull down menu for "Key Interface" and match the serial# in your email with the code shown next to each interface. The serial number must match in order for the key to work. Select the proper interface, and then paste or type your license key into the "Key" field. Click the "Start ET/BWMGR" button. The system should start successfully. Now return to the Startup Menu.

To register your system, you will have to have access to the outside world, which means that at least your default gateway will have to be configured and any firewalls will have to be disabled for ports 4000 to 5000. You must also have a working DNS setup. If you get a "server down" message, it's possible that the server really is down, but more likely the problem is that you can't reach the server for some reason, so check your connectivity to www.etinc.com. This can be done by going to the main "Update System" screen, and then clicking on "Check Versions", which will attempt to connect to etinc.com and will display a reasonably verbose explanation of any errors encountered. See the BWMGR FAQ for more information. To register your system, Click the "Register ET/BWMGR" button.

Connecting to the System from a Network

Once you complete the initial configuration, most configuration tasks can be done via the HTML interface. If you need to get into the command line interface, you can access the console remotely via either Telnet or SSH.

Telnet vs SSH:

Both Telnet and SSH require the use of a program on the client end to connect. There is a Telnet client included as part of most Windows installations. For security reasons, you cannot log in directly as "root" when you access the console remotely. When connecting with Telnet or SSH, you will have to first log in as the "admin" user. Once logged in, you can use the "su" command to become the super-user (root) to perform administration tasks or use the ET/BWMGR tools:

su -

Telnet is a plain-text protocol while SSH encrypts all communications between the client and the server, including password authentications. This is intended to prevent password sniffing. SSH also provides host authentication via a host key, which is stored by the client the first time it connects to a server, and verified at the beginning of each connection. If the host key changes for any reason, SSH will warn the user and refuse to connect unless they take manual action. This reduces the possibility of someone hijacking an IP address and attempting to steal passwords. Telnet and SSH are configured and accessable on the unit by default. It is recommended, especially if you or your staff may be accessing the system from outside your local network, that you use an SSH client to connect.

Different clients may have different interfaces (particularly from a Windows Box), but from a standard unix system you can access the system remotely via telnet with the command:

telnet a.b.c.d

where a.b.c.d is the address to use. If successful, you should see a login prompt. Again, you cannot log in as "root" when accessing the system from a network (via Telnet or SSH). so you should log in using "admin" with the appropriate password ("saturn5" by default). Then you can use the "su" program to change to super-user ("root" is super-user by default) as follows:

$su - <Enter>
password: saturn5
ET/R1710#

Don't forget the "-" option, which allows you to inherit the root user's paths, so the system and BWMGR programs can be run without using full pathnames.

To access the system via ssh, enter a command similar to the following:

ssh -l admin

where the -l option indicates that you want to log in using the user name "admin".

Setting up the Hard Drive Backup System

On appliances with two externally-accessable drive bays, the second drive (if not used as the cache disk on supported appliances) can be used for the spare disk. Looking at the front of the case, the main disk is always installed in the left-hand drive bay, and the spare disk in the right. Note that on newly- purchased appliances with the spare disk option, you must enable the scheduled task that backs up the contents of the main disk to the spare disk. Once you have enabled the backup, you can check the status of the backups by viewing the log file "/var/log/backup_appliance".

Enabling/Configuring the Hard Drive Backup

Select "System Functions" and then click on "Scheduled Commands". You will see a table with the list of commands and the status for each. Look for the command "/usr/local/bin/backup_apliance". To change the status or configure the time(s) at which the backup occurs, click on the command name.
At the "Edit Cron Job" menu, you can turn the backup on or off by clicking "Yes" or "No" at the top. In the "When to Execute" box, you can select the time(s) at which the backup will be run. The default is to run once a day, at 4:51 AM.

What to do if your main Hard Drive fails

If your main disk fails, then you can switch to the spare disk. The appliance must be halted and powered off before swapping drives. Depending on your appliance, there may be a release on the front of the drive bay that will allow the drive to be removed, or you may need to slide open the top of the case in order to remove a setscrew. Remove the main drive, and set aside. Then remove the spare disk, place it in the main drive bay, and boot the appliance.

Initializing a new backup hard drive

If your appliance has IDE disks, then you must power-off the appliance before installing the replacement drive. SATA drives can be installed while the appliance is running, but cannot be accessed until the appliance is booted with the drive installed. Once the spare drive is installed and the appliance is rebooted, run the following command as the "root" user:

buildspare

This will partition and format the spare disk. The main disk will be backed up at the next scheduled time.

Other Configuration Options

Configuring the ET/RXX00 as a Router:

Appliance units with multiple ethernet interfaces are configured as a bridge by default. Here are the steps you must take on a factory-fresh ET machine to enable routing:

From the ET/ADMIN interface, select the "Bandwidth" link on the left, then click on "Setup Bridging" icon.
You will see a list of the interfaces and their bridging status in the "ifac" column. . For each interface, click on the interface name, and change the bridging mode to "disabled", then click on "submit".

Now that you've disabled bridging, you must enable routing. From the main ET/ADMIN menu, select the "Network" tab, then "Network Configuration". Follow the instructions above on IP configuration to set the IP address for each interface.

<-- Return to Network Configuration

The next and final step is to use the "Routing and Gateways" tool to enable IP forwarding. Find the line "Act as Router?", and check "yes". Make sure that the default router for the machine is set properly, then click on "save". You will then have to reboot the system. As noted above, using a machine with the -FO failover ethernet option as a router renders the failover function useless, so it's recommended that you not do this.

Changing the ET/ADMIN Password:

The ET/ADMIN password for the default user "admin" can be changed by clicking on "Administration" and selecting "ET/Admin Users", then clicking on the user "admin" in the left column. The second line is the new password entry form. Click "set to", enter the new password, then click on "save". You will then receive an "invalid login" message. Login to ET/ADMIN using the new password.

Note that the user names for the system (which are used for Telnet/SSH and logging in at the console, for example), are not the same. The GUI has its own user/password combinations that are by default unrelated to the normal system users and passwords. In reality, there are 2 distinct "admin" users: one for the ET/ADMIN interface, and one for the system. The passwords for the 2 must be set independently. The "admin" login to the ET/ADMIN interface is the equivalent of "root" and has full access to change aspects of the operating system (known as superuser privileges). The other "admin" is the Unix user, which is simply used when connecting to the system using telnet or SSH. See the example for connecting via telnet and using the su command to become the superuser.

Changing the System Passwords

It is highly recommended that you also change the passwords of "root" and "admin". This can be accomplished by clicking on "Users and Groups" under the "System" tab. Click on each user, then select "Clear-text password", and type the new password in the field. When you click "save", the password will be encrypted and updated. Note that you can also use this area to add new users to the system and to manage their passwords. This menu ONLY changes system passwords. Changing the "Admin" user in this menu will only affect telnet and SSH access, not the ET/ADMIN GUI.

Notes on the Failover Watchdog Timer:

If your system has the Failover Ethernet option (-FO) installed, then there is a program called "bypassd"
which monitors your system's "sanity" and informs the failover hardware that the system is working properly. If the system fails, or if the bypassd daemon stops running, the failover hardware will connect the 2 ethernet ports, allowing traffic to flow. You can manually take the system offline to do maintenance with the Failover GUI function (located under the main "Admin" tab in the ET/ADMIN HTML interface). It is also recommended you take the unit offline before performing an upgrade.

