Table of Contents

Packing List

- One (1) WebMux unit

- One (1) Power cord

- One (1) User Manual

- One (1) Warranty registration card

Main Components

Front View

Toggle Power Switch
This switch toggles power on and off. To power off, the switch must be pressed and held for 5 seconds.

Reset Button
Press and release the reset button to reset the WebMux. This process may take several minutes to complete.

Up Arrow Button, Down Arrow Button
When each button pressed, the value of the cursor location increases or decreased. It goes through lower case letters, upper case letters, numbers and symbols. When cursor is located at the left most position on the LCD, up and down arrow also allow user to select different item to setup.

Left Arrow Button and Right Arrow Button
When each button is pressed, the cursor moves to the left and right.

Check Mark Button, and Cross Button
Check Mark Button confirms the selection, Cross Button cancels the selection. At any time during the system running, hold down to the Check Mark Button will invoke the configuration menu allowing the IP address changes.

Rear View
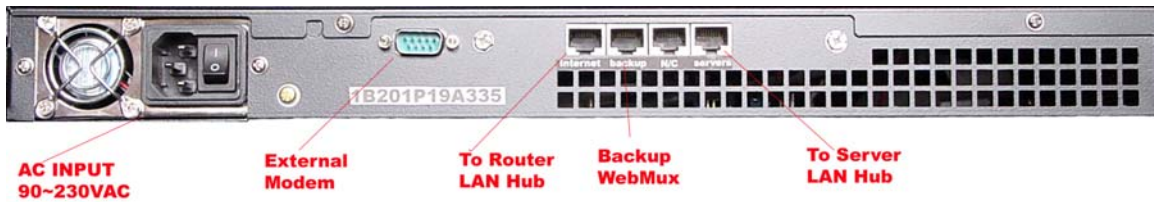
Server LAN Port
Connect this port to the Server LAN switch or hub. This port connects to the servers and your local computers. It is the right most RJ45 socket. In Out-of Path configuration, this is the only Ethernet cable to be connected.

Backup WebMux Port
Optionally, you may connect another WebMux to this port so that you can have redundancy. If you have more than one WebMux, you can connect them using cross over cable, or regular cable with a hub.

Router LAN Port
Connect this port to the Router LAN switch or hub. In most situations, this port connects to the Internet side network in NAT mode. It is the left most RJ45 Socket.

> **Please note: The Router LAN and Server LAN port are not interchangeable.**

External Modem Connect Port
To utilize the phone pager function of the WebMux, please connect the external modem to this port. In some cases, if you prefer support engineers not using diagnostic port over Internet, our support engineers can also connect through modem to assist you for setup issues. An USRobotics V.Everything modem is required, US Robotics part number 3CP3453. Modem dip switch has 3, 8, and 10 down, rest up. A standard external modem cable also needed. Check with your modem supplier for the cable.

Power Switch
This switches the WebMux on and off. When in the "off" position, the front panel power switch is disabled.

Power Cord
Please use the supplied power cord to connect the WebMux™ to power source. 1U WebMux has a 115V/230V AC universal power supply.

WebMux Overview

Key Features

The WebMux is a standalone network appliance designed primarily to load balance IP traffic to multiple servers. The WebMux includes the following key features.

- **Improves performance** by distributing the traffic for a site or domain among multiple servers. No one server will be bogged down trying to service a particular site.

- **Provides high availability** by tracking which servers are functioning properly and which servers are out of service. If a server unexpectedly goes down, the WebMux will automatically re-direct the traffic to other servers, or will bring a standby or backup server online to service the traffic. WebMux does application level health check to many network protocols on servers.

- **Provides Persistent Connections** by memorizing the user browser session and the server session and sending the same user to the same server. This is important for sites using shopping cart and dynamically generated pages, like BroadVision, ASP and JSP sites.

- **Provides fault tolerance**. This installation requires two WebMuxes, a primary and a secondary. Two WebMuxs will automatically sync the configuration datum.

- **Easy management**. It can be managed via a secured web browser session from anywhere in the world. By using https 128 bit encryption to the management web console, remote management of server farms is truly possible.

- **Operating System independent.** No software or agent to load on the servers. Non-intrusive load/failure detection and management.

- **Provides Proxy function**. When communication is initiated from behind the WebMux, the WebMux will substitute its own address for the internal address.   This allows the web servers to initiate communication for services such as credit card validation and mapping services. (Note: this function only works in NAT mode).

- **Built-in Firewall Protections.** Stop possible hacker intrusion into your network from Internet. All IP addresses and ports are blocked except the farm IP address. Built-in functions will detect any possible denial of service attack and make your services always available. (Note: this function only works in NAT mode with "Forwarding Deny", see setup for details).

- **In-Path or Out-of-Path Load Balancing.** In normal setup, the WebMux can be configured In-Path, to act as firewall in addition to the load balancer and health checker. However, if outbound traffic is much larger than inbound traffic and you already have a firewall in place, or change of IP address causes problem, consider using Out-of-Path configuration. Out-of-Path load balancing is also called direct routing, or one leg operation.

- **Informs you** of the status of your network. It provides phone pager and email notification so that the network administrator can be paged or emailed whenever a server or WebMux goes down, and when it returns online. This feature could reduce server room night shift operator costs, or timely repair should the server goes down unexpectedly.

The WebMux Family

The 1U WebMux family consists of two models. They are:

- The WebMux
- The WebMux Pro

The table below compares the features of the models.

|	WebMux	WebMux Pro
Topologies:		
Ethernet/Fast Ethernet	Yes	N/A
GB Ethernet (1000Base-TX)	N/A	Yes
Balancing Method:		
Round-Robin	Yes	Yes
Persistent Round-Robin	Yes	Yes
Weighted Round-robin	Yes	Yes
Persistent Weighted Round-robin	Yes	Yes
Least Connections	Yes	Yes
Persistent Least Connections	Yes	Yes
Weighted Least Connections	Yes	Yes
Persistent Weighted Least Connections	Yes	Yes
Weighted Fast Response	Yes	Yes
Persistent Weighted Fast Response	Yes	Yes
Fault Tolerance:		
Diskless Design	Yes	Yes
Port aggregation	Yes	Yes
Failover via serial link	Yes	Yes
Service aware	Yes	Yes
Server aware	Yes	Yes
Backup server	Yes	Yes
Performance:		
Maximum concurrent connections	1,440,000	5,760,000
Maximum new connections per second	7,000	40,000
Maximum throughput per second	200 MBit/s	1 GBit/s
Maximum Internet Link Speed	2 X T3	1.5 X OC-12

Management:		
Secure web browser access	Yes	Yes
In service/Not in service	Yes	Yes
Page alarms	Yes	Yes
Email Notification	Yes	Yes
Configuration access	Yes	Yes
Remote telnet access	Yes	Yes
Persistent connections	Yes	Yes
Port mapping	Yes	Yes
Port-specific services	Yes	Yes
Year 2000 compliant	Yes	Yes
Security Features		
Network Address Translation	Yes	Yes
Network Port Translation	Yes	Yes
TCP SYN protection	Yes	Yes
TCP DoS protection	Yes	Yes
SSL support	Yes	Yes
Device Support:		
Maximum virtual servers	Unlimited	Unlimited
Maximum real servers	65,532	65,532
Device's role in the network	IP router	IP router
UDP-based service support	Yes	Yes
Misc.		
Overnight Exchange Unit	Service Contract	Service Contract
Free Email/Phone Support	Three Years	Three Years
Warranty on Hardware/Firmware	Three Years	Three Years

Power and Cooling Requirement

90 – 130VAC 2.5A or 190-235VAC 1.5A at 50-60Hz input power required. Absolute operating temperature range is 0-40C. Recommended operation ambient temperature not to exceed 30C. Max heat producing factor is 405 BTU/hr.

Network Overview

The WebMux has two modes, In-Path, or NAT (Network Address Translation) and Out-of-Path (Direct Routing) mode. Each mode has its advantage and disadvantages. Lets look the NAT mode first.
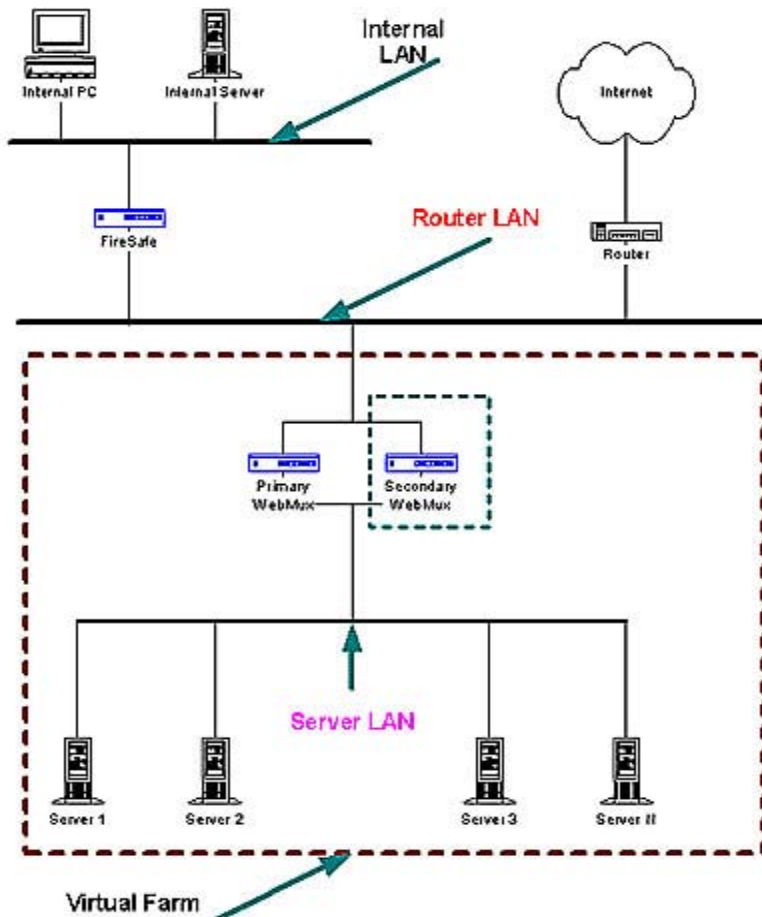

The main purpose of the WebMux is to balance the traffic among multiple web or other servers.   The diagram above shows an NAT installation with two WebMuxes. In this configuration, one WebMux is serving as the primary, and the other is serving as the secondary, or backup, providing a fault tolerant solution.

In order for the web servers to share the incoming traffic, the WebMux must be connected to the network.   There are two interfaces on the WebMux.   One interface connects to the **Router LAN**. This is the network to which the Internet router is connected. The other interface is connected to the **Server LAN**. This network connects all the web servers. The WebMux routes traffic between these two networks.

Next, a **Virtual Farm** or multiple farms must be configured on the WebMux. A virtual farm is a single representation of the servers to the clients. A farm consists of a group of servers that service the same domain, website or services.   For example, to configure a farm (or virtual farm) to serve www.cainetworks.com:

- First, Server 1 and Server 2 would each need the website www.cainetworks.com configured on them and HTTP/HTTPS services started, and

- Second, a farm on the WebMux is defined with Server 1 and Server 2 in it. The servers would be setup to either share the traffic, or setup as a primary server and standby server. In either case, if Server 1 goes down, then all traffic will be automatically directed to Server 2 by the WebMux.

In Out-of-Path mode, only one network in the setup, that is the server LAN, is connected to the Internet through the firewall and router. Internet traffic or local connections can both be directly sent to WebMux, which routes the packets to the proper server(s), then the server routes the return traffic back to the remote or local clients directly.
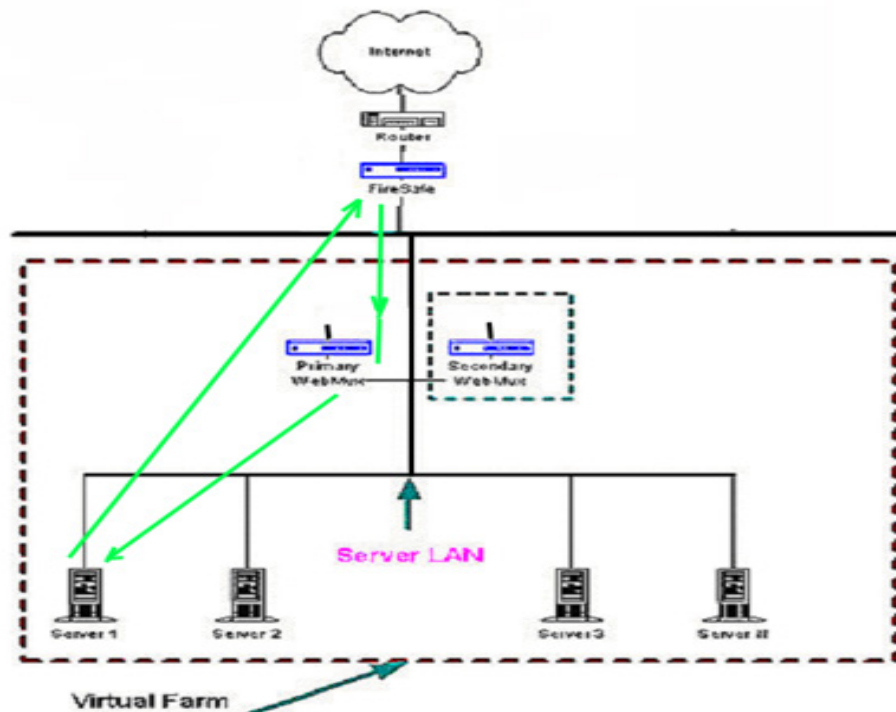
In most situations, the incoming traffic is in small requests, and return traffic from servers back to clients is large amount of data, pictures, or documents. Using direct routing will allow up to 100 times more traffic to be handled by the WebMux load balancer. The disadvantage for direct routing is that the firewall protections built-in to WebMux will no longer function. Users then must provide their own firewall for incoming and outgoing traffic.

Sample Configurations

Single WebMux
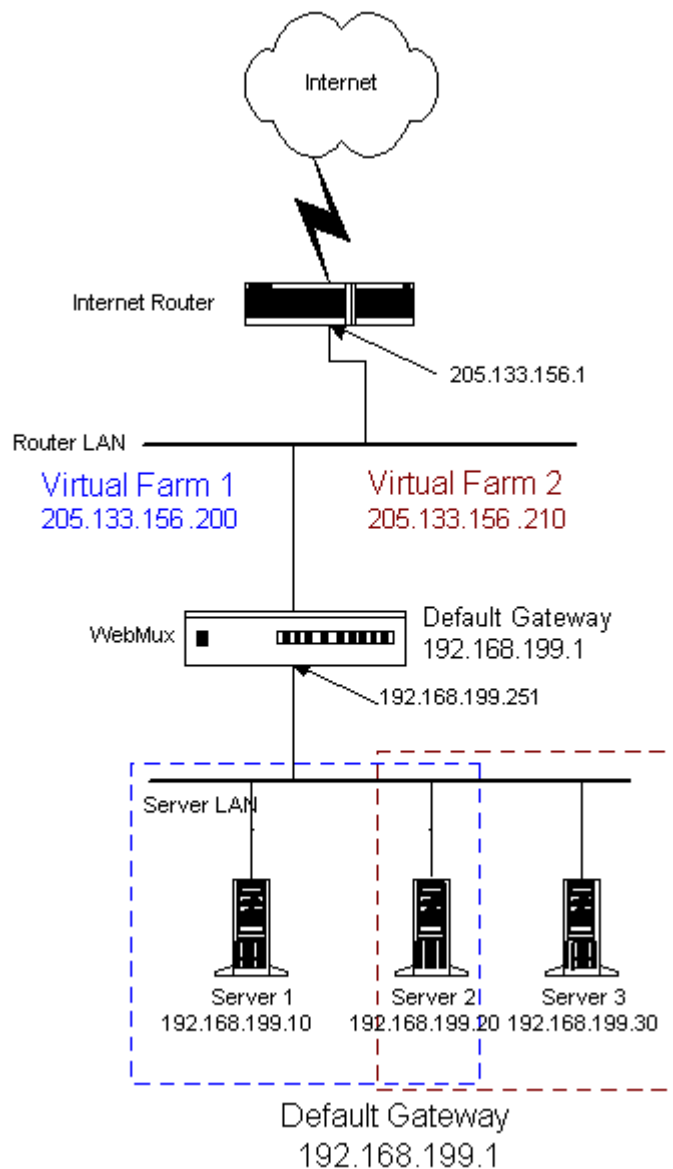
- This installation requires one WebMux.

- One WebMux interface connects to the Router LAN. The other interface connects to the Server LAN.

- The WebMux translates the Internet addresses to an internal non-routable class-C address. In this example, the netmask is 255.555.255.0. The IP address of the WebMux interface attached to the Server LAN is 192.168.199.251.

- The Default Gateway for all the servers is 192.168.199.1.

- Farm 1 IP address is 205.133.156.200. Servers 1 and 2 serve Farm 1.

- Farm 2 IP address is 205.133.156.210. Servers 2 and 3 serve Farm 2.

- Change to the server: made default gateway to 192.168.199.1, as well as the IP address to the 192.168.199.xxx address. If on the server there is a service attached to the IP address (HTTP/S, FTP, etc), please make sure the service will run on the new IP address.

Note: Although WebMux working with any IP address range, all server IP addresses should be Internet non-routable address so that the source address from the Internet does not conflict with the IP addresses on the Server LAN.

Note: If there is a firewall between the WebMux and the Internet Router, a rule must be defined in the firewall to allow the IP address of the WebMux interface on the Router LAN along with the farm IP address to communicate out to the Internet on all ports. If you are doing Network Address Translation of the farm address to a non-routable address, then both the farm address and WebMux interface address must be translated to communicate outbound on all ports.

Redundant Installation
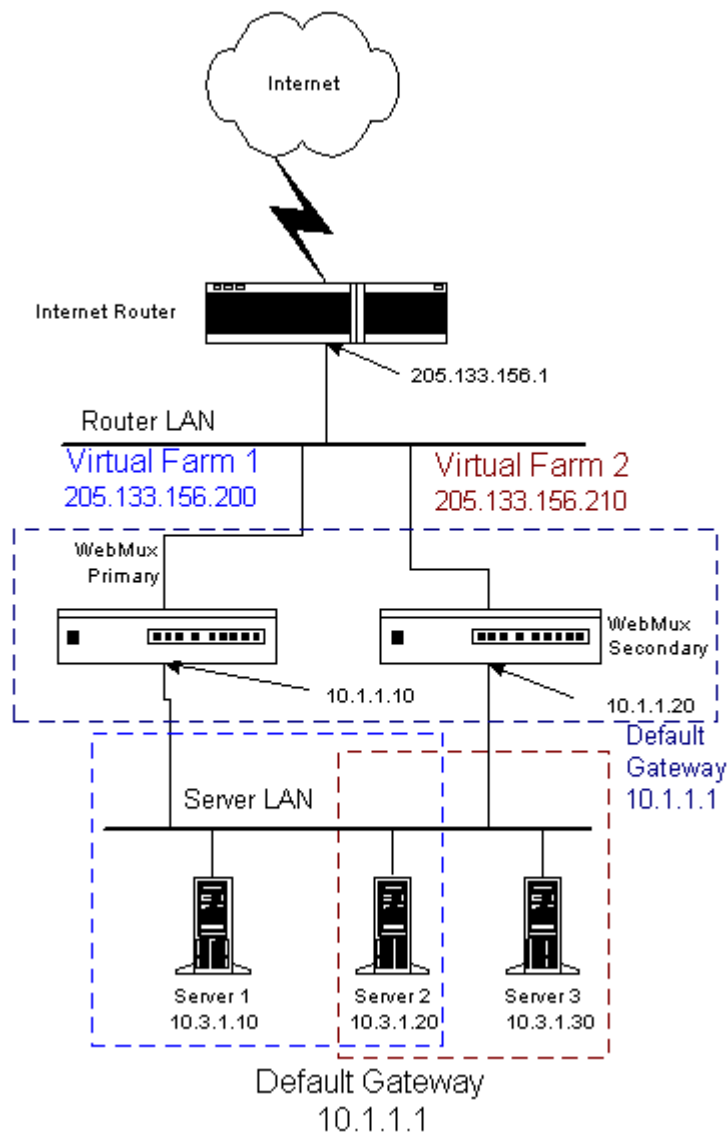
- The installation requires two WebMuxes. One will be the primary, and the other the secondary. They connect together with the Ethernet cable that is either cross-over or through a hub. The primary redundant interface IP address is 192.168.255.253; the secondary redundant interface IP address is 192.168.255.254. They can not be changed.

- Both WebMuxes connect to the Router LAN, and to the Server LAN. Each WebMux interface has a unique IP address.

- The registered Internet IP address range is a class C address range. The IP address of the WebMuxes' Virtual Farms must be in the same network range as the Internet router.

- The WebMux translates the Internet addresses to an internal non-routable class A address. In this example, the subnet-mask 255.0.0.0. The IP address of the WebMux interfaces attached to the Server LAN are 10.1.1.10 and 10.1.1.20.

- The Default Gateway for all the servers is 10.1.1.1.

- Farm 1 IP address is 205.133.156.200.

- Servers 1 and 2 serve Farm 1.

- Farm 2 IP address is 205.133.156.210.

- Servers 2 and 3 serve Farm 2.

- Change to the servers: made default gateway to 10.1.1.1, as well as the IP addresses to the 10.3.1.10/20/30 addresses. If on the server there is a service attached to the IP address (HTTP/S, FTP, etc), please make sure the service will run on the new IP address.

NOTE: Although WebMux working with any IP address range, all server IP addresses should be Internet non-routable address so that the source address from the Internet does not conflict with the IP addresses on the Server LAN.

Note: If there is a firewall between the WebMux and the Internet Router, a rule must be defined in the firewall to allow the IP address of the WebMux interfaces on the Router LAN in addition to the farm IP address (could be same as the WebMux Router LAN IP address) to communicate out to the Internet on all ports. Since WebMux doing Network Address Translation of the farm address to a non-routable address, the farm addresses on the WebMux interface must communicate outbound on all ports defined in the farms.

Installation without IP Address Change

Out-of-Path Mode:
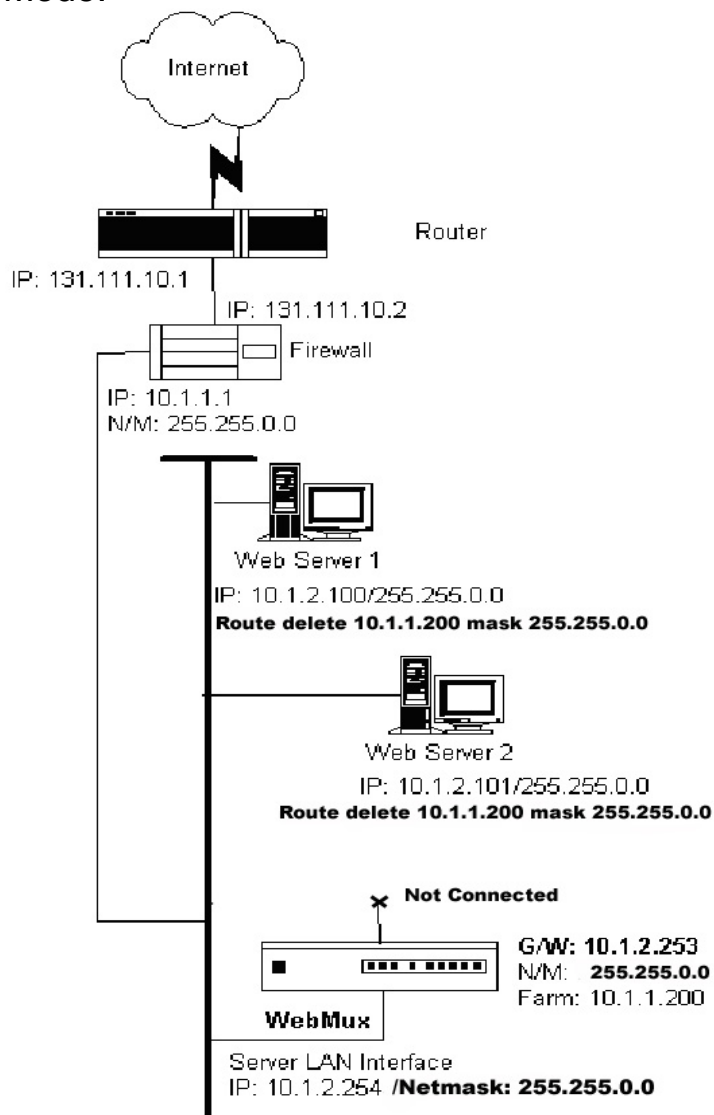
The above diagram is an example about how to configure the WebMux in out-of-path mode without changing the IP addresses of the web servers and other servers that already exist on the network. This is particularly helpful when the changing of an existing network of servers causes problems.

In this configuration, all the servers still remain on the same IP network, and can communicate. From the servers "view", the WebMux is on the same network as the servers. On the WebMux, only server LAN cable is connected, since there is only one network in direct routing mode. WebMux takes at least two IP addresses to work in this mode, server LAN Interface IP address and farm IP address.

Out-of-path mode also allows two WebMuxes to fully backup each other. Two WebMuxes connected to each other through a cross-over Ethernet cable.

Two simple changes must be made to each server in the farm. 1) To have a new loop back adapter installed and have its address set to the farm address. Do not set the gateway on the loop back adapter. Please refer to Appendix 1 and Appendix 2 for how to configure a loopback adapter, as well as how to remove the route from the servers. **Please note for Out-of-Path to work properly, the loopback adapter must route the return traffic through the real network interface. Please refer to Appendix 1 and 2 for more details on how to configure the loopback adapter on servers. In case the server running Windows 2003, the route created during adding loopback adapter cannot be deleted, please make sure loopback adapter has much higher metric.** 2) If your service is bind to any specific IP address, add the loopback adapter's IP address to that service.

The firewall configuration must be changed to point to the new farm address on the WebMux. Since WebMux always uses one IP address in the server LAN, the farm address must be a different IP address in the server LAN in Out-of-Path mode.