Notes on the Hardware Watchdog:

Most of the systems (including all -SM machines, the ET/R4000i, and all ET/R1X00 units with two on-board ethernet ports) sold have a built-in watchdog timer which allows the machine to be automatically reset if it crashes or locks up. This watchdog is controlled by the same utility that handles the Failover ports, however it is an independent function (Failover simply bypasses the machine, while the motherboard watchdog issues a hard reset). Also, you do not need a failover card installed to enable this feature. The motherboard watchdog is DISABLED by default. To enable it, you must edit the file "/etc/rc.local" and uncomment the line that refers to your motherboard. There is one line for the ET/R1500, one for the ET/R1700, and one for the ET/R4000. Once you have done this, the watchdog utility will be run after the next boot.

Recovering Lost Passwords

Again, there are two types of passwords; system passwords and ET/ADMIN passwords. If you can log in via telnet or SSH, but are unable to access the GUI as user "admin", do the following. SSH (or telnet) to the appliance as "admin", then su to become root. At the prompt:

```
# cd /usr/local/webmin
# perl changepass.pl /etc/webmin admin password
```

This will change the "admin" user's password to password. If you are trying to change the password for a different ET/ADMIN user, simply replace "admin" with the correct username.

If, however, you are able to access the ET/ADMIN but not able to access the system via telnet or SSH, then you can change the system passwords via the ET/ADMIN as described above.

Changing the MySQL password:

Changing the default "saturn5" password for the MySQL database is recommended only if you plan on allowing external access to the database: by default, external access is simply not allowed. If you wish to change the password, you can do it via the command line or by using the ET/ADMIN MySQL interface.
Changing the password for the MySQL database via the command line: As root, perform the following command:

```
#mysqladmin -u root password yourpassword
```

If using the ET/ADMIN interface, click on the "Servers" tab, then the "MySQL Database Server". If you have not used this module previously, you may have to enter the current MySQL password (by default, "saturn5") before doing anything else. Under the "Global Options" section, you will see an icon for "User Permissions". Click on this icon, then find the entry for username "root", host "localhost". Click on the user to edit their settings. Do not change any permissions for the "root" user, simply select "Set to..." on the "Password" line and type the new password in the adjacent text field, then click "Save".

Then, make sure you are using the same password in the BWMGR section of the ET/ADMIN. Click on the BWMGR icon, then find the button labeled "edit defaults" on the same line as "Graphs". By default, this MySQL password is set to "saturn5", and if you change the MySQL password without changing this entry, no new data will be stored by rules with statistics enabled and you will be unable to retrieve past data, until you change your settings to match.

Other Appliance Functions

Using SSL Encryption with the graphical interface:

If you are using a browser that supports secure connections via SSL, then you may wish to enable SSL in the web interface. Click on the "Admin" tab, then select the "Admin Configuration" icon. Select the "SSL Encryption" icon. Check the top box to enable SSL encryption, then click "save". You may have to log in to the ET/ADMIN again. Your browser may also pop up several notices about expired certificates. Accept the certificates and continue. Much like SSH, SSL encrypts the web traffic generated by the ET/ADMIN interface, including initial password authentication, and is recommended for all remote access. Please note that when connecting directly to the ET/ADMIN interface with SSL enabled, you must use the "https://host.name:10000". Using the "http://" prefix (or no prefix) will not connect properly (generally with a "connection reset by peer" error message). If you are using Apache redirects make sure your redirect has the appropriate prefix.

Using the Apache HTTP Server with the ET/ADMIN:

The Apache webserver runs on port 80, while the ET/ADMIN interface runs on port 10000.
By default, the Apache server is configured to start at boot time. If it is not running, you can enable it in the ET/Admin GUI. Note that it may be necessary to set the hostname prior to starting Apache.

Under the "System Functions" tab, click on the icon "Boot Startup Tasks".

FreeBSD:

You will see a box with the contents of the file "/etc/rc.local". The second line should read:
#/usr/local/bin/apachectl start
To enable Apache on boot, remove the "#" character from the start of the line. Click on "Save", then hit your browser's "Back" button. Go to "Admin Index", select the "Servers" tab, then click on "Apache Webserver". To start the server immediately, click on "Start Apache" at the top right of the screen.

Linux:

Find and click on 'httpd' in the left-hand column. To start the Apache server immediately, click the "Start Now" button, and a confirmation message should appear. Now click "return to action" and make sure to change "Start at boot time" to 'yes' before saving the configuration.

Apache Redirects:

If you do not plan to use the appliance as a web server, but wish to access the ET/ADMIN via Apache, configure the webserver to make the ET/ADMIN the default page. (enable it first as shown above).

1)From the ET/ADMIN menu, click on the Servers tab, then select Apache Webserver
2)Under the Virtual Servers heading, select Default Server , then click on "Aliases and Redirects".
3)Next to the line "URL Redirects" you will see a "from" and "to" field. Put a forward slash in the "from" field (/), and in the "to" field place the following line (replace a.b.c.d with the IP of your appliance):

"http://a.b.c.d:10000" # Use this line if you have not enabled SSL
" https://a.b.c.d:10000" # Redirect to the SSL enabled port

Once you click on "apply changes" (at the top of the screen), simply connecting to http://a.b.c.d will call up the ET/ADMIN interface, and enable SSL if appropriate.

Using Public Graphs - Allowing Customers To View Graphs from WWW:

Because the ET/ADMIN GUI Interface has superuser priveleges and can modify any aspect of the running system, it is completely password protected. Hence, if you wish to allow your customers to access their public graph directories, you must use another access method, one that does not give root access. The ET/R series systems come with the Apache web server pre-installed, which can be used to view customer graphs. Here are the steps that must be taken to provide customer graph access.

1) Configure the graph you wish to allow acccess to, using the ET/Admin GUI: Select the graph name from the main BWMGR setup menu. Click the "Configure" button to the right of the graph name. Make sure the "Graph Directory" is "/graphs". Set a password for access if desired, and change the "Graph Access" type to "Public". *NOTE* leaving the password field blank will allow access to the graph information using only the graph name (no password required).

2) Test your setup by accessing "http://yourhostname/custgrph.htm". You should see text boxes for "Date", "Name", and "Password". Enter the graph name and password (if you've set one) in the fields and then click "Daily Graph". This should confirm that the public graph access is working.

The "custgrph.htm" file is an example of how to interface with the ET/BWMGR and allow customer logins. It can be used as-is, or it can be used as a template for creating your own login page. If you do customize this file, make sure you use a different name, as the changes made to custgrph.htm will be lost when you upgrade the machine using the "Update System" module.

Setting up an external MySQL database

If you're keeping statistics for a large number of rules, and/or your traffic levels are high, you may find that the response time of database functions is rather slow. Its also possible that your system will not be able to handle both bandwidth management and statistical gathering if you are trying to gather statistics for 1000s of rules on a heavily utilized system. In such cases, you may

benefit from running an external database. This will allow database processing (lookups and row insertion) to be completely offloaded to another system. Note that you will need to do this on your own, as we don't support MySQL generally except as it applies to functions within the appliance, and to provide examples that are known to work on a correctly configured system.