Before you Start

Please collect the information about names and IP addresses designated by the arrows in the network topology below.
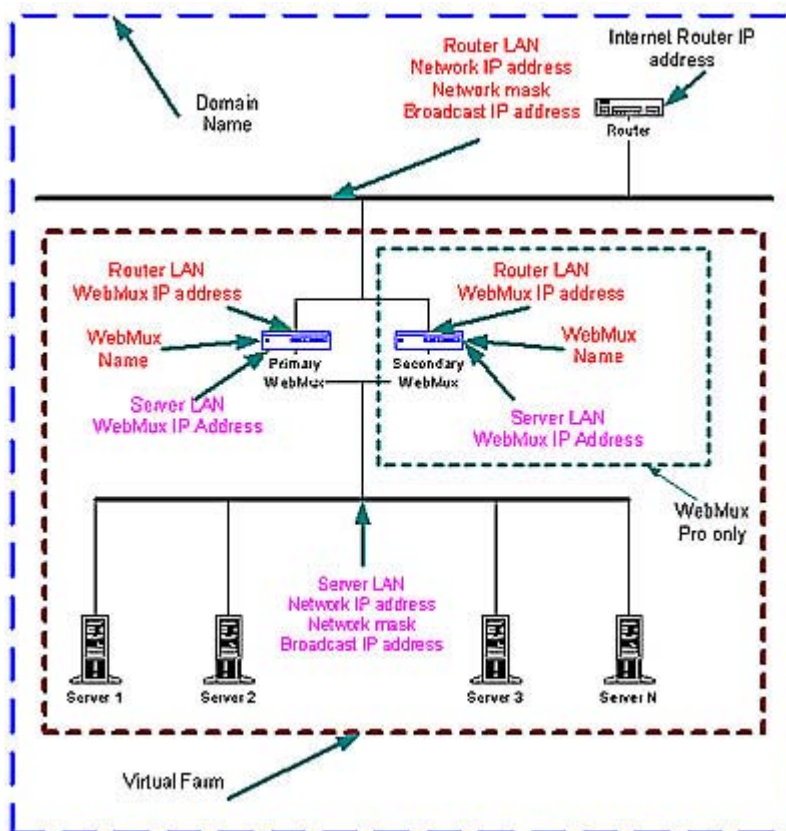
Network Terminology

A **Virtual Farm** includes the WebMux setup and the servers under it. Functionally, it acts as a single unit on a network. For example, http://www.cainetworks.com is one virtual server farm; https://www.cainetworks.com is another farm, and ftp://ftp.cainetworks.com is the third farm. The first farm works on a set of servers on port 80, the second farm consists of another set of servers on port 443, and the third farm works on a set of servers on port 21. Please note WebMux does support combining 80/443 ports as one single farm, so that same client browsing the site in HTTP mode will be send to the same server for HTTPS requests. In the combined mode, ports 80/443 will be combined into one farm.

To serve the Internet, there must be at least one **Internet Router.** This local area network that connects the router and the WebMux is called the **Router LAN**. In this LAN, the WebMux takes the Internet traffic and distributes it to the servers behind it. The LAN connecting WebMux and real servers together is called **Server LAN**.

In NAT mode, only WebMux boxes are connected to both **Router LAN** and **Server LAN**. At least one WebMux is needed to define the **Router LAN** and the **Server LAN**.

The side of the WebMux that connects to the **Router LAN** is to send and receive all the IP packets from the router to the Internet. The side of the WebMux that connects to the **Server LAN** is to send and receive IP packets to and from the servers in the farms. By properly configuring WebMux, one can create one or more Virtual Farms on top of physical hardware.

Hardware Setup --- Collect Information

- Make a drawing of the existing network and note all the configuration settings. This will help you to fall back to the existing configurations if needed.

- Make a new drawing for the new setup with the WebMux™ and the web farm in place. This will be used as a guide for setup and preparation of all the necessary material and equipment.

- Collect all the IP addresses, their network masks, network addresses, and broadcast addresses for the Server LAN and Router LAN WebMux interfaces. The IP address of the Internet router is also needed.

- Label all the cables. Prepare additional cables if needed.

- Make sure there are enough electrical or UPS outlets for all the new equipment.

Hardware Setup ---Setup the new network

- Power down all the devices on the network.

- If you have a secondary WebMux, connect the WebMuxes with a cross-over Ethernet cable.

- Connect the servers to the Server LAN

- Connect the WebMux(es) to the Server LAN

- Connect the WebMux(es) to the Router LAN (NAT mode only).

- Power up all devices in the network.

- Verify that all the devices are up and running.

- You are now ready to configure WebMux.

Hardware Setup ---Configuration Summary

**CAUTION: _Do not_ proceed without collecting all necessary information.**

- Turn on WebMux. Turn on the switch on the back of the WebMux and push the power-on button in the front momentarily. You will see the version number like this:

- After self-test, hold down the Check-Mark button on the WebMux until LCD displays the first question – "**Enter WebMux host name**".

- During the initial configuration, you will be asked to provide names and IP addresses. (See next section.) Each item is explained in the order it is asked.

- Answer the questions. Reboot. **Note:** When reboot is complete, the service statistics screen will appear.

- Run the Management Browser.

Initial Configuration

Enter WebMux Host Name:
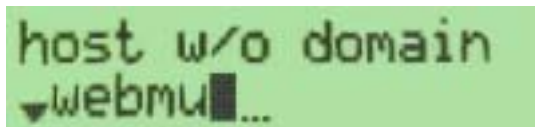
Enter the host name of the WebMux. Use the right arrow to move the position, the up and down arrows to select characters, left arrow to move back in position, check mark button to confirm the change. This host name is for identification purposes. You may call it webmux1, webmux2, etc. (Trick to enter name
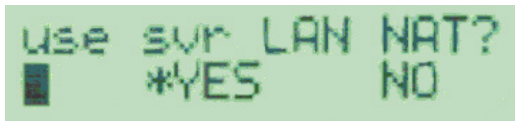
quickly: If you hold down the up/down button for more than a second, the letter will start changing quickly.) Note the left most down arrow on the LCD allowing user to skip certain entries.

Enter WebMux Domain Name:

```
domain
‡cainetworks.co█
```

This is for identification only, no effect for network operation. Although it can be any name, we suggest using the primary domain name of the Router LAN network. If you have only one domain, use that domain name. Note the left most position on the LCD has changed to an up and down arrow, allowing the user to go back and forth for questions and answers.
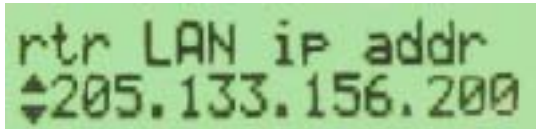
Choose NAT mode or Out-of-Path Mode:

```
use svr LAN NAT?
█    *YES    NO
```

This is where to choose NAT (Network Address Translation) or Out-of-Path mode. "*" is a default or selected option. Network address translation provides protection to the servers; it can handle large amounts of data as noted in the specification. It provides the best security for isolating servers from any other part of the networks.   Out-of-Path provides better performance when huge amounts of data need to go back to clients (up to 100X more than specification chart); it also does not require a change to the server IP address. If choosing NAT, continue to the next setting; otherwise, skip next few settings and go to direct routing. If answer NO here, please continue setup referring to page 21, the <u>Out-of-Path Setup Information</u> section.

NAT Mode Related Configuration

Enter Router LAN WebMux Proxy IP Address:

```
rtr LAN ip addr
‡205.133.156.200
```

This is the IP address that the WebMux uses as the external IP address when it functions as a proxy. This IP address can be used to setup the first farm. When any server behind the WebMux (on the Server LAN) initiates communication with another host, the WebMux substitutes the servers' IP address with this address. (This is true for all services, except FTP services, which use the FTP farm IP address for passive FTP connection).

Enter Router LAN Network IP Address Mask:

```
rtr LAN net mask
♦255.255.255.   0
```

This is the network mask of the Router LAN network. It is usually 255.255.255.0 for class C networks.

Enter Server LAN WebMux IP Address:

```
svr LAN ip addr
▮192.168.199.251
```

This is the IP address of the WebMux interface that connects to the Server LAN. This IP address must also be unique for each WebMux. This address must be different from the server LAN gateway address. The purpose of this IP address is to allow WebMux checking the network and server healthy situation. Even for the backup WebMux, this address must be unique. It is highly recommended to add this IP address to your servers /etc/hosts file, along with the gateway IP address, to allow faster name resolution, especially on Linux/Unix.

In an installation with a primary and secondary WebMux, one unique IP address is required for each WebMux interface that connects to the Server LAN. Those two unique IP addresses are in addition to the gateway IP address that is floating between the primary and secondary WebMux.

These IP addresses cannot be your Internet registered addresses. They must be Internet non-routable. For example, you can assign addresses in a 10.0.0.0 network address range, or a 192.168.199.0, etc.

Enter Server LAN Network IP Address Mask:

```
svr LAN net mask
▮255.255.255.   0
```

This is the network mask of the Server LAN. For a class A network, it may be 255.0.0.0. For a class C network, it may be 255.255.255.0.

Enter Server LAN Gateway IP address:

```
svr LAN gateway
♦192.168.199.   1
```

This IP address will be the Default Gateway entry for all the servers on the Server LAN. In an installation with two WebMuxes, if a gateway IP address of 10.1.1.1 is used, this address will 'float' between the primary and secondary WebMux. If the Primary went down, the 10.1.1.1 address will float to the backup.

In the single WebMux setup, this address CANNOT be the same as the WebMux IP interface address on the Server LAN. For the NAT setup, please continue to the <u>Common Configuration</u> section on next page.

Out-of-Path Related Configuration

Enter Server LAN WebMux IP Address:

```
svr LAN ip addr
▌192.168.199.251
```

This is the IP address of the WebMux interface that connects to the Server LAN. This IP address must also be unique for each WebMux. The purpose of this IP address is to allow the WebMux to check the network and server health. Even for the backup WebMux, this address must be unique. It is highly recommended to add this IP address to your servers /etc/hosts file, along with the gateway IP address, to allow faster name resolution, especially on Linux/Unix. Please also refer to Appendix for adding loopback to servers.

In an installation with a primary and secondary WebMux, one unique IP address is required for each WebMux interface that connects to the Server LAN. Those two unique IP addresses are in addition to the farm IP address that is floating between the primary and secondary WebMux.

Enter Server LAN Network IP Address Mask:

```
svr LAN net mask
▌255.255.255.  0
```

This is the network mask of the Server LAN. For a class A network, it may be 255.0.0.0. For a class C network, it may be 255.255.255.0.

NAT and Out-of-Path Common Configuration

Enter External Gateway:

```
external gateway
▌192.168. 11.  2
```

This is the common setup for both NAT and Out-of-Path modes. In NAT mode, the WebMux needs to know this to route the server replies back to the clients. Although in Out-of-Path mode this is not being used to route return traffic back to the Internet clients, WebMux does check the connectivity to the incoming side on this gateway or through this gateway to the ISP side routers.

Is this a Primary WebMux?

```
Primary webmux?
    *YES    NO
```

If this is the Primary, answer Yes. If this is the Secondary WebMux, answer No. The secondary WebMux automatically gets configuration information from the Primary once it sets up. If this is the only WebMux, answer Yes.

Primary WebMux Information

This question is not asked for the Secondary WebMux.

Is this WebMux running solo without a backup WebMux?

```
running solo?
     YES   ▌NO
```

If the Primary WebMux is running in a standalone configuration (see sample configuration – Standalone WebMux.), answer Yes. If you plan to add 2nd WebMux later, you may answer no.

Clear Allowed Host File?

```
clr alowd hosts?
▌    YES   *NO
```

Allowed host file prevents any unauthorized access to the WebMux Management Console. If a workstation's IP address is not in the allowed host file, that computer will not be able to reach the WebMux management console through the network. However, sometimes a wrong IP address is entered so that no computer can access the browser management console. At that point, clearing the allowed host file will allow any browser to access it. By default, the allowed host list is empty so that any IP address can access WebMux. We do encourage adding only host IP addresses that you do allow to manage WebMux into the list. See configuration through browser interface for more details.

Remake /home/webmux/conf/passwd?

```
remake passwds?
     YES   *NO
```

This function is provided in case you have forgotten the passwords to access the **Management Console**. Please use a browser to access Management Console for normal password changes. The factory default password is the same as login ID on the screen. Answer Y to reset the Passwords to factory default. Answer N to leave them unchanged.

Enter Admin http Port Number:

```
http admin port
█
................24
```

This is http port number for accessing Management Console in non-secure mode. Any unused port number can be used. Factory default port number is 24, one could choose to use any unused port below 10214 or port number above 1024 for this. Using port number above 1024 will need to setup an admin farm. This farm is for preventing port collision in case passive FTP is one of the farms. Using port number below 1024 will not need to setup this farm.

Enter Admin https Port Number:

```
https admin port
█
..................35
```

This is the https port number for accessing Management Console in secure mode. Factory default port number is 35, one could choose to use any unused port below 1024 or port number above 1024 for this. Using port number above 1024 will need to setup an admin farm. That is for preventing port collision in case passive FTP is one of your server farms. Using port number below 1024 will not need to have this farm.

Discard Changes Made?

```
discard changes?
▲   YES   *NO
▼
```

User can select Yes at this point, all the changes made will be discarded. By default the answer is NO, all the change will be saved to internal solid state storage. Changes will take effect after next reboot.
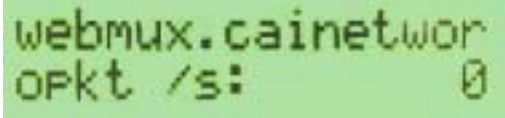
The next question will be **Reboot Now?**
Reboot now?

```
reboot? (hold ✓)
▲
▼
```

This is the end of initial configuration. Most of the setup or changes require a reboot to take effect. Press and hold the center Check-Mark button to make the WebMux reboot. User UP arrow button to "Discard Changes" and "Yes" to exit without change.

```
REBOOT...
```

After the WebMux is rebooted, the statistics of the incoming package, outgoing package, etc will be displayed on LCD periodically.

```
webmux.cainetwor
opkt /s:         0
```

What if I made mistake in my configuration?

One can always make changes to the hardware settings by press the Check-Mark button for three seconds when the statistic screen showing. It will start the prompt questions which will allow the user to navigate from one prompt to another by using the up/down button on the left most LCD position. For example, if you configured the Allowed Hosts wrong and lock yourself out, you can go to the push buttons and select "Clr Allowed Hosts" option, save changes and reboot, which will allow all the IP address to access the management console through browser. You can clear the allowed hosts but not reset the password, or change one option and not change the others.

Management Console

After the Initial Configuration, user should be able to connect a web browser to the WebMux. The web browser does all of the WebMux management. The following sections explain each of the easy to use management console screens.

- Login
- Administration Setup Page
    - Change Password
    - Set Clock
- Status
- Add Farm
- Modify Farm
- Add Server
- Modify Server

Login

Start Login Page:
- Start a web browser from your management workstation.
- Set URL to **http***://webmuxip:webmuxport/***cgi-bin/login**
    - **webmuxip** is the IP address of the WebMux on the server LAN.
    - **webmuxport** is the management port address of the WebMux. The default ports are 24 for an unsecured connection, and 35 for the secured connection. Use https instead of http on the URL line if you decide to use port 35 for secure communications.
- The following login page will appear.

Note: In order for use a browser to manage the WebMux, the browser must be set to accept all cookies.

User ID:

There are two preset user IDs

- **Super User** - Allows access to all screens and functions provided by the WebMux.
- **WebMux** - Does not allow the user to access or change any settings viewing only (Firmware version prior to 5.8.09 allowing farm changes).

Password:

Fill in the correct password for the selected User ID. **The password is case sensitive.**

The default passwords are:

| ID	Password
superuser	superuser
WebMux	webmux

It is recommended to change the passwords periodically. No new user ID can be added.

Login:

After entering the correct password, click Login.

Note: For first time setup, please login as **Super user** and go to the Administration Setup by clicking the **Setup** button. It is important to set up the Server Farm Gateway IP address and network mask first.

Main Management Console
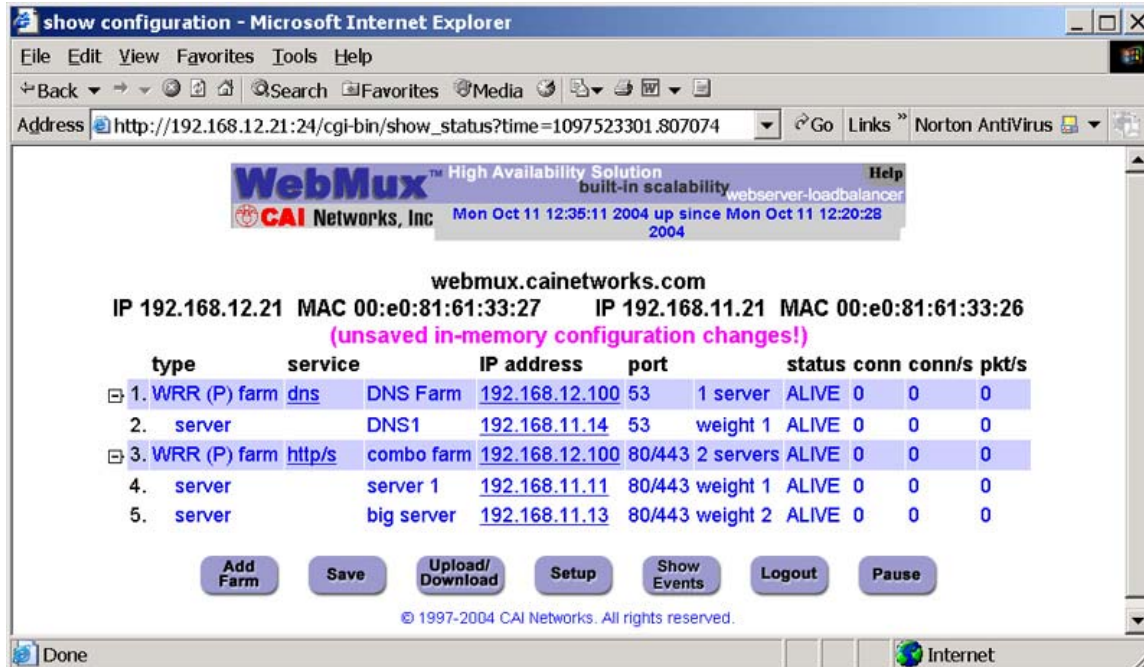
Once logged into Management Console, this main screen will show. To continue configure WebMux, normal steps are:

> Click on the "Setup" button to change administration and setup related information;
> Click on "Add Farm" button to add a server farm at a time;
> Click on the "IP address" portion of the farm display to add servers;
> Click on "Save" button to save the farm/server configuration.
> Click on "services" on each farm to adjust the timeout for each kind of services. Note that same protocol services between farms will share the same timeout value.

Add Farm

Click **Add Farm** to add a virtual web or FTP site. The "ADD FARM" screen will appear. Please see that section later for details.

Save

Changes made to the "Farm" and "Server" will take effect immediately. The changes however are not saved permanently to the flash memory until the "Save" button is clicked. Unsaved farm/server settings will be lost during power outage or WebMux reboot.

Download/Upload

This button will allow user to save and restore the WebMux configuration to and from their management workstation. See later chapter for details.

Setup Button

This button brings up the "Administration Setup" page. "Super User" login is required to access this page. See related section later for details.

Show Event

This button will display all the events since WebMux last reboot. The event includes server failure or state change.

Logout

It is not recommended to leave the management browser login unattended. Click the **Logout** button to close the session. The "Login" screen will re-appear.

Pause

The status screen automatically refreshes frequently to provide most up to date status. You can use the **Pause** button to freeze the auto refresh.

Resume

After the **Pause** button being pushed, the button will change to **Resume** and the auto refresh stopped. Click the **Resume** button to restart the auto refresh.

Adjusting Timeout for Each Service

Click on the service type of each farm will allow you to change the timeout value of layer 7 testing for each different service. Please note this change is global that will affect all the farms using the same type of service. For example, the default timeout for checking HTTP protocol alive or not is 5 seconds. If web server does not respond to the WebMux protocol chat within 5 seconds, WebMux will declare that server is dead and switch that server out from service and notify the operator through email or pager. However, if your web server did not really dead but for some reason not responding to the checking request, WebMux would false alarm. To avoid this, user can change the timeout value to a larger value. Many times, servers can not resolve the IP address for the back end of WebMux IP address could cause server not responding to WebMux's protocol checking. Adding the WebMux server LAN IP address and server LAN gateway address to the name resolution table will help resolve this problem. Please read the Q&A section for more information.

Administration Set Up

After login as superuser, click on the setup button, you will come to this screen:

Allowed remote host IPs:

The WebMux management console and diagnose login only allow logins from these IP addresses to establish a management session. You can access from more than one IP address by specifying all the allowed IP addresses separated by a ":". Netmask following the IP address specify the range of hosts can access management console. For example, 192.168.12.0/24 will allow all hosts in 192.168.12 network to access it. If this field is left blank, you can access the management software from any IP address. It is recommended to set this up for security reasons. When wrong IP address entered, management console login will not be possible. Use push button on WebMux to clear the allowed host list. This field is blank by default.

Dialout prefix:

Some phone systems require a prefix for outside phone numbers. If a prefix is required, enter it here. Leave it blank if a prefix is not required. For most Analog PBX, this will be "9". Do not enter anything in here, if modem is not connected.

Pager phone numbers:

This is the pager phone number to be dialed when an abnormal condition occurs. Enter the number without any of the special characters or spaces. It should be in the format of a single long integer. Add 1 and the area code if needed. Do not use "()" or "-" or blank spaces. Do not enter anything in here, if modem is not connected.

Server for email notification:

In addition to paging, the WebMux can send email notifications. Enter the IP address of the email server that will forward the notifications. Please note: Because the WebMux does not resolve names, this entry must be an IP address. Changes to the email server allowing WebMux relaying messages is necessary.

Addresses for email notification:

Enter the email addresses to be notified. Separate multiple addresses with a colon. For example: johndoe@anywhere.com:janedoe@anywhere.com

Server gateway IP address:

The WebMux appears to all the servers in the farms as a gateway or router. This is the IP address for WebMux assuming the router role for the servers. This address should be the gateway IP address in the web (or other) servers. It is highly recommend adding it to the /etc/hosts file on your servers.

> **Please note**: For first time setup, it is very important to set up this address and the Server Farm network mask (below) first. Also when setting up the servers, you may be asked to fill in the default gateway IP address for the server. Use this IP address to setup all the servers under it. The WebMux will not function properly if this IP address is not set correctly for both WebMux and the servers.

WebMux http control port:

Since WebMux load balancing incoming HTTP traffic, the HTTP port for the management console must be set to a different port. By default, the port is 24. You can change the port, if so desired. Front push button can also change this.

WebMux https control port:

Since WebMux load balancing incoming HTTPS traffic, the HTTPS port for the management console must be set to a different port. By default, the port is 35. You can change the port, if so desired. Front push button can also change this.

WebMux diagnostic ports:

The WebMux allows diagnostic sessions from remote access for factory technical support or trained network engineers through ssh or telnet. Access is also subject to the restriction of the "Allowed-Host" setting earlier. "superuser" can login with its password using "ssh" to run certain diagnostic tools (help shows the commands, how to use these commands are not supported). When this entry is blank, any diagnostic access is denied. This entry should remain blank under normal operations. Default port numbers are 77 / 87. The first port is ssh and second is telnet. If only one port specified, only ssh login is possible. You will need to notify us the port numbers before obtaining support from us.

Connection warning threshold:

The WebMux monitors the number of connections established. When the number of connections is greater than the value entered, the WebMux will page the designated numbers. For example, if a DoS attack is occurring, the number of connections to the site would be extremely high. Assuming they exceeded the value set for the "connection warning" threshold, the designated numbers would be paged.

Least significant bits in client IP address to ignore for persistent connections:

This feature allows persistent connections to be handled properly when communicating with America Online's bank of cache servers. With AOL's cache servers, the IP address of the cache server becomes the source address. Since an end user can be send through multiple cache servers; it is possible the requests for one HTML page being routed to different web servers in the same session. Therefore, applications, such as shopping carts, that require persistent and secure connections will not work properly. This feature will treat multiple cache servers as one source, thus WebMux can properly handle the persistent requests from browsers. From customers' feedback, number three (3) is good enough for most AOL requests.

The WebMux will use the entry to determine how to load-balance the traffic. It calculates based on two to the power of the entry as the number of IP addresses

to combine.   When too large a mask applied, it will defeat the load balancing function of WebMux.

ICMP Packet input policy:
- **Accept:** The WebMux will allow all ICMP packets to travel through the WebMux. For CLI arp commands working properly, this must be accept.
- **Deny:** The WebMux will NOT allow any ICMP packets to travel through the WebMux.

> **Note:** During installation, having the ability to PING the other hosts on the networks is typically useful.   When the installation is complete, setting the "ICMP packet policy" to DENY, is recommended as a security precaution.

Forward Policy:
- **Accept:** The WebMux will route IP packets both directions. WebMux will not act as a firewall in this mode.
- **Deny:**   The WebMux will NOT allow any incoming IP packet traveling through the WebMux, except IP packets in farm IP/port. This is the default setting.

Front Router Connection Verification:
It can be "none", "ARP", "TCP Connection", or "ping". Depending on the front end router, this can be changed. For example, most Cisco routers will talk to WebMux through ARP and TCP Connection; however, most Cisco DSL modems will only talk to WebMux through Ping. The change to this verification method will take effect after WebMux being rebooted.

Front Router Connection Verification IP Address:
It can be the router in front of the WebMux, or a router in your ISP's WAN. It is recommended to have the router IP address as the verification IP address. However, it can be any address that is reachable on your Internet side.

Persistence Timeout:
WebMux will keep track the browser connections if the persistent farm is defined and accessed. Within the timeout time period, WebMux will send any request from the browser IP address to the same server. Our survey shows 5-6 minutes is the best value for most cases. The larger the persistence timeout value, the less chance user connection get lost. However, by keeping a lot of connections in the WebMux memory, the maximum number of concurrent connections will drop.

Outbound Connection Timeout:
WebMux keeps track the outbound connections. This outbound proxy function provides communication tunnels for servers behind it to talk to other computers on the Internet side. This type of connection is different from the connections

from outside through server farms to the servers. After the connection closed from the servers to the outside computer, it will wait this timeout minutes before it removes that from the tracking table. Setting this too long will cause WebMux allocating too much memory, thus reduce the memory for other functions. The default value is 15 minutes. This function has no effect in Out-of-Path mode.

Server Scan Mode:

WebMux talks to the real servers in the farm through the layer 4-7 protocols every few seconds. This is important process for monitoring servers' health situation. If there are a lot of farms and a lot of servers, WebMux may not be able to get around checking all the servers in few seconds. In concurrent mode, WebMux will start multiple protocol scanners to chat with servers concurrently. Concurrent mode uses more memory, may have other side effect. For most setups, sequential scan is recommended.

URL for Custom Service Check:

Sometimes WebMux built-in server health check is not enough for the special needs. When one ASP/JSP server's output is depends on the database server and database server connection is down, one might want to redirect the traffic to a different server, or make the ASP server out of services. To accomplish that, WebMux allows a farm being set using a "service" called "custom defined TCP service". It will then call the CGI's URL on the server defined in this field. This will involve a custom developed CGI code by your software developer on your server and place it on the path. Upon success the page should return HTTP response code 200 and a plain text page beginning "OK". The URL is truncated to 255 bytes (to be a string of at most 256 bytes with a terminating null). The response from the server must fit in 4k, including all non-display tag and headers etc. This custom CGI code must complete within 15 seconds or the server considered dead. Please see appendix 5 for sample code.