Following are the steps necessary to use an external MySQL database. In our example, assume the ET/BWMGR is running on IP 10.0.1.5, and the remote MySQL server on 10.0.1.33. The default password of 'saturn5' is used in the examples.

On the remote machine (10.0.1.33):

1) install and start the MySQL server (Appliance users unfamiliar with this process should refer to http://www.etinc.com/mysql.htm for steps 1-4)

2) Set default root password for the server:

```
# mysqladmin -u root password 'saturn5'
```

3) Install the ET/BWMGR software tarball on to the remote machine, or just copy /usr/hdlc/db from the bwmgr machine.

4) Create the ET/BWMGR databases:

```
# cd /usr/hdlc/db
# sh et_createdb
```

5) Allow access to the ET/BWMGR databases from the bwmgr machine.

```
# mysql -u root -p etbwmgr
Enter password: saturn5
mysql> grant ALL on etbwmgr.* to root@10.0.1.5 identified by 'saturn5';
mysql> exit
```

On the ET/BWMGR machine (10.0.1.5):

6) Test the connection from the bwmgr machine. If you get the "mysql>" prompt its working properly:

```
# mysql -u root -p -h 10.0.1.33
Enter password: saturn5
mysql> exit
```

7) use the "Edit Defaults" button on the ET/BWMGR GUI to change the database settings. Make sure database host points to the remote location of the MySQL server. Make sure the user name and password match the GRANT statement you used.

8) re-start bwmgrd on the bwmgr machine (or reboot).

```
# killall bwmgrd
# /usr/local/sbin/bwmgrd
```

Enabling and disabling snmpd (and other services):

Enabling or disabling any service can be done via the ET/ADMIN interface, as shown in Using the Apache HTTP Server with the ET/ADMIN. FreeBSD users should find the line in /etc/rc.local that pertains to the service they wish to modify, and either add or remove the # character to disable/enable the service at boot time. In LINUX, you can enable or disable services by clicking on "System" and then selecting "System Startup" icon and selecting the appropriate service.

Checking System Processes:

You can see a list of the active processes running on the system by connecting to the ET/ADMIN interface, and going to

System Functions -> Running Processes

bwmgrd must be running in order for the statistical gathering capabilities of the bwmgr to be utilized. It should be enabled by default. If bwmgrd is not running, it may be because the bwmgr is not running. This can be verified by selecting the "Bandwidth Manager" link, and noting the status of the bwmgr software.

Rebooting the System

From the main ET/ADMIN menu, select the "Admin" tab, then the "Reboot and Shutdown" icon. Clicking on "Shutdown" will halt the machine. To boot the machine after halting requires either a hard reset or "ctrl-alt-delete" from a keyboard. Clicking on "Reboot" will restart the machine. Both options will prompt for confirmation before actually bringing the system down.
Accessing the Bandwidth Manager

Configuring WAN interfaces:

If you have a system with WAN cards installed, you can edit your WAN interfaces by clicking on the "Network" tab and then selecting the ET/HDLC WAN Configuration icon.

You should see a menu which shows you the ports which have been detected in the system. On FreeBSD, the ports are named eth?, and on LINUX they are named ets?. Each port must be configured with a line protocol and also (typically) with an IP address pair. The exception to this is if you are bridging, in which case the interface may or may not need an IP address assignment.
Setting the WAN Interface Protocol

To set the protocol that will be running on a particular WAN port, click on the "Config Port" button to the left of the associated interface. This will bring up a menu that allows you to select the protocol to run on the card. Typically, all you have to do is select the protocol and them hit "Update Config File" or "Save and Apply". Selecting "Update Config File" will update the startup file which is run at boot time. Selecting "Save and Apply" will also apply the settings immediately to the port. Note that the ports must be configured in order (that is, you can't configure eth2 before eth1).
Setting the WAN IP Addresses

To set the IP addresses of the WAN card, select "IP Config" to the right of the port you wish to configure. Then set the Local and Remote IP addresses. Typically, point to point interfaces do not require netmasks (they are host addresses by default). Even if you are given a netmask, typically the system will not use it. Again, to save the info, click the "Save Config" or "Save and Apply". If you selected "Apply", you should see the new setting on the screen.

This document is designed simply to help in the initial setup of your appliance. Full documentation on utilizing and configuring ET/BWMGR software can be found on the Emerging Technologies web site under "Support".

Post-Configuration Security

Once you have your system configured and running in a stable manner, there are a few simple steps you can and should take to ensure that only authorized users can access the system. These appliances are not meant to be accessable by the internet at large, except in specific cases (for example, those users running a web server and/or allowing their customers to view graphs.) The below examples assume the bandwidth manager has an address of 207.252.1.110, and the machines allowed to connect are in the subnet 207.252.1.0/27 (netmask of 255.255.255.224).

* Create firewall rule(s) that enable only your local net, or individual machines, access to your system. This rule should be created on the interface you are connected to on the inside, unless you are running an ET/R1700 with the Failover hardware. Then you should create the rule on the administrative port.
Example: # bwmgr fxp0 -x 1000 -name IntAllow -fw -ipprot tcpconnect -saddr 207.252.1.0 -saddrmsk 255.255.255.224 -daddr 207.252.1.110

* On your external (outside) interface, create a firewall rule that denies ALL access to the IP address of your system. Or, if you are using the Failover hardware, create this rule on the administrative port. Leave room in your ruleset to create specific allow rules if you have an employee who needs to work on the machine remotely, or to allow traffic to a specific port (80) in the event that you allow your customers to view their graphs.

Example: # bwmgr fxp0 -x 1500 -name DenyAll -fw -ipprot tcpconnect -daddr 207.252.1.110 -priority FW-Deny
* Change the default passwords for admin, root, and the "admin" user in the ET/Admin GUI. This is less of a priority if you've already blocked external access to the machine, but it is still a good thing to do. If, for some reason, you do not block access to the bandwidth manager appliance, changing the passwords is an absolute requirement.

System Updates

Updating Your System Over the Internet:

Your system includes a 30 trial of our "Auto-Update" service, which allows you to automatically update your appliance with the latest code from our server. In order to use the update service, you will have to first register your system as previously described. If you do not receive your system promptly due to customs you can request that we extend the 30 day trial to account for the time lost. You MUST make this request BEFORE you register the system. Once you register the system we cannot extend the trial.

After 30 days, you can purchase the service for a fee (currently $250/year). This fee includes a new license key so that your key will work for the duration of the subscription. If you subscriptions lapses for more than 30 days (either your trial subscription or a yearly subscription), then the cost of the subscription increases by $100. When you receive a new key, either for a new auto-update subscription or extension, then you must **register** the new key, then **start** the BWMGR with the new key **before starting the update**. If you fail to do both of these steps, then the BWMGR may not start properly after the update.

Updating your system is accomplished via a button on the ET/ADMIN GUI. In the "Admin" section, you will see an link labelled "Upgrade System". Clicking on this link will give you two options. You can view the release notes for your OS, or you can press the "Check Versions" button which will connect to the upgrade server and compare your version to the one on the server. If you have a valid subscription and have registered the installation, you should see a listing of the software versions you are currently running, as well as the versions available on the update server. There are two software releases available. The "Stable" release is a version of the ET/BWMGR that has been in service for some time, and free of serious bugs. There is also the "Newest" release, which is of course the most recent version available. While we test these releases in-house (with special attention to functions that are new or have been changed), there are sometimes issues that do not manifest themselves until very specific conditions are encountered. If you do encounter any problems running the newest release, we recommend that you notify our support team. You can always "downgrade" to the Stable release if you encounter problems with the newest, however we recommend that unless you are prepared to monitor your system after upgrading, you consider using stable releases.

"View Upgrade Details" will list the available versions, display the release notes, and allow you to view the log of the last upgrade. It is highly recommended that you read all of the release notes available before upgrading your machine.

The "Change Defaults" section allows you to set your preference for the appliance to reboot itself following a successful upgrade. The automatic reboot is disabled by default on new systems.

If, for any reason, the bandwidth manager cannot access the update server, you will not see any of the above information. Instead, you will see an error message explaining what failed, along with possible causes and solutions.

At times, (including the releasing of new software), the update server may be unavailable. You will see a message indicating that the server is locked. Most maintenance takes less than one hour.

Once you begin an upgrade, it is very important that you do not interrupt it in any way, including closing your web browser, clicking the "stop" or "back" buttons, etc. If this does happen, the best thing to do is wait a few minutes, then go back to the update screen and start another upgrade. Once the upgrade is finished, you must reboot the appliance, unless you have selected an automatic reboot, in which case you will see a message to this effect, as well as a button which can be used to cancel the reboot. You can reboot the appliance by clicking on the word "reboot".

Update Subscription Notes:

In order to use your update subscription you will need to register the appliance on the IP address that will be used to obtain the updates. This implies that you cannot change the address of the machine, or the update server will not allow you access. If you need to change the address of the machine you will need to contact support and inform them of the move. You will then have to re-register the license key after we have authorized the change.

Reverting to the Previous Version:

If an upgrade fails, either because it was interrupted (by a user, by loss of network connectivity, or other failure), it is possible that the system may be in an unstable state. If you are unable to complete an upgrade, or if an upgrade appears to succeed and you then have serious problems after rebooting, you can use the "Revert" feature of the upgrade utility. Before each upgrade is begun, a backup of several key files (including the current kernel and BWMGR drivers/modules) is done, assuming the previous upgrade succeeded. This way, you always have a fallback to a known-good version. It is necessary to reboot the appliance after the reversion is complete. Note that configuration items, such as your rulesets, are not included in the reversion. To keep a copy of those and other files in a safe location, use the backup tool as explained in the next section.

Routine Maintenance

Monitoring System Status:

The "System and Server Status" is a useful tool for quickly checking the status of services on the appliance. This module is located in the "Administration" section of the ET/Admin GUI. When the module is selected, you will see a list of the configured monitors and the status for each. A green check icon indicates that the service is running. A red X icon indicates a service that has stopped or is not running. A black circle indicates a service that is not installed or configured.

Clicking on the name of each monitor will show an extended status. For example, clicking on "Bwmgrd Stats Daemon" will show the current status, usually "bwmgrd is running". If the service is not running, you should see the error message instead.

The monitor can also be configured to periodically check the configured services. Clicking the "Scheduled Monitoring" button will take you to the configuration menu. Make sure that "Scheduled checking enabled" is checked "Yes", and fill in the email notification section. Make sure you enter an email in the "Email status report to" field, and check the radio button to the left of this field.

The default setup has monitors configured for the MySQL database server, the bwmgrd stats collection daemon, the Apache webserver, and the Squid proxy server. Additional monitors can be configured, using the "Add Monitor of type" button after selecting the appropriate monitor from the pull-down list. One useful monitor type is "Disk Space". Select a partition and the minimum free space before creating the monitor. Assuming you have scheduled monitoring enabled, you will be emailed when free disk space on the selected partition is below this amount. Typically both /var and /usr partitions should be monitored.

Backup & Restore Overview:

The ET/R series servers allow the user to backup select portions of the Operating System, configuration files, and user data to either a local file, to a remote file via FTP, or a local ZIP drive. This feature is independent of the spare drive backup feature on appliances that support spare drives. There are three sets of files that can be backed up individually. We recommend making a backup of at least your ruleset and password information (the "Configuration" backup set) shortly after receiving the box and doing the initial configuration, as well as any time major changes are made to your BWMGR ruleset.

* Configuration Backup

Backs up the contents of /etc and /usr/local/etc/bwmgr/config. Includes all configuration options, such as usernames, passwords, BWMGR rulesets and graph configurations, IP address, DNS information, and others. Also included are copies of the databases used for ET/BWMGR rules (specifically, profiles, controls, and notifications). This set should be backed up soon after receiving the unit and configuring the rulesets, as well as any time major changes are made to rulesets or username/password files. Unlike the other two backup sets, this one will fit on a 1.44MB floppy disk.

* Database Backup

This set backs up the contents of the MySQL database, which holds the data for every rule that has statistics enabled. The BWMGR ruleset is also included in this set. A good candidate for a regular backup to a remote location, as this data changes continually. If you are not storing statistics, you may not want/need to back up this particular set.

* System File Backup

This backs up all system binaries, libraries, and configuration as well as users home directories. This backup should be performed only after system upgrades, since the files included shouldn't change often. This set does NOT include any BWMGR-related configuration files or data, but it does include binaries such as "bwmgr" "bwmgrd", etc.

Backing Up:

In the ET/ADMIN interface, view the "Admin" tab. Click the "Backup/Restore" link. You will be presented with a series of buttons: the first three, "Setup Files", "Data Files", and "System" are used to backup various parts of the system. The "Restore" button can be used to restore any backup previously made. When you click any of the backup buttons, you will see three buttons: "Change Destination", "Change Fileset", and "Start Backup". If you click on a backup set for the first time, you will be asked to use the "Change Destination" button to pick the location to store the backup contents. If you have not chosen a destination, clicking on the "Start Backup" button will display an error.

* Change Destination :

This leads to a menu that allows you to choose where the backup will be stored. You will see a list of possible backup

destinations. Make sure the radio button next to your desired choice is selected before clicking on the "Save" button. If a backup location is unavailable, it will not be listed as a choice. When selecting a remote location (FTP), you must fill in all of the text fields with the proper information. To successfully transfer a file via FTP, you must enter the hostname of the FTP server, your username, password, and the directory where you wish to store the backup. If any of these fields are blank, the configuration will not be saved, and an error message(s) will indicate exactly what is missing. Clicking "Cancel" at any point will return to the main backup menu without saving any changes. Once the changes are successfully made, the browser will return to the main backup screen. Obviously, use of the FTP backup requires that you have access to an FTP server on another machine.

* Change Fileset :

Note This setup option should typically not be altered except by those users that are familiar with the layout of the filesystem structure and wish to add or remove files from the pre-defined backup sets. For each backup, clicking on this button will show two text boxes. The first, labelled "Include", is a list of all files and directories that will be added to the backup. The second, labelled "Exclude", is a list of files and/or directories that should NOT be a part of the backup (typically only used when an individual file in a directory that exists in the "include" list needs to be excluded from the backup). Only one box may be edited at a time. Click the "Save" button immediately underneath the text window to save your changes. Click "Cancel" to return to a previous menu without saving.