UDP NTP Time Server IP Address:

From version 5.4, WebMux can sync its internal clock with any UDP NTP server. By default it points to a tier 2 NTP server. You can also set it to your Internet NTP server, or wipe out the entry to not sync to any NTP server.
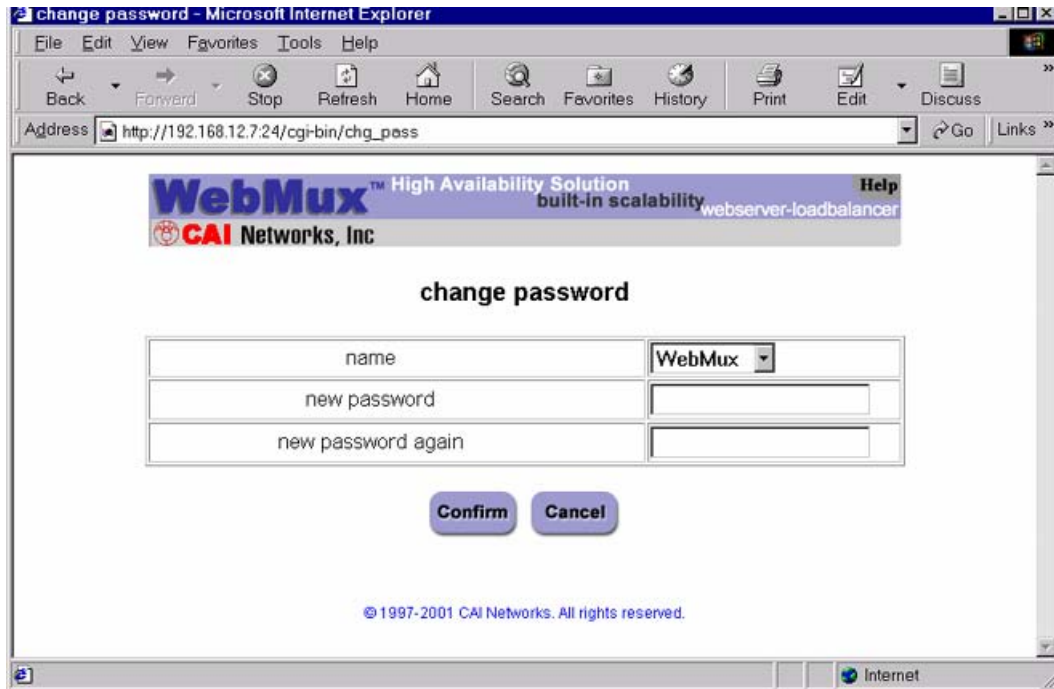
Reset Stranded TCP Connections:

When a server failed to function, there could be many TCP connections still in TCP_WAIT state. If this set to "Yes", when client tries to access the failed server, WebMux will pretend the server sending TCP Reset to the client, thus free all the TCP_WAIT state connections. By default this setting is "No" to be consistent with prior versions.

Reboot:

Changes to "server gateway address", "server farm network mask", "WebMux http control port", and "WebMux https control port" requiring a reboot for the new

configuration to take effect. You can use the **Reboot** button to reboot the WebMux remotely.

Change Browser Login Password:

Name:
Select the login name for which the password is to be changed.

New Password:
Enter the new password. This is the password to which the login will be changed.

New Password Again:
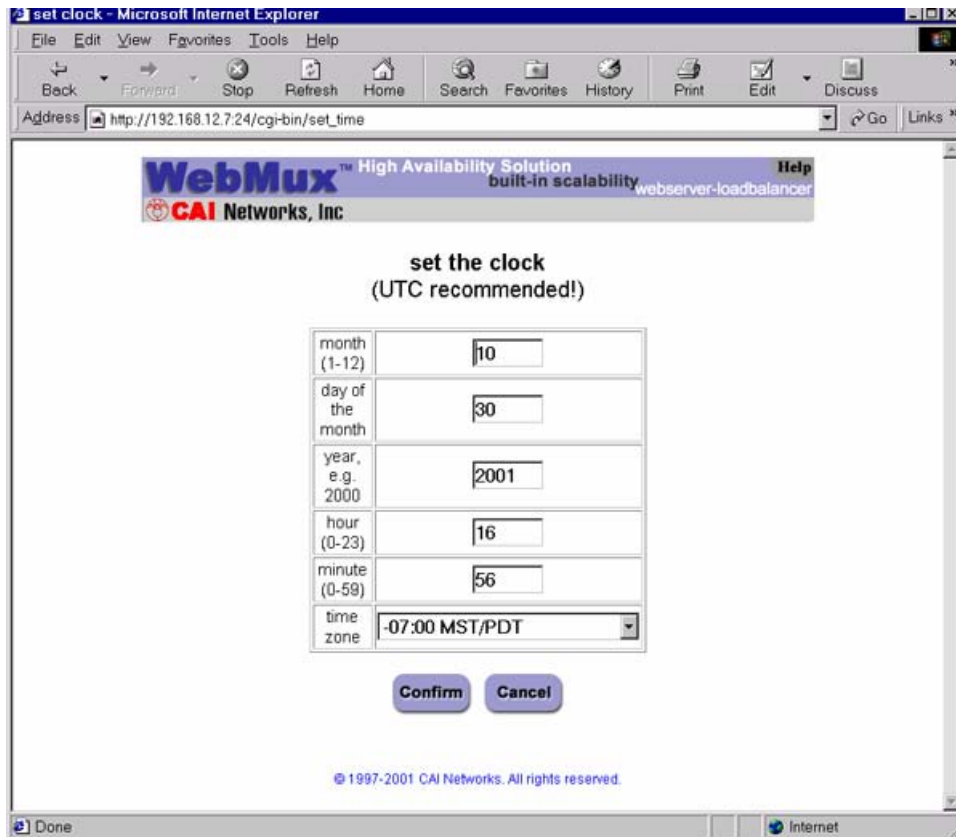Enter the same password as in the previous box.

Confirm/Cancel:
Click **Confirm** to execute the change. Click **Cancel** to return to the previous screen WITHOUT changing the password.

Change PIN:

To protect WebMux from unauthorized change from front push buttons, a PIN can be entered here to prevent saving any change from the front panel. By default, there is no PIN.

Set Clock:

Click this button to go to the "Set the Clock" page. The time and date of the WebMux then can be set. Please note that WebMux internally uses GMT time zone, not your local time zone, per W3C/HTTP protocol. If the timezone did not set correctly, the browser access could be denied, due to "cookie" time out.   If the UDP NTP server setup correctly, there is no need to set clock any more, since WebMux automatically sets its clock periodically.

Month:
Enter the number of the month, 1 through 12. Leading zeroes are not necessary.

Day of the Month:
Enter the day of the month, 1 through 31.

Year:
Enter the year. Enter all 4 digits.

Hour:
Enter the hour of the day. Use the 24 hour clock, or military time.

Minute:

Enter the minute of the hour.

Note: The recommendation is to set the WebMux clock to UTC (GMT) time.
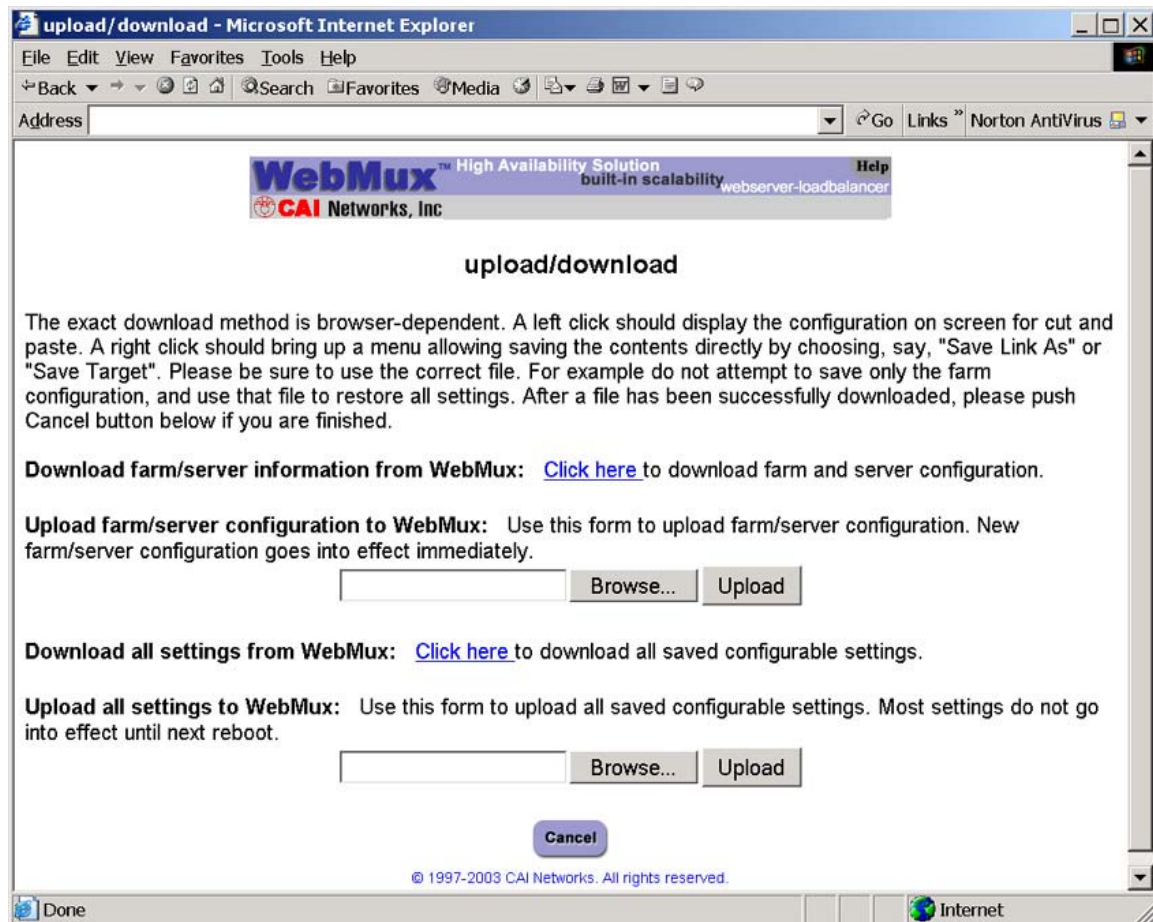
Time Zone:
Select the time or hour offset to the UTC (GMT) time. You can set WebMux to your local time, if your time zone is selected here.

Confirm/Cancel:
Click **Confirm** to execute the date and time change. Click **Cancel** to return to the previous screen WITHOUT making any date or time changes.

Upload/Download

Download:
This feature allows the SAVED (not necessarily the active) configuration to be saved at the Administrative Browser workstation. Click on the **Click Here** to display the configuration. Choose 'File->Save As' from the browser menu to save it as a text file. Changes can be made to this file and uploaded to the WebMux without changing the first comment line.

Upload:
Upload allows a configuration file that has been saved at the browser workstation to be uploaded to the WebMux. Enter the full path of the configuration file, or click on **Browse** to search for the file**.** Click **Upload** to upload the file to the WebMux. This file will IMMEDIATELY become the saved and active configuration. Upload ALL Settings to WebMux will actually upload settings including IP address and farm setups. If you want to replace WebMux with a new unit, you could save the configuration and upload all settings to WebMux, so that you do not need to go through step by step configuration (require both WebMuxes on the same firmware revision).

Add Farm
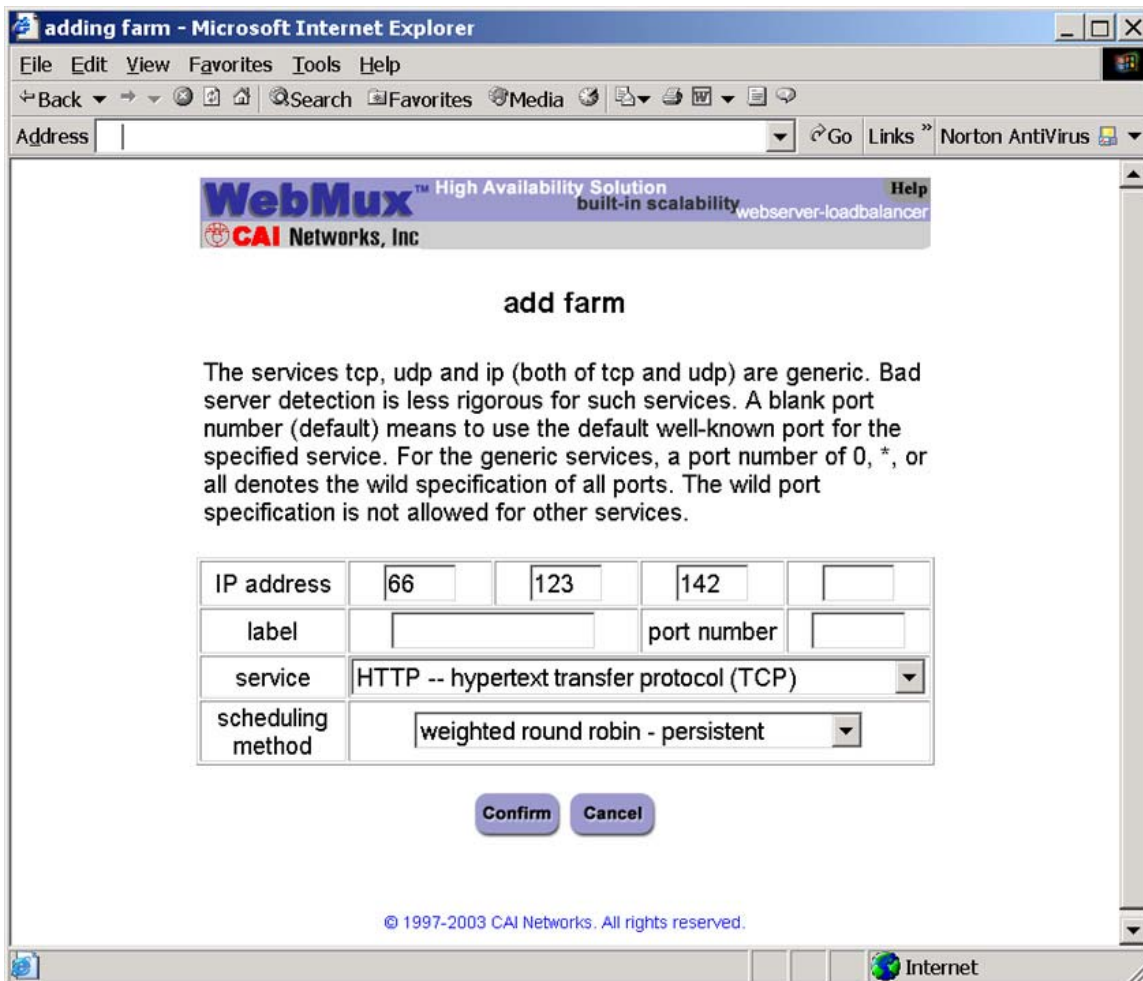
Farm IP address:
This is the IP address of the new farm.