* Start Backup:

Clicking this button will begin the backup process. If you are backing up the configuration set to a floppy, please make sure that it is in the drive and not write-protected before starting the backup (Otherwise you will see a floppy error message). The same applies to the ZIP disk. Once the backup begins, please do not close the browser until the page has finished loading, otherwise the backup may fail or be cut short. The "System" backup will take a relatively long time to finish; regular reports will be printed that show the filesize of the backup in progress.
Once the backup file is created on the local drive, it will be transferred to the remote location if you have selected one. Regardless of the ultimate destination of a backup set (ZIP, FTP, etc) the file will also be stored in the default location for local backups: /usr/local/backup. For FreeBSD users, a "config" backup set would be stored in the file "/usr/local/backup/etbackup.config.tgz". Linux backups use a different filename - "/usr/local/backup/etbackupl.config.tgz" for the above example. So even if you backup a file and lose the ZIP drive you stored it on, it may still be on the local hard drive. This won't help in the event you have a hard disk problem, however; you'll need to restore from the remote location.

Restore:

Clicking on the "Restore" button will prompt you to pick which backup set you would like to restore. Select the set you would like to restore, and press the "Continue" button.
Now you will need to pick the location to restore from. This is handy if you've backed up to multiple locations, but otherwise only one will work properly. Naturally, the floppy disk option will only appear on "Configuration" backup sets, and the ZIP disk option will NOT appear on that set; nor will it appear on systems that do not have a ZIP drive installed.
From this screen, pressing "Restore!" will immediately begin the restore process, so take care to check that you've selected the right backup set. Of course, if you select a backup that doesn't exist (has not been backed up previously, or to a different location), an error will be displayed. You can use the "back" button on your browser or the "Return to Previous" button at the bottom of the page to return to an earlier restore menu. Since all backups are stored first on a local partition, selecting "local filesystem" as the restore location will restore from the last-backed up version of a backup set.
After a configuration or system restore, it is necessary you reboot the machine after the restore, since system binaries and libraries may have been updated.

Maintaining the Statistics Database - Purging Old Data:

If you are using the database to gather statistics, you will have to purge old data from the database after some period of time, as eventually you will run out of disk space. How much data you can store on your disk will depend on the amount of disk space available, and the number of rules for which you are gathering data. The rule of thumb is 1.2MB of disk space used per rule, per month. To get an idea of how much disk space you have available, you should periodically check your system from the system console. To see your current disk usage, either configure a Disk Space Monitor, or log into the system as "root" and issue the following command:

df

You should see something similar to the following:

Filesystem 1K-blocks Used Avail Capacity Mounted on

/dev/ad0s1a 116695 47582 59778 44% /
/dev/ad0s3f 3964470 1146036 2501277 31% /usr
/dev/ad0s3e 148823 7601 129317 6% /var
procfs 4 4 0 100% /proc

The above shows that 31% of /usr is in use (the database is stored on the /usr partition). For each mounted partition, you will see the amount used, amount free, the mount point, and the amount used expressed as a percentage of available space. This number can actually run higher than 100%, since about 5% of the disk is "reserved" and not counted as free space. If you see a number approaching or exceeding 100% for /usr, you must free up some space. Unless you have installed other applications and/or data, the database files should be taking up the most space. You can easily delete old graph data from the database, by issuing the following command in the "Execute SQL" field in the "MySQL Server" module, located in the "Servers" tab. Click on the database you wish to modify ('etbwmgr') and you will see the "Execute SQL" button. In the resulting text box, enter your SQL commands: The first thing you should do is check to make sure there is data to delete in the time span you plan to delete data from (in the below example, we want to delete anything prior to Jan 1, 2002)

select count(*) from bwdata where date < "2002/01/01"

then press the "Execute" button.

This will result in a text box containing the total number of entries for all rules in the time period matched. If zero, then there is no data matched. There are approximately 4300 entries per rule per month, so bear that in mind when interpreting the results. Assume now that our query above results in about 2,500,000 matches, which is roughly approximate to 4 months worth of 150 stats rules. This means that clearing this data will probably free up about 720MB of disk space. Now let's clear the data:

delete from bwdata_daily where year <= '2002' OR month < '7'

then press the "Execute" button. Be careful here that your logic is correct so you don't delete data you want to keep. After you've deleted the previous years you don't need the year specification.

Note the European date format. This will discard any data before the date specified in the format YYYY/MM/DD. Note that you must be very precise in doing this or you may delete current data, and if you don't have a backup there's no way to restore data deleted from the database. The MySQL GUI will not return any result after a successful delete. You should either re-run the select query above, or use "df" to see if you have more space available on the /usr partition. Combining regular backups with purges will both keep the database at a reasonable size and allow recovery from an accidental purge or other failure.

Deleting data from your database will not necessarily free up the disk space it was using. Because of fragmentation, delete just frees space within the database file itself (ie creates empty records which can be used for new data). In order to free the old space, you'll need to "optimize" the database, which will defrag it and free the disk space. In the SQL command box, enter:

optimize table bwdata

then press the "Execute" button.

Repairing a Broken Data Base

See Troubleshooting

Using the Recovery CD-ROM

The recovery CD-ROM allows you to boot your system and perform various functions, including repairing a hard drive crash, restoring files and even upgrading the base operating system on your drive. In the event of a physical drive failure, the CD-ROM will allow you to rebuild a system using a blank hard drive, and load it with the latest release.

If your appliance has a CD-ROM drive you can purchase a recovery CD-ROM from the Emerging Technologies website. If your appliance does not have a CD-ROM you may be able to add a CD-ROM drive to your system. Contact ET support to find out if you can ugrade your system.

Note that most of the recovery functions of the CD-ROM require an active auto-update subscription. If you don't currently have an update subscription you can buy a package which includes the CD-ROM and an update subscription.

Detailed instructions for using the recovery CD-ROM are available on the ET web site.

Support

Support is available by creating a support ticket on www.etinc.com. Telephone support is only available for critical, "system down" problems. When you send your email, please try to explain your problem in detail so that we can help you without having to ask you for more info. When sending files, please cut and paste them into the email rather than sending attachments. Support is generally available between 10am and 6pm M-F. Email is usually answered over the weekends whenever possible.

Troubleshooting

See the latest Troubleshooting Documentation.

ET Recovery CD Setup Manual (FreeBSD)

What is the ET/Recovery CD?

System Requirements.

Basic Operation.

- Common uses.
- System Repair
- Automated Filesystem Repair.
- Recovering Missing or Damaged Files.
- Upgrade/Installation.

Removing the CD from the drive.

Booting an upgraded or newly installed appliance.

What is the ET/Recovery CD?

The ET/Recovery is a bootable CD-ROM that can be used to facilitate system repair and data recovery, as well as for upgrades of existing appliances and new installations onto appliances where the hard drive has been replaced.

System Requirements.

ET/Recovery will work on any ET/R series appliance where the following requirements are met:
* CD-ROM drive installed
* Celeron 600 or higher speed/class processor
* CD boot enabled in the BIOS (boot order should be CDROM, floppy, IDE HD).
* A working internet connection and valid license key/Auto-Update to perform upgrade functions.

Setup Notes

* The ATAPI CD-ROM drive MUST be attached to the Secondary IDE controller as a Master drive.

* Make sure the first serial port (COM1) is enabled with the default values (3F8, IRQ3). If this is not done, the machine will lock up during the first boot stage. The serial port is not used, however the kernel on the CD requires it to be there.
* Select the CDROM as the first boot device. (order should be CD-ROM, floppy, IDE HD)

Basic Operation

Load the CD in the drive, and boot the appliance. After a few moments you will see a login prompt. Log in with the default username and password, and you will be displayed a short welcome message and the root prompt (#).

login: root
password: saturn5

You can receive a quick list of the available commands by typing "help" at the prompt. All of the standard UNIX commands are available as well. If you are planning on running any of the commands that require an internet connection, run 'etip' to configure your network as the first step.

NOTE: Even if you are using a cache system, and have your IP address on an interface other than fxp0 or em0, you MUST select your key interface when using 'etip' on the Recovery CD. Otherwise, it will not recognize your license key, and the advanced features will not work.

NOTE: if you have a floppy-based backup of your appliance configuration, then you can use that floppy in conjunction with the ET/Recovery CD. Simply place the floppy in the drive before booting from the CD. This may be useful for upgrades or

recoveries on remote systems, or appliances that do not have a regular console attached. This means that you do not have to run 'etip' to configure the IP address or enter your license key. It also means that instead of the default "saturn5" passwords, the UNIX passwords from your appliance will be used. Once the CD has booted, you can telnet or SSH in to the appliance using the same IP and login information as you would normally use.

Overview

How do I use the CD?

All of the commands require you to be logged in as the super-user (root). If you are using a monitor and keyboard (AKA console), you can simply log in as "root". If you are using a boot floppy and connecting remotely, then log in as "admin" and use the "su -" command to become the superuser.

SYSTEM REPAIR

* filesystems : Is your appliance not booting because 'fsck' is failing at boot time?

Run the 'fix' command This will attempt to examine, repair, and then mount your appliances FreeBSD filesystems. Once this is done, your filesystems will be mounted on the /mnt directory. If it is not possible to repair the filesystems, you will see a message to that effect.

* boot problems : Has a recent change to your BWMGR (or other system) configuration prevented a successful boot?

Run the 'fix' command described above, and your filesystems will be mounted on the /mnt directory. You can then make the necessary changes to your startup scripts, to enable your system to boot. If the filesystems have errors that cannot be repaired, then they will be mounted as read-only.

Recovering Missing or Damaged Files

* If you are missing files, or suspect files have been corrupted, and you cannot perform an auto-update from the ET/Admin GUI [or if the auto-update does not fix the affected file(s)]

Run the 'fix' command, then run either the 'restorefile' or 'checkfiles' command.

When using the 'restorefile' command, you must specify any file(s) you want to restore, eg;

restorefile etc/rc.local

Note that trying to restore "/etc/rc.local" will fail because of the leading / character. To restore multiple files, simply use quotes:

restorefile "etc/rc.local etc/rc.bwmgr bin/login"

'restorefile' will list each file as it is being restored, and will display an error for each file specified that cannot be found on the CD-ROM. If this occurs it is recommended that you use the 'checkfiles' command instead. 'Checkfiles' requires a valid internet connection, license, and auto-update subscription. You will be prompted for all required information, if you have not already entered it.

If 'checkfiles' does not fix the problem you are having, then you can use the 'etrestore' command, which is a more involved process that includes overwriting all system files. Unlike 'checkfiles', etrestore requires that the CD Operating System version matches what you have installed on the appliance. If they do match, you will be prompted to continue.

UPGRADE/INSTALLATION

* upgrade :

Use the 'etupgrade' command to upgrade OS versions, or to wipe out all user, password, and BWMGR settings. Databases are left intact, but we recommend that a backup be performed before upgrading as a precaution. If you have booted with a floppy in the drive that contains a backup of your appliance configuration, the network settings will be transferred onto the newly created disk.

* full install :

Use the 'etinstall' command to install the appliance image onto a blank disk, or to upgrade an appliance if you do not need to keep your old stats info or do not have a backup. Please note that a dual-boot appliance will become FreeBSD-ONLY after upgrading in this fashion. If you really wish to retain the dual-boot capability, use the 'etupgrade' command. If you have booted with a floppy in the drive that contains a backup of your appliance configuration, the network settings will be transferred onto the newly created disk.

Removing the CD from the drive

You cannot remove the CD from the drive until the machine has been shut down. It is very important that the machine be shut down properly. From the root prompt, run the 'halt' command, which will shut down the system properly. Once the machine is halted, then you can eject the CD tray and remove the disc. Also remove the floppy disk if it is loaded.

Booting an upgraded or newly installed appliance:

Once you remove the CD (and floppy) and boot your appliance, you will need to configure the appliance much like a newly-purchased appliance. However, if you booted your ET/Recovery CD with a floppy in the drive that contains a backup of your appliance configuration, the network settings will be transferred onto the newly created disk, so you can skip the 'etip' step. Here is the recommended action list.

1) Run 'etip' to configure network settings (not necessary with boot floppy).

2) Connect to the ET/Admin GUI on the appliance's IP address.

3) If you wish to restore your passwords and ET/BWMGR configuration, then:
a. Place the floppy disk in the drive.
b. Select the "Backup/Restore" link in the "Administration" section.
c. Select "Restore".
d. Select the first option, "ET/BWMGR Configuration files only".
e: Select "floppy disk" as your backup source, and then "Restore!"
f: Remove the floppy when the restore is finished.

4) Perform an Auto-Update.
a. Select "Update System" from the "Administration" section.
b. Click "Check for Updates"
c. Select either the latest "Stable" release, or the newest release as you prefer.

5) Reboot (regardless of whether the update process indicates a reboot is required).

Troubleshooting

ET/BWMGR Software and Appliances:

ET/BWMGR Software and Appliance - Common Problems

Following are common problems and potential solutions with systems running ET/BWMGR systems:

Loop Messages on console and/or in /var/log/messages

A bridge configuration depends on each MAC address on your network being accessible via only one port of the bridge. A LOOP occurs when any given MAC address can be reached on both sides of the bridge. This is not necessarily a problem if you get one or two isolated messages - especially during testing when you may be moving machines around or plugging them into different ports. If you see a screen full of these messages, this means that two or more bridged ports on the appliance are plugged into the same switch or hub. Specifically, the message tells you that the MAC address was received on both of the referenced interfaces. Constant looping can either halt your system or make it painfully slow, and must be resolved. It indicates a serious flaw in your network setup.

In a Bridge configuration, packets cannot pass or you get a lot of errors.

This can be caused by a number of problems.

(If you know you are getting errors on 1 or more interfaces, go to #2)

1) First, check your configuration. Using "bwmgr showbridges", verify that the 2 ports are both in the same bridge group. Make certain that the 2 devices (one on one side of the bridge and one on the other) are both on the same logical network. Make sure you have no rules defined on either interface. Also verify that only the primary bridge interface (shown by showbridges) has an IP address on the logical network that you are bridging. Typically secondary interfaces will have no IP address assigned. You should be able to access the machine from both sides of the device (using a device on the same logical network, of course). First try pinging on the primary interface wire. Then the other. If neither work, then you most likely have a logical setup problem.