The farm address could be the Internet known address or the address has been translated by your firewall. For example, if you want to create an http farm for www.yourdomain.com, the farm IP address will be the IP address for www.yourdomain.com from your DNS record. If the IP address of www.yourdomain.com is 205.188.166.10, then the Farm IP address is also 205.188.166.10. The WebMux will then translate the farm address to the web server address in your DMZ or internal network.

From version 4.0.3, we also introduced "label" for the farms and servers. Once the label is being specified, WebMux will display in the Show-Status screen the label for the farm and server, instead of the IP addresses. Although labels can be anything, it is better to have meaningful and unique label for each farm or

server. From version 5.6, name label also being used to check HTTP layer 7 protocols as part MIME header in virtual hosting. The format of the farm name label will be www.xyz.com, max length 75 bytes. If the server returns error code 401, WebMux consider that server dead. For both IIS and Apache servers doing virtual hosting, farm name label must be an existing web site name on the server. For more information on Virtual hosting, please go to Appendix 4 for details.

In NAT mode, if you use WebMux for your intranet, then the farm IP address will be the IP address of the original web or application server. The IP addresses of the original web or application servers must be changed so that the WebMux can translate farm IP address to the server IP address. You can use WebMux Router LAN IP address as your farm address. You can add multiple farms to this IP address, as long as the port number is different. So you can save real IP address. In this mode (NAT), WebMux acts as a firewall also. All servers behind WebMux can reach to the outside through WebMux. From outside, the traffic can be seen all come from WebMux router LAN IP address, or proxy address. If a WebMux is placed behind a firewall, please consider the rules for proxy address. All farms IP addresses should have rules to allow incoming traffic to the address and port number, as well as return traffic for each farm IP address from any port to anywhere.

In Out-of-Path mode, farm(s) must be a different IP address than the WebMux Server LAN IP address. At this mode, only server LAN cable is connected. Multiple farms can be added to one IP address, as long as the port number is different from each other. In this mode, each server must add a loopback adapter and under Windows server, the route for the loopback adapter must be removed. Please refer to Appendix 1 and 2 for more detailed procedures. WebMux has been tested extensively working with all versions of Windows, Linux and HP-UX 11.X under this mode. Other OS should also working fine.

Caution: Once a new farm is added, the IP address of the farm cannot be changed. To correct the IP address, the old farm has to be deleted and a new one to be created.

Port:
This is the port number for the farm. If you are choosing one of the known services below, you do not have to specify anything in this field. However, if the service you choose is not listed in the list below, you will need to specify a port number here. For example, for MS Terminal Services, use port number 3389.

Service:
This is the service of the new farm. Select a service type to create a farm using its well-known port. If a port other than a well-known port for TCP or UDP service is to be used, then choose one of the "Generic" selections, and enter the port number in the PORT NUMBER box. No port number needed to be specified, if the service protocol is on the list. WebMux has level 7 protocol checks for the

known ports in the list. For Custom Defined TCP Service (custom health check), please specify the URL for the CGI code in the setup screen.

Caution: Once a farm is created, the port number cannot be changed. Like the IP address, the old farm must be deleted and a new one created, in order to change farm settings. Please choose "Generic TCP" and specify port number, if service is not listed below. If multiple ports to be used, please also select "Generic TCP" and specify port number "0".

| Service	Well-Known Port#
DNS – Domain Name Service (TCP)	53
FTP – File Transfer Protocol (TCP)	21
HTTP – Hypertext Transfer Protocol (TCP)	80
HTTPS – Secure Hypertext Transfer Protocol (TCP)	443
HTTP/HTTPS Combined Ports	80/443
NTP – Network Time Protocol	123
POP3 – Post Office Protocol	110
SMTP – Simple Mail Transfer Protocol (TCP)	25
Generic TCP	User Specify
Generic UDP	User Specify
Generic TCP/UDP	User Specify
Generic no port scan (TCP)	User Specify
Generic no port scan (UDP)	User Specify
Generic no port scan (TCP/UDP)	User Specify
Custom Defined TCP Services	80 or User Specify

Scheduling method:

The scheduling method is the way in which traffic is distributed among the servers in the farm. Eight different methods are supported. If you are using a shopping cart service, a persistent scheduling method is recommended.

- Least connections
- Least connections - persistent
- Round robin
- Round robin - persistent
- Weighted least connections
- Weighted least connections - persistent
- Weighted round robin
- Weighted round robin – persistent
- Weighted fastest response
- Weighted fastest response - persistent

Modify Farm

Modify farm can be invoked from the Status screen by clicking on the farm IP addresses or labels.
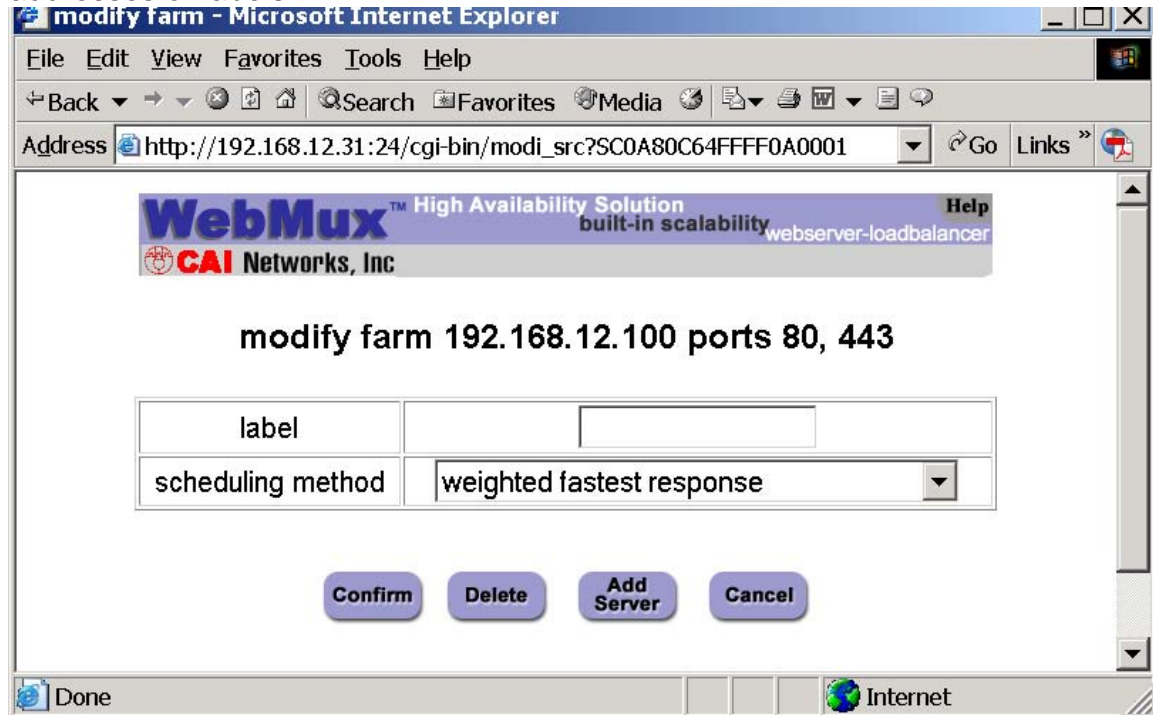
Farm IP address and port number:

These numbers are displayed here for reference purposes. These fields are set in the "Add Farm" screen. Once set, they are not changeable. If they must be changed, delete the farm and then add a new one.

Label:

The label field can be changed to make it fit better for describing the farm. Change this will not affect how load balancing works.

Farm scheduling method:

Eight different methods are supported:

- Least connections
- Least connections - persistent
- Round robin
- Round robin - persistent
- Weighted least connections
- Weighted least connections - persistent
- Weighted round robin
- Weighted round robin – persistent
- Weighted fastest response
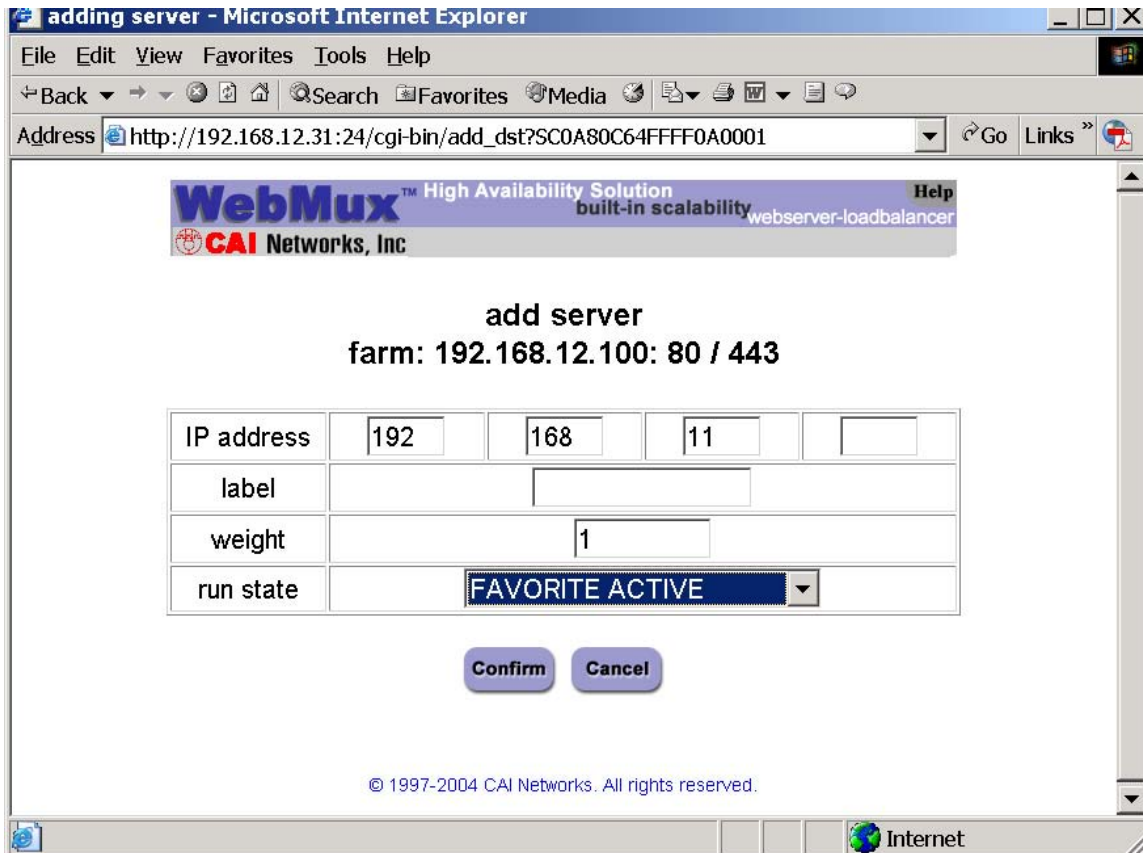- Weighted fastest response - persistent

Delete:

Click this button to delete the entire farm.

CAUTION: This function also deletes **ALL** the servers under this farm.

Add Server:

Click this button to add a new server to this farm.

Server IP Address:

This is the IP address of the server to be added.

From version 4.0.3, WebMux allows adding label next to each server's IP address. The purpose of labeling a server is only for helping name the server in the farm. It has nothing to do with the name resolution of the server. Although label can be anything, it is always better to have meaningful and unique label for each server.

CAUTION: Once the server is added, the IP address cannot be changed. To correct the IP address, the server must be deleted and a new one be created.

Server Port Number:

Enter the port number of the server to be added.

> **CAUTION:** Like the IP address, once created, the port number cannot be changed. To correct the port number, the old server needs to be deleted and a new one to be created.

Weight:

Scheduling priority weight. Valid integer numbers are between 1 and 100. A server that has a weight of 2 will be directed twice as much traffic as a server with a weight of 1.

A special zero weight setting is provided for a graceful shut down of a server. When the weight is changed to zero, the WebMux will not send new connections, but will maintain all current connections to the server. The connections will gradually reduce to zero as current clients' sessions terminated. When there are no connections, the server is functionally "dead" or off line until the weight is changed back to a valid number. Then the server can then be shutdown or taken out of service without affecting any users.

> **Caution:** Unlike a server that can go down unexpectedly, the WebMux will not move a STANDBY server to ACTIVE when one or more server's weight is set to zero. If the weight of all the servers in a farm were set to zero, then the farm would be "down" because none of the servers are accepting new connections.

Run State

- **Active -** The server will be put into service immediately after it is added. However, once it is failed, it will stay Standby mode, until manually set its run state to Active again through the browser interface. This will give system administrator time to fix the system or reboot the server once some software/hardware update is going on.
- **Favorite Active** – The server will be put into services immediately after it is added. If a Favorite Active server failed, once it is operational, WebMux will automatically put it back to the Active state.
- **Standby -** The server will be put into STANDBY, or backup, mode after it is added. The WebMux will change a STANDBY server to ACTIVE when one or more ACTIVE servers fail.
- **Last Resort Standby –** The server will be put into STANDBY state, unless all other servers are out of services, this server will not be switch in. This will allow the last server to show a different web page from others.