2) If that doesnt work, check for errors on the interfaces. Use "netstat -i" in FreeBSD or "ifconfig interface" in

LINUX. If you are getting errors when you try to pass data you may have a wiring problem. Using crossover cables direct to Cisco equipment is a known problem area, as Ciscos do not NWAY (ie negotiate links) correctly in general. If you are getting errors, you can usually solve the problem by forcing the interface on the switch and the ET/BWMGR system to the same setting. You can use ifconfig in FreeBSD (see man interface for details on command and options), and mii-tool in LINUX. If possible, try to use the bwmgr box setting and force the switch or router. If that doesnt work, try to force both. If you can't get that to work, you can put a small switch in between which with allow separate negotiation by each device. We've found that a cheap switch can often solve the problem.

To set the interface in FreeBSD:

ifconfig fxp0 media 100baseTX mediaopt full-duplex

would set fxp0 interface to 100Mb/s, Full Duplex. See the fxp man page ('man fxp' on the console) for a list of options.

To set the interface in LINUX:

mii-diag -F 100baseTx-FD eth0

would set eth0 to 100Mb/s Full Duplex

Bridge won't pass packets - System/Appliance

if you do NOT have a Failover-equipped appliance, one possibility is that the secondary port is not connected: The primary ethernet port (eth0/fxp0) is part of the motherboard and cannot come loose. The secondary port(s) are located in PCI expansion card slots internally, and there is a small chance that they may move enough during shipping to move out of the slot. If this happens, typically the interface will not be shown in the system at all. From the command line, you can issue the command "bwmgr showbridges". If only eth0/fxp0 is listed, this is your likely culprit. You can also check with the "ifconfig" command from the command line. For example: *ifconfig eth1* (on a LINUX system) or

ifconfig fxp1 (on a FreeBSD system) or

ifconfig dc0 (on a FreeBSD 5-port system)

If the system indicates that the device cannot be found, then the second port (the ethernet card in the box) is probably unseated. If you suspect that a board has become unseated, you need to take off the cover and reseat the board. **If you do so, make certain that you call Emerging Technologies, Inc. at (631) 271-4525 and tell them; otherwise you may void your warranty**. Note that this procedure is only required when the port cannot be found; if the port is shown via ifconfig and the ET/ADMIN (Networking->Network Configuration->Configure Interfaces) reseating the card should not be necessary.

If the interface is present, see above

ET/BWMGR is Limiting Too Much

If you have a limit set to (for example) 256000, and you can't get a local application to use that much, these are the likely causes: One, you could be losing packets. Check your interface for errors and look for drops on the rule. You could also have a tcp window problem. Try using different settings for tcpwindow to keep the window from being set too low. Try 5000 to start. A setting of 64000 effectively disables window shaping. If you still get overlimiting and you are running LINUX with a standalone license, make sure you build a kernel on that machine. There have been reports that running ET generated kernels on AMD Athlon CPUs result in some timing errors. Rebuilding a custom kernel on the machine seems to fix the problem.

Registration Problems

"Server Down" message

If you get this message, it means that your system did not get a response from our server. Registration requires a "handshake" on a udp port in the 4000-5000 port range. Usually this occurs because the return message from our server was blocked by a firewall. If support tells you that your registration request was received by our server, then the problem is on your end.

"Invalid Key" message

This usually means that you are trying to register a key that can't be registered, such as a 30 day test key.

No Graphs or Graphs are Empty

If you have a problem viewing graphs, there is likely some problem interfacing to your database. If the graph is not created or you get a broken graphic symbol on your browser, then you should check your HTTP_ROOT and default graph directory in your ET/BWMGR defaults settings.

If you have empty graphs and you know that data is being collected (ie you see hits on the associated rule), then the data is not being put into the database for one reason or another. Things to check are:

- Check the System Status module, and make sure that bwmgrd and MySQL are running. bwmgrd is the daemon that puts the stats data into the MySQL database.
- If bwmgrd is not running, click on "Bwmgrd Stats Daemon", and check the current status for the reason. Also check /var/log/bwmgrd.log for errors or information. Make sure that when it starts it says that its using the database.
- If bwmgrd.log doesn't indicate it is using the MySQL database, check your settings using the "edit defaults" button from the GUI.
- Your database may be damaged. See the next section and check the bwdata table.

MySQL Problems and Database Repair

If you are having problems with the MySQL database, you should first take a look at the following log files: */usr/local/var/mysql/HOSTNAME.err* (HOSTNAME refers to the hostname of the machine) and */var/log/bwmgrd.log*

There are two types of potential problems that can affect MySQL databases. In the first type, the database will be completely inaccessible. If none of your stats rules (even the ones you know are getting hits) show any data from ANY time periods, then either the MySQL server is down, or you have a password problem that is preventing you (and the BWMGR) from accessing the database. Make sure your defaults are correct in the GUI (database name, username, password). You can also confirm that the MySQL server is running and the default password (saturn5) works in the ET/Admin GUI by clicking on "servers" -> "MySQL Server". If you get a menu of the databases, this means the server is running. If the passwords check out and the server is running, you may have to check /var/log/bwmgrd.log and make sure "bwmgrd" is running.

The second type of problem can be caused by a corrupt database, which is very rare and can be caused by a previous system or MySQL server crash. In this case, the server is still running, but some or all of your stats rules are unable to store or retrieve information from the database. You will likely be able to retreive older stats information, but not current ones. You may also see a large number of "Duplicate entries for key X" messages in /var/log/bwmgrd.log. What you should do in this case depends on when your last backup of the database was. If you have a very recent backup of a working database, then restoring that may be the best option. Otherwise, it's recommended you make a local backup of the databases in /usr/local/var/mysql, and issue the following command as the user "root":

fixdb

The 'fixdb' command will shut down bwmgrd and the MySQL database, and attempt to repair your database tables and then restart MySQLD. This can be a slow process, especially with large databases. When the process is complete, if the repair was successful you should see the following line:

"Starting mysqld daemon with databases from /usr/local/var/mysql"

If you see this line and no further error messages, then you can then re-start bwmgrd.

/usr/local/sbin/bmwgrd

If you continue to have database problems after running 'fixdb', then use the manual method below:

First, change your directory to the location of the 'etbwmgr' database files, and list the files.

#cd /usr/local/var/mysql/etbwmgr
#ls -la

```
drwx------  2 mysql  mysql     512 Oct 11 14:55 .
drwx------  4 mysql  mysql     512 Oct 14 11:24 ..
-rw-rw----  1 mysql  mysql  107696 Oct 14 14:00 bwdata.MYD
-rw-rw----  1 mysql  mysql   24576 Oct 14 14:00 bwdata.MYI
-rw-rw----  1 mysql  mysql    9042 Oct 11 14:55 bwdata.frm
-rw-rw----  1 mysql  mysql      67 Oct 14 14:00 markers.MYD
-rw-rw----  1 mysql  mysql    2048 Oct 14 11:25 markers.MYI
-rw-rw----  1 mysql  mysql    8710 Oct 11 14:55 markers.frm
```

You should see a listing similar to the above, although the filesizes will be different. If you do not have the same files, and instead see "bwdata.ISD" and "bwdata.ISM", then instead of running "*myisamchk*" in the below examples, you must run "*isamchk*" instead.

The next step is to check your database for errors. Below is the output from an uncorrupted database.