Modify Server

Modify Server can be invoked by clicking on the server IP address on the Status screen.
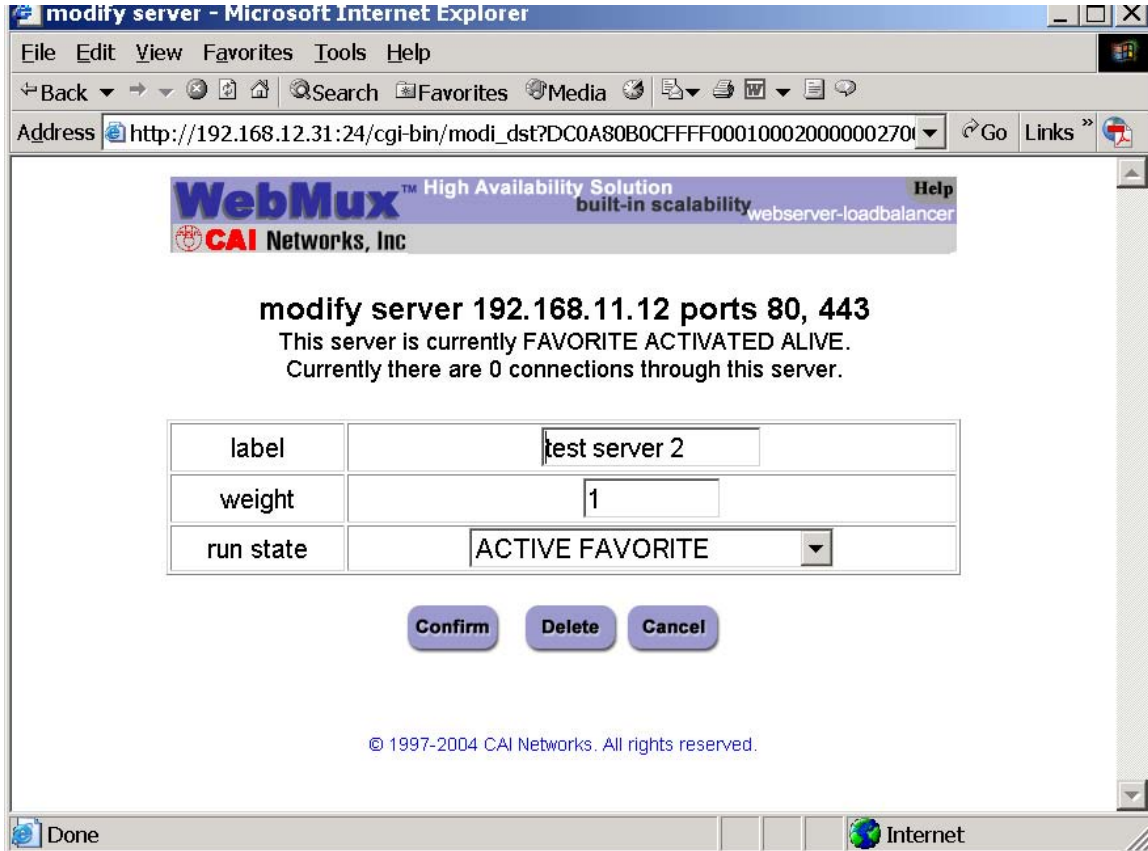
Destination server IP address and port number:

These parameters are set in the "Add Server" screen. Once set, these fields cannot be modified. To correct this setting, delete the server and add a new one.

Label:

The label can be changed at any time. The change will not affect how server is performing in the farm; rather it is for description purpose only.

Weight:

Scheduling priority weight. Valid integer numbers are between 0 and 100. Change weight to zero will quite the incoming connection while all existing connection continues until time out or connection terminated by client and server. Although all number from 1 to 100 will allow traffic goes through, using a smaller number of weights in each server will have best load distributing result.

Running state:
- Active
- Favorite Active
- Standby
- Last Resort Standby

Initial setup change Through Browser

Sometimes users like to change the basic settings for the WebMux through browser interface, for example, when WebMux located in a hosting center across the country. If one has information about the WebMux current basic settings, one could change those parameters through browser. On the browser, enter the following URL:

https://webmux_ip:webmux_manage_port/cgi-bin/rec

For example, if your webmux IP is 192.168.12.1, and your webmux_manage_port is 24, your URL will be
http://192.168.12.1:24/cgi-bin/rec
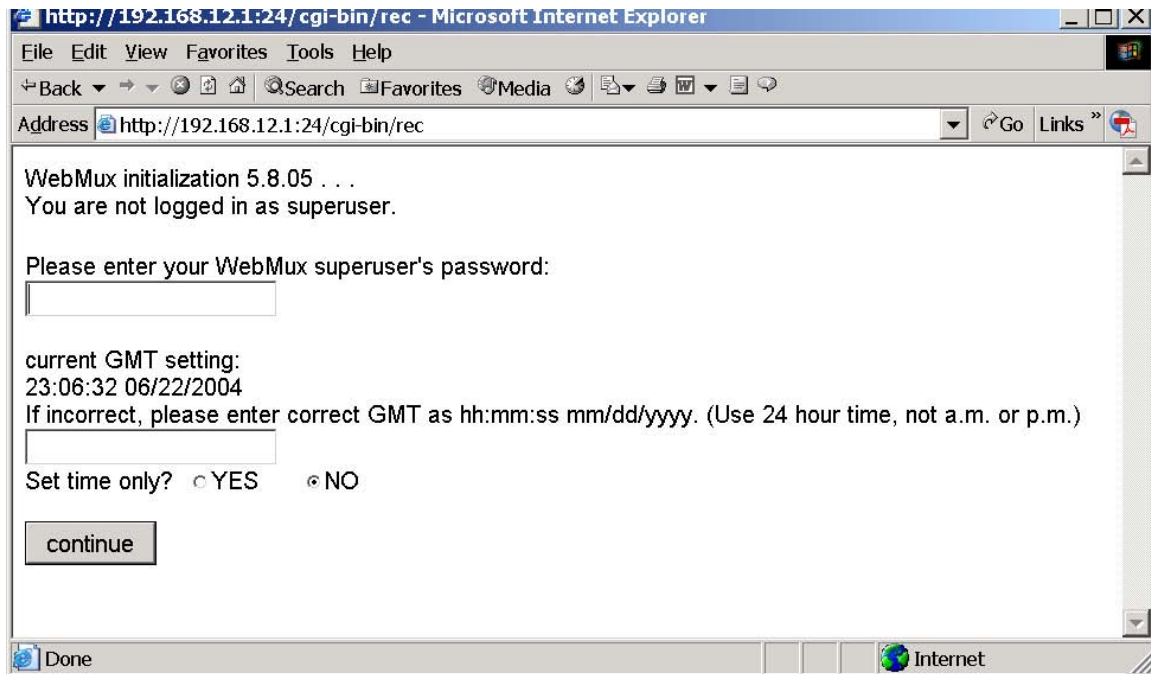
The first screen in "rec" – reconfiguration, asks for the supervisor's password. The default supervisor's password is "supervisor", however, the actual supervisor's password may had been changed by the system administrator. If you could not remember the supervisor's password, someone has to go to the keypad to reset the password. See page 22 for more details.

The next question on the screen asks to set the time in the WebMux. WebMux uses its clock to set cookie for the management browser. When a WebMux manager login more than 8 hours without activity, WebMux will log out the user based on the cookie. However, if the clock is off by more than 8 hours, the manager will not be able to login into WebMux. The second section on the "rec" screen will allow the manager to correct the clock, if it is off.

After enter proper password and set clock information, then "continue" button will bring up this screen:

When the mouse moving over a field, the current value will be automatically filled the field. One may change it based on the new information obtained from ISP or network engineers. Once you press on the submit button, WebMux will save all the changes to its internal slid state storage and reboot itself with the new value.

Initial Configuration Worksheets

Configuration Before WebMux Installation

Equipment	IP Address
Internet Router (or Firewall) Address	
Webserver(s) Default Gateway	
Web Site IP Addresses	

Configuration After WebMux Installation

Question	Entry	
	Primary	Secondary
Host Name		
Domain Name		
NAT or Direct Routing		
Router LAN Information (NAT ONLY)		
Router LAN WebMux Proxy IP Address		
Router LAN Network IP Address Mask		
Router LAN Network IP Address		
Router LAN Broadcast IP Address		
Server LAN Information		
Server LAN WebMux IP Address		
Server LAN Gateway IP Address		
Server LAN Network IP Address Mask		
Server LAN Network IP Address		
Server LAN Network Broadcast Address		
Administration Setup Information		
External Gateway Address		
Remake /home/webmux/conf/passwd	Y/N	Y/N
Administration HTTP Port Number		
Secure Administration HTTP Port #		
Is this WebMux primary	Y	N
WebMux running solo without backup	Y/N	
Reboot?		**Y/N**

Sample Configuration Worksheets

Standalone WebMux

Configuration Before WebMux Installation

Equipment	IP Address
Internet Router (or Firewall) Address	205.133.156.1
Webserver(s) Default Gateway	205.133.156.1
Web Site IP Address	205.133.156.200

Configuration After WebMux Installation

Question	Entry
Host Name	webmux
Domain Name	Cainetworks.com
NAT or Out-of-Path	NAT
Router LAN Information	
Router LAN WebMux Proxy IP Address	205.133.156.200
Router LAN Network IP Address Mask	255.255.255.0
Router LAN Network IP Address	205.133.156.0
Router LAN Broadcast IP Address	205.133.156.255
Server LAN Information	
Server LAN WebMux IP Address	192.168.199.251
Server LAN Gateway IP Address	192.168.199.1
Server LAN Network IP Address Mask	255.255.255.0
Server LAN Network IP Address	192.168.199.0
Server LAN Network Broadcast Address	192.168.199.255
Administration Setup Information	
External Gateway IP address	205.133.156.1
Remake /home/webmux/conf/passwd	Y
Administration HTTP Port Number	24
Secure Administration HTTPS Port Number	35
Is this WebMux primary	Y
WebMux running solo without backup	Y
Reboot?	*Y*

You will also need to change the Web server IP address to 192.168.199.10, and its default gateway to 192.168.199.1. Add a farm for 205.133.156.200 and add a server to the farm at 192.168.199.10. You can then add more servers at 192.168.199.20 and 192.168.199.30. You can also add additional farm at

205.133.156.210, and add above three servers to the 2nd farm.

A Redundant Installation

Configuration Before WebMux Installation

Equipment	IP Address
Internet Router (or Firewall) Address	205.133.156.1
Webserver(s) Default Gateway	205.133.156.1
Web Site IP Address	205.133.156.200

Configuration Before WebMux Installation

Question	Entry	
	Primary	**Secondary**
Host Name	webmux1	webmux2
Domain Name	Cainetworks.com	Cainetworks.com
NAT or Out-of-Path	NAT	NAT
Router LAN Information		
Router LAN WebMux Proxy IP Address	205.133.156.200	205.133.156.200
Router LAN Network IP Address Mask	255.255.255.0	255.255.255.0
Router LAN Network IP Address	205.133.156.0	205.133.156.0
Router LAN Broadcast IP Address	205.133.156.255	205.133.156.255
Server LAN Information		
Server LAN WebMux IP Address	10.1.1.10	10.1.1.20
Server LAN Gateway IP Address	10.1.1.1.1	
Server LAN Network IP Address Mask	255.0.0.0	255.0.0.0
Server LAN Network IP Address	10.0.0.0	10.0.0.0
Server LAN Network Broadcast Address	10.255.255.255	10.255.255.255
Administration Setup Information		
External gateway IP address	205.133.156.1	205.133.156.1
Remake /home/webmux/conf/passwd	Y	Y
Administration HTTP Port Number	24	24
Secure Administration HTTPS Port	35	35
Is this WebMux primary	Y	N
WebMux running solo without backup	N	
Reboot?	*Y*	*Y*

Direct Routing Installation of WebMux

Configuration Before WebMux Installation

Equipment	IP Address
Internet Router (or Firewall) Address	10.1.1.1
Webserver(s) Default Gateway	10.1.1.1
Web Site IP Address	10.1.1.200/255.255.0.0

Configuration After WebMux Installation

Question	Entry
Host Name	webmux
Domain Name	Cainetworks.com
NAT or Out-of-Path	Out-of-Path
Server Configuration	
Server IP address	No Change
Server NetMask	No Change
Server Default Gateway	No Change
Server add loopback adapter	10.1.1.200
Route Deletion Refer to Appendix 2	10.1.1.200
WebMux Server LAN Information	
Server LAN WebMux IP Address	10.1.2.254 (any)
Server LAN Servers' IP Address Mask	255.255.0.0
Server LAN WebMux IP Address Mask	255.255.0.0
Server LAN WebMux farm IP Address	10.1.1.200
Server LAN WebMux Broadcast Address	10.1.255.255
Administration Setup Information	
WebMux External Gateway IP address	10.1.1.1
Remake /home/webmux/conf/passwd	Y
Administration HTTP Port Number	24
Secure Administration HTTPS Port Number	35
Is this WebMux primary	Y
WebMux running solo without backup	Y
Reboot?	*Y*

There is no change to each server's IP address, netmask and gateway address. There is need to add a loopback adapter to each server, and assign the farm address to the loopback adapter. For MS Windows, it always adds a route for the

loopback adapter, which will need to be removed, please refer to Appendix 2. In the virtual farm, each server uses its original IP address to join the farm.

Contact Information

For latest product and support information, please visit our web site at**:**
http://www.cainetworks.com

To reach us by e-mail:
Support: support@cainetworks.com
Sales: sales@cainetworks.com

To reach us by phone:
Support: 714-550-0901 X2

FAQs

Q.   I can't login with my browser. It always says you are not logged into?

R.   To use your browser to manage the WebMux, it must be set to accept all cookies. Because the cookie sets expired in 8 hours, you also need to make sure your hardware clock set correctly using GMT. The message indicates your system clock off. Please refer to page 45 for how to set the internal clock.

Q.   I can't login with my browser. Because server does not response?

R.   Your IP address is not on the allowed host list, or wrong IP addresses entered by accident. Using front push button to clear that list.

Q   If I have multiple servers assigned as STANDBY, how does the WebMux choose which server to use if an ACTIVE server goes down?

R   The WebMux checks the standby servers in orders and activates each one until their total weight meets or exceeds the server that is unavailable

Q.   Will a server with weight 0 act as a STANDBY?

R.   No. A weight of 0 indicates that the server will not accept any new connections. The state is considered neither ACTIVE nor STANDBY. This is for quite the new connections for the server so that it can take out from services.