#myisamchk bwdata

```
Checking MyISAM file: bwdata
Data records:     849   Deleted blocks:       0
- check file-size
- check key delete-chain
- check record delete-chain
- check index reference
- check data record references index: 1
- check data record references index: 2
- check data record references index: 3
```

If you see errors listed, the next step is to attempt repair. Note that although there are a couple of repair approaches, if you can't recover the data using the following command, it may be difficult to do any recovery, unless you are very familiar with database interaction. Please note that if you see the following lines, this does NOT indicate a serious database corruption.

```
myisamchk: warning: 1 clients is using or hasn't closed the table properly
MyISAM-table 'bwdata' is usable but should be fixed
```

The key line to look for in order to determine whether a repair is needed is the last two lines of output:

```
"MyISAM-table 'bwdata' is corrupted
Fix it using switch "-r" or "-o"
```

If you see these lines, then the next step is to attempt a repair: First, shut down the MySQL server:

mysqladmin -p -u root shutdown (you will be prompted for the password to complete this step.)

Next, backup the /usr/local/var/mysql directory manually or using the "Backup" feature of the ET/Admin.

myisamchk -r bwdata

If you have an appliance or your mySQL distribution is built using /var as the default directory, you may not have enough space in the partition to repair your database. In this case, create a temp directory in your /usr partition if you dont already have one and specify it as the temp directory as follows

#mkdir /usr/local/temp
#myisamchk --tmpdir=/usr/local/temp -r bwdata

If the repair is successful then you will be able to restart the MySQL server and you are done. If the repair is not successful your only reliable option is a restore from your last backup or to re-create an empty database (You do have backups, right?).

/usr/local/bin/safe_mysqld --user=mysql & (Restart the MySQL server.)

If you see big spikes in your Graph Data when rebooting

If you see big spikes in your graphs that correspond to a reboot, it probably means that bwmgrd was started before mysqld, either because you started them in the wrong order or because of timing issues with system threads. Make certain that you start mysqld before bwmgrd, and then you allow at least 2 seconds in between for mysqld to get its act together. You can do this with a "sleep", or by running something else in-between.

You'll need to manually remove the "spikes" from the database with an SQL DELETE. Figure out approximately what the data size is (from the graphs, noting a duration of 300 seconds) and look for data that far exceeds a normal reading for the graph. So, for example, if the normal high reading is 120kbs for incoming data, that equates to a "bytes_in" setting of about 4.5 million bytes. (120,000/8 * 300). You could search the database on the given date for values over 8 million, and you should be able to locate your spike data. Just delete the row, as the reading is invalid.

"Can't Get Statistics" Error Messages

If you see "can't get statistics for *rulename*" messages in your /var/log/bwmgrd.log file, it means that a rule was deleted (or failed on startup) that the statistical system still thinks should be there. When you delete a rule gracefully from the GUI, the marker file that bwmgrd looks for is removed. If the rule was removed purposefully, you can get rid of this message by deleting the associated file in the /usr/local/etc/bwmgr/config directory.

What to do if your system/appliance doesn't power up properly

If the unit is completely unresponsive (ie, no fan noise, nothing on the screen, no beeping), check all power connections, as well as all switches. The ET/R1500 series have a main power switch on the power supply as well as a "power-on" switch on the front panel. For users with the 2U enclosure option, make sure that you have the correct voltage (see power supply requirements). If the outlet and power cord test good (test on a monitor or other appliance with a standard AC input), and there's still absolutely no response from the unit, contact Emerging Technologies for technical support or RMA service.

If the unit powers up, but freezes before the OS boots, then it's possible that the CPU fan/heatsink has popped off its mount during shipping. Please make a note of what's on the monitor, then power-off the machine and contact Emerging Technologies' technical support.
(LINUX Only) If the boot stops at the message "Starting system logger:", this is likely due to an incorrect or missing DNS setup. You must wait for the current program (syslogd) to timeout while trying to get the hostname. This may take up to 3 minutes, so be patient. Once the machine has booted, make sure DNS is enabled and setup properly.

If the unit displays the power-on self-test (POST), but does not find a bootable device, it's possible (although very unlikely) that the IDE cable has come loose from either the hard drive or the motherboard. Please notify Emerging Technologies' support staff before opening the box!
If the monitor remains blank, but the fans start and you hear a series of beeps from the unit, this indicates a problem with the memory. The ET/R1500 units use standard DIMM RAM modules. Either the module has come loose from its seating, or has failed completely. Contact Emerging Technologies' support staff before opening the box and attempting to re-seat the RAM. If re-seating the RAM does not work, we will likely issue an RMA.

Disaster Recovery

This section deals with a situation wherein your appliance does not boot, either due to a crash that fsck (the UNIX "chkdsk" or "scandisk" equivalent) cannot deal with gracefully, or a panic during the boot process. In either case, you can either use the ET/Recovery CD to fix the problem, or take manual control of the appliance at boot time.

If you do not have a Recovery CD, then you must follow the step-by-step instructions below. If you do have a CD, boot the appliance with the CD-ROM in the drive, and use the "fix" command to repair and mount the appliance filesystems automatically. If you are experiencing a panic, you can make the necessary changes after running "fix", since the appliance

filesystem will be accessible in the "/mnt" directory. See the ET/Recovery Manual for more information.

Manual Instructions:

FreeBSD

Hit "F1" at the boot menu to select FreeBSD. After a few seconds, you will see the text "kernel= " as the kernel is loaded, followed by a 3-second countdown. Press the spacebar (or any key besides enter) to interrupt the boot. You will then see a "boot>" prompt. Enter the following command to boot into single-user mode:

```
boot> boot -s
```

Alternately, if you are loading a debug kernel, you must instead do this:

```
boot> unload
boot> load kernel.dbg
boot> boot
```

This will load the debug kernel for a single boot.

You will be prompted to enter the shell for root, if you are entering single-user mode. Simply hit "enter" to accept the default of /bin/sh. Now you should have a root prompt - key in the following series of commands:

```
# /sbin/fsck -y /
# /sbin/fsck -y /var
# /sbin/fsck -y /usr
```

This last command should take a few minutes to complete, at which time you can either continue the boot, or you can make appropriate changes to your startup files. If you need to make any changes, you must first enable read/write access to your filesystems:

```
# mount -a
```

If you know exactly what is causing the problem, then you can take specific action to fix it. If you suspect a BWMGR rule is causing problems, but don't know which one, then you can bypass starting the ET/BWMGR like this:

```
# mv /etc/rc.bwmgr /etc/rc.bwmgr.sav
# mv /etc/rc.bridge /etc/rc.bridge.save

# exit
```

LINUX:

Hit "F2" at the boot menu to select Linux. Next will appear the "LILO:" prompt. Type " linux -s " at the prompt and press enter. You may have to enter the root password to get a shell prompt. At the prompt, type the following commands:

```
# /sbin/fsck -y /
# /sbin/fsck -y /usr
```

This last command should take a few minutes to complete, at which time you can either continue the boot, or you can make appropriate changes to your startup files. If you need to make any changes, you must first enable read/write access to your filesystems:

```
# mount -a
```

If you know exactly what is causing the problem, then you can take specific action to fix it. If you suspect a BWMGR rule is causing problems, but don't know which one, then you can bypass starting the ET/BWMGR like this:

```
# mv /etc/rc.bwmgr /etc/rc.bwmgr.sav
# mv /etc/rc.bridge /etc/rc.bridge.save

# exit
```

Hopefully you will be able to boot after performing this procedure. If not, please contact Emerging Technologies for technical assistance.