Q.   Is the Server LAN and the Router or Front LAN required to be on separate IP subnets?

R.   It is required that the server LAN and the router LAN be separate IP subnets.

Q.   What notification services are compatible with the WebMux?

R.   Airtouch and PageMart are the services that are currently supported. Any SMTP server can be used for sending email notifications.

Q.   If I'm running a Unix-based FTP, such as wuftp, how can I get the ftp server in the farm to resolve the WebMux IP addresses?

R.   The IP addresses typically will not be able to be resolved since the servers in the farm are typically using non-routable or private network addresses. In order for wuftp to resolve the IP addresses and stop complaining, place the non-routable IP address entries in the /etc/hosts file on those servers.

Q.   How come my servers in the farm showing in red color from time to time, even the servers are okay?

R. Your servers are trying to resolve WebMux's IP address to name so it could log them into log file. To avoid this problem, set the servers not resolve the IP addresses, also adding all the IP address to the /etc/hosts file on your servers. For example,
www.mydomain.com   1.2.3.4   // use your real IP address
webmuxgw   192.168.199.1   // server lan gateway
webmuxip   192.168.199.254   // server lan WebMux

Q. How many browsers can simultaneously access the WebMux management console?
R. The limit is 4.

Q. I have added a new farm/server, but the changes are not showing up on the STATUS screen.
R. The web browser caching pages may cause this. If the new configuration does not appear after clicking on Reload or Refresh, then clear the cache or temporary files on the browser.

Q. Will my web server be able to communicate to a credit card validation service, like Cybercash?
R. Yes. Any communication initiated from the internal or private network, the WebMux will substitute the IP address of its router LAN interface for the IP address of the host initiating the conversation. Any service that requires a specific IP address to allow communication into their network, the IP address of the router LAN interface must be the one provided. We have CyberCash engineers worked with us to test this is working fine.

Q. Can I use the WebMux as a proxy server for other hosts in my internal network?
R. Yes. The function that allows the web servers to talk to services such as the credit card validation, allows the WebMux to function as a proxy server for any host in the internal network. The WebMux will translate all internal addresses to the IP address of the "first farm" defined. This is the farm that is created when answering the question: **Enter Router LAN WebMux proxy IP address:**.
Configuring other computers using WebMux's proxy function is easy – just point the gateway IP address to the WebMux backend IP address.

Q. Do I need to have a firewall in front of WebMux?
R. In most cases, no. WebMux blocks all the incoming traffic from router LAN to your internal network. Unless there is a farm defined for a port number, the outside traffic will not be able to reach to any server or computers behind WebMux. WebMux does not have the management functionality for restricting which IP address or services an internal

host can reach to the outside. If such restriction is desirable, then additional firewall is needed.

Q.　　What can I do if the service that I want to load balance is not in the list?

R.　　WebMux as is already supports many different services. In the case if your service is not in the list, you could use generic TCP and/or UDP to set your farm. If that is still not good enough, you may contact us for developing a special service aware module for you. In most cases, there is a very reasonable fee to be charged.

Q　　Why secondary WebMux did not take over when I powered down Primary WebMux?

R　　1) Two WebMux not on the same version of firmware. Or 2) Secondary WebMux monitors primary WebMux as well as few other things. Before it takes over, it makes sure it can reach to the router LAN gateway, as well as at least one server defined in any farm. If secondary WebMux cannot reach to the front router LAN gateway, or it cannot see any server in any farm, then it will consider the primary disconnect or power down was done purposely by operator.

Q　　Why my FastIron Switch set to 100MB fix speed does not work with WebMux?

R　　WebMux uses Intel network chipsets internally. Intel chipsets follows all industrial standards and have good performance and reliability. However, we did discovered some of the Foundry Networks switches does not negotiate with Intel chipsets well. To make them work together, one will need to set the switch to "auto negotiation" on speed, instead of fixed 100. They will communicate each other at 100BT or 1000BT (Pro version only).

Regulations

Notice to the USA
Compliance Information Statement (Declaration of Conformity Procedure) DoC FCC Part 15: This device complies with part 15 of the FCC Rules.

Operation is subject to the following conditions:

1) This device may not cause harmful interference, and
2) This device must accept any interference received including interference that may cause undesired operation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try one or more of the following measures:
> Reorient or relocate the receiving antenna.
> Increase the separation between the equipment and the receiver.
> Plug the equipment into an outlet on a circuit different from that of the receiver.
> Consult the dealer or an experienced radio/television technician for help.

Notice for Canada
This apparatus complies with the Class B limits for radio interference as specified in the Canadian Department of Communications Radio Interference Regulations. (Cet appareil est conforme aux norms de Classe B d'interference radio tel que specifie par le Ministere Canadien des Communications dans les reglements d'ineteference radio.)

Notice for Europe (CE Mark)
This product is in conformity with the Council Directive 89/336/EEC, 92/31/EEC (EMC).

Caution: Lithium battery included with this device. Do not puncture, mutilate, or dispose of batter in fire. Danger of explosion if battery is incorrectly replaced. Replace only with the same or equivalent type recommended by manufacture. Dispose of used Battery according to manufacture instruction and in accordance with your local regulations.

Appendix 1 – How to Add A Loopback Adapter

Installing the MS Loopback Adapter

1. Click **Add Hardware** -> Add a new device -> No, I want to select the hardware from a list, and select **Microsoft Loopback Adapter** from the list and click **OK**.

2. At the **MS Loopback Adapter Card Setup** screen hit **OK** to the default of 802.3

3. You should be prompted for the path to the NT setup files. Click **Continue** once the path is correct.

4. Click **Close**. Reboot maybe necessary. Go to step below for **Configuring the MS Loopback Adapter**

Configuring the MS Loopback Adapter

1. If not there already, goto **Start > Settings > Control Panel > Network > Protocols** tab.

2. Select **TCP/IP** and click the **Properties** button

3. You should be at the **Microsoft TCP/IP Properties** dialog box. Be sure the **MS Loopback Adapter** is the Adapter selected. Enter your farm IP address for **IP address** (**Subnet** should be match your servers, change it if not)

4. Click Apply, then OK, then Yes when prompted to restart the computer

For Windows 2003 Server, make sure the metric is the highest number in routing table, stop here. For Windows 2000/NT Systems, please proceed to the Appendix 2 for remove the route entry in the routing table. For Linux, HP/UX, and FreeBSD perform the following:

Linux 2.4 Systems:
Login as root, and add this command to the bootup script:
Iptables –t nat –A PREROUTING –d farm_ip_address –j REDIRECT

For HP/UX 11.00 and 11i:
Please make sure PHNE_26771 and related patches applied first.
Login as root, and add this command to the bootup script:
Ifconfig   lo0:1   farm_ip_address   up

For FreeBSD: ifconfig lo0 inet farm_ip_address netmask 255.255.255.255 alias

Appendix 2 - How to make route delete reboot persistent

1. In a Windows system, go to boot drive root by cd C:\;
2. Use a text editor to create a text file, in which it contains one line: route delete 10.1.0.0 mask 255.255.0.0 10.1.1.200
3. In above file 10.1.0.0 is the network destination, 255.255.0.0 is the Netmask for the network, and 10.1.1.200 is the farm address, also is the address for the loopback adapter address.
4. start Scheduled Task in control panel;
5. Click "add Scheduled Task"; then next;
6. "Browse" to the .bat file we created -- like webmux.bat under c:\ ;
7. Choose "Perform this task" -- "when my computer starts".

That will delete the route every time the Windows computer reboots. Please make sure after "route delete" the only route left in the routing table for the loopback adapter is this one (your actual IP address and netmask maybe different):

10.1.1.255   255.255.255.255   10.1.1.200   10.1.1.200   1

All other routes for the loopback adapter must not show in the routing table. On both Windows and Unix, routing table can be seen by execute this command: "netstat –rn" .

Please note for Windows 2003 servers, the route for the loopback adapter can not be deleted. However, since Windows 2003 server automatically taking a highest metric number, the route does not need to be deleted.

Appendix 3 - Phone Paging Codes

When an error occurs, the WebMux will send an error code to the regular numerical pager assigned in the Administration Setup page. Please refer to the Management Browser - Administration Setup section on setting up phone pager numbers.

To be as compatible as possible to different types of pagers, only numeric error codes are used. The minimum requirement is the pager should be able to display up to 18 digits. If the pager cannot display 18 digits, some codes may get truncated.

For WebMux (Single and with Secondary)

- 99*IIIIIIIIIIIIPPPP* - A server went down. This 18-digit code (no spaces) starts with 99 followed by 12 digits of the IP address (without the periods) of the server. The last four digits represent the port number of the server.

- 00*IIIIIIIIIIIIPPPP* - A downed server went back up. This 18-digit code (no spaces) starts with 00 followed by 12 digits of the IP address (without the periods) of the server. The last four digits represent the port number of the server.

- 98//////////////[PPPP] – Gateway (router LAN) does not respond. 12 digits number after the 98 is the IP address of the gateway. Port number is optional.

- 01//////////////[PPPP] – Gateway comes back in service. 12 digits number after the 01 is the IP address of the gateway. Port number is optional.

- 88//////////////PPPP – WebMux has detected more connections than the threshold defined in the setup screen.

- 40 - last resort servers taken out of service for a farm.

- 41 - last resort servers put in service for a farm.

- 73   - WebMux cannot reach to the back LAN.

- 74   - WebMux cannot reach the front LAN.

- 75   - Primary or Secondary cannot reach the other WebMux through the serial cable.

- 76   - Serial cable communication restored.

- 55 - User configuration cannot be parsed by WebMux (after the configuration restored through browser).

For WebMux Primary Only

- 66 - Secondary is not responding.

For WebMux Secondary Only

- 71 - Primary failed. Secondary took over from Primary.

- 72 - Primary went back up. Control returns to the Primary.

Appendix 4 – Virtual Hosting Issues

Servers serving more than one web site may do virtual hosting. WebMux supports virtual hosting by checking the virtual server's response. There are three different situations for WebMux to handle.

If the service is HTTPS, there is no way to do virtual hosting on the same IP addresse. However, each HTTPS farm can be on a different IP address on the same server. The reason that each HTTPS server must have its own IP address is that any web server software, IIS or Apache, can not see the URL in the HTTPS packets, since they are encrypted. The IIS or Apache server only decrypts the URL after the packet is sent to a particular process. Since no web server software supports virtual hosting HTTPS on the same IP address, WebMux does not need to do anything extra other than load balancing all the packets for that particular farm.

If the service is HTTP, then any web server software, IIS or Apache, can host almost unlimited virtual farms on each IP address. Many hosting centers handle this situation by putting all the servers serving each virtual host on a server farm on the WebMux. The WebMux will load balance the traffic for all the incoming traffic for that IP address to different servers in that farm. During farm setup, the label for the farm could be one of the virtual farm's base URL, say www.mydomain.com , WebMux actually periodically read a page from this URL. If server that serves that URL does not response correctly, WebMux will mark that server dead. Since every server in that farm serves all the virtual farms, WebMux expects the problem with one server in one URL will affect all the URLs in that farm.

Another situation is the server that serves HTTP virtual sites using a single private IP address already before load balancing. After adding load balancer, some the sites want to have their own IP addresses. WebMux allows set up separate farm for each site having its own public IP address, but point to the same sets of servers in the private network. In this situation, each separate farm could have its own label as www.site1.com and www.site2.com, etc. WebMux will actually do health check on each URL by periodically read a default page from that site.

In the virtual hosting situation, the label and response from the web servers are critical for reliable services. WebMux checks the label and checks the server for its health situation based on the URL supplied in the label. If the server response is 500 or greater, which is an error code indicating server internal error, WebMux will excludes that server from serving the farm. If server responses 402, which indicating access is denied for that virtual farm, WebMux will mark that server dead. We have checked with IIS server and Apache server, they both follow the same rules.

Appendix 5 – Sample Custom CGI Code

The custom cgi-bin checking program may be written in Java, VB, C, or Perl, for example, or it may be a WB or shell script. Here is sample script written for the linux shell bash which sees if an SSH daemon is running as its check criterion.

```bash
#!/bin/bash
echo "Content-type: text/plain"
echo          # blank line
if ps -C sshd &>/dev/null ; then
      echo "OK"
      echo "SSH service available"
else
      echo "NOT OK"
      echo "SSH daemon not running"
fi
```

Appendix 6 – Access CLI Commands

Once the diagnose ports set, superuser could use ssh or telnet to access the CLI commands to help troubleshoot network problems or server problems. There are maximum two diagnose ports. The first one will be SSH and second one will be Telnet. If there is only one port specified, only SSH access is allowed.

"ssh –l superuser –p port_number webmux_ip_address"

Can be issued from any Linux/Unix computer. For Windows computer, PuTTY can be freely downloaded over Internet.

Once login into CLI, following screen will be shown:
Enter "help" for list of commands.
Enter "cmd --help" give help for the command "cmd".
Enter "exit" or "logout" to end this session.

Following are commands available in CLI:
 arp - manipulate the system ARP cache
 arping - ping <address> on device <interface> by ARP packets, using source
        address <source>.
 factory_reset – reset WebMux settings to original settings, clear all current
        setting.
 getallsettings - save all WebMux settings from WebMux to your PC
 getconfig – save all farm/server settings from WebMux to your PC
 ifconfig – display and configure a network interface(s)
 netstat – display network connections, routing tables, interface statistics, etc.
 ping - send ICMP ECHO_REQUEST packets to network hosts
 putconfig - restore farm/server settings from your PC to WebMux
 rec_cmdline – allowing configure basic WebMux IP without using pushbutton.
 tcpdump – capture and display network traffic
 traceroute - print the route packets take to network host

Most commands can be found on Unix, for detailed usage, please refer to any Unix man pages. Our support center does not support the usage of these commands.

Index