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

Configuration Port ("CONSOLE")

The Configuration Port is used to configure WebMux™ and is only required when initially setting the WebMux™'s IP address. Use a serial cable to interface the WebMux™ to a PC set up to access via a serial connection.

USB ports ("USB")

Unused.

Router LAN Ports ("LAN 1" to "LAN 4")

Connect one or more of these ports to the Router LAN switch. In most situations, the port(s) connect to the Internet side network in NAT mode.

Server LAN Ports ("LAN 5" to "LAN 7")

Connect one or more of these ports to the Server LAN switch. These ports connect to the servers and your local computers. In Out-of Path configuration, these are the only Ethernet cables to be connected.

PLEASE NOTE: The Router LAN and Server LAN ports are not interchangeable.

Backup WebMux™ Port ("LAN 8")

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 a cross over cable, or a regular cable with a hub.

Disk Activity Indicator ("HDD")

This indicator light will flash when the solid state disk is being accessed.

Alarm Indicator ("ALARM")

This light will illuminate when an alarm condition exists.

Power Indicator ("PWR")

This light will illuminate when there is power to the WebMux™.

Rear View

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

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

External Modem Connect Port ("COM")
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 to not use diagnostic ports over the Internet, our support engineers can also connect through the modem to assist you with setup issues. A US Robotics 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 is also needed. Check with your modem supplier for the cable.

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.

- **SSL Termination** to reduce the cost of multiple certificates.

- **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. The 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. The two WebMuxes 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, secure 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 (layer4/5 only).** 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 problems, consider using Out-of-Path configuration. Out-of-Path load balancing is also called direct routing, or one leg operation.

- **Transparent Mode.** In this mode, the WebMux™ behaves as an Ethernet bridge between the servers and the Router LAN. The main advantage is that the network settings in the servers do not have to be changed, no loopback adapters or IP address changes needed. The servers will be connected behind the WebMux™ but will appear to be on the same LAN that the WebMux™ is connected to.

- **Layer 7 Load Balancing.** WebMux™ can direct traffic to specific groups of servers within a farm according to a match pattern in HTTP MIME header. This allows you, for example, to group servers that serve only a specific type of content while serving other types of content on another group of servers. WebMux™ Layer 7 load balancing also includes URI load directing with host name MIME header matching and cookies in order to memorize the user browser session and the server session and send the same user to the same server. This is important for sites using shopping cart and dynamically generated pages.

- **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.

- **IPv6 Support**. (Out of Path mode only). WebMux™ is ready for the next generation of internet protocol, IPv6.

- **Multiple Address Port (MAP)** farm to integrate multiple ports and IPs as one server.

The WebMux™ Family

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

- The WebMux™ 481S
- The WebMux™ 591SG
- The WebMux™ 680SP

The table below compares the features of the models.

Model Number:	481S	591SG	680SP
Layer 4 Performance			
Maximum concurrent connections	1,440,000*	2,880,000*	5,760,000*
Maximum transactions per second	15,000	50,000	100,000
Maximum throughput per second	200 MBits	1GBits	4GBits
Maximum Internet link speed	2 X T3	1.5 X OC-12	1.5 X OC-12
Layer 7 & SSL Acceleration			
Max. 1024bit RSA terminations/second (round trip)	120	250 1200** 2400***	4000* 6000***
Max. Layer 7 connections/s	10,000	30,000	50,000
Number of SSL certificates	32	32	32
Load Balancing Methods			
Cookie content based	Yes	Yes	Yes
URL based	Yes	Yes	Yes
Round-robin	Yes	Yes	Yes
Persistent round-robin	Yes	Yes	Yes
Weighted round-robin	Yes	Yes	Yes
Persistent weighted round-robin	Yes	Yes	Yes
Least connections	Yes	Yes	Yes
Persistent least connections	Yes	Yes	Yes
Weighted least connections	Yes	Yes	Yes
Persistent weighted least connections	Yes	Yes	Yes
Traffic Management Methods			
URL based content switch	Yes	Yes	Yes
Cookie based content switch	Yes	Yes	Yes
Fault Tolerance			
Diskless Design	Yes	Yes	Yes
Port aggregation	Yes	Yes	Yes
Failover via network connection	Optional	Optional	Optional
Failover via Ethernet link	Yes	Yes	Yes

Service aware	Yes	Yes	Yes
Server aware	Yes	Yes	Yes
Backup server	Yes	Yes	Yes
Security			
Network Address Translation (NAT)	Yes	Yes	Yes
TCP SYN protection	Yes	Yes	Yes
Address mapping	Yes	Yes	Yes
Port mapping	Yes	Yes	Yes
TCP DoS protection	Yes	Yes	Yes
HTTPS/SSH management	Yes	Yes	Yes
Topologies			
IPV4/IPV6 support	Yes	Yes	Yes
GB Ethernet (1000Base-TX)	Yes	Yes	Yes
Rackmount 1U form factor	Yes	Yes	Yes
Device Support			
Interface to switches	Gigabit x2	Gigabit x2	Gigabit x8
Maximum virtual servers	Unlimited	Unlimited	Unlimited
Maximum real servers	65,532	65,532	65,532
Device's role in the network	Bridge/router	Bridge/router	Bridge/router
UDP-based service support	Yes	Yes	Yes
Management			
Secure web browser access	Yes	Yes	Yes
In service / Not in service	Yes	Yes	Yes
Phone / pager alarm notification (ext modem req)	Yes	Yes	Yes
Email Notification	Yes	Yes	Yes
Configuration access	Yes	Yes	Yes
Remote telnet/SSH access	Yes	Yes	Yes
Persistent connections	Yes	Yes	Yes
Port-specific services	Yes	Yes	Yes
Miscellaneous			
Factory warranty	3 years	3 years	3 years
Free telephone and email support	3 years	3 years	3 years
Free factory pre-configuration	Yes	Yes	Yes
Overnight pre-sent exchange unit	Optional	Optional	Optional
24x7 Gold Premium Support	Optional	Optional	Optional
30-day money-back guarantee	Yes	Yes	Yes

NAT(in-path) mode. Much higher performance in Out-Of-Path mode
* *With CAI-RSA3500 option card*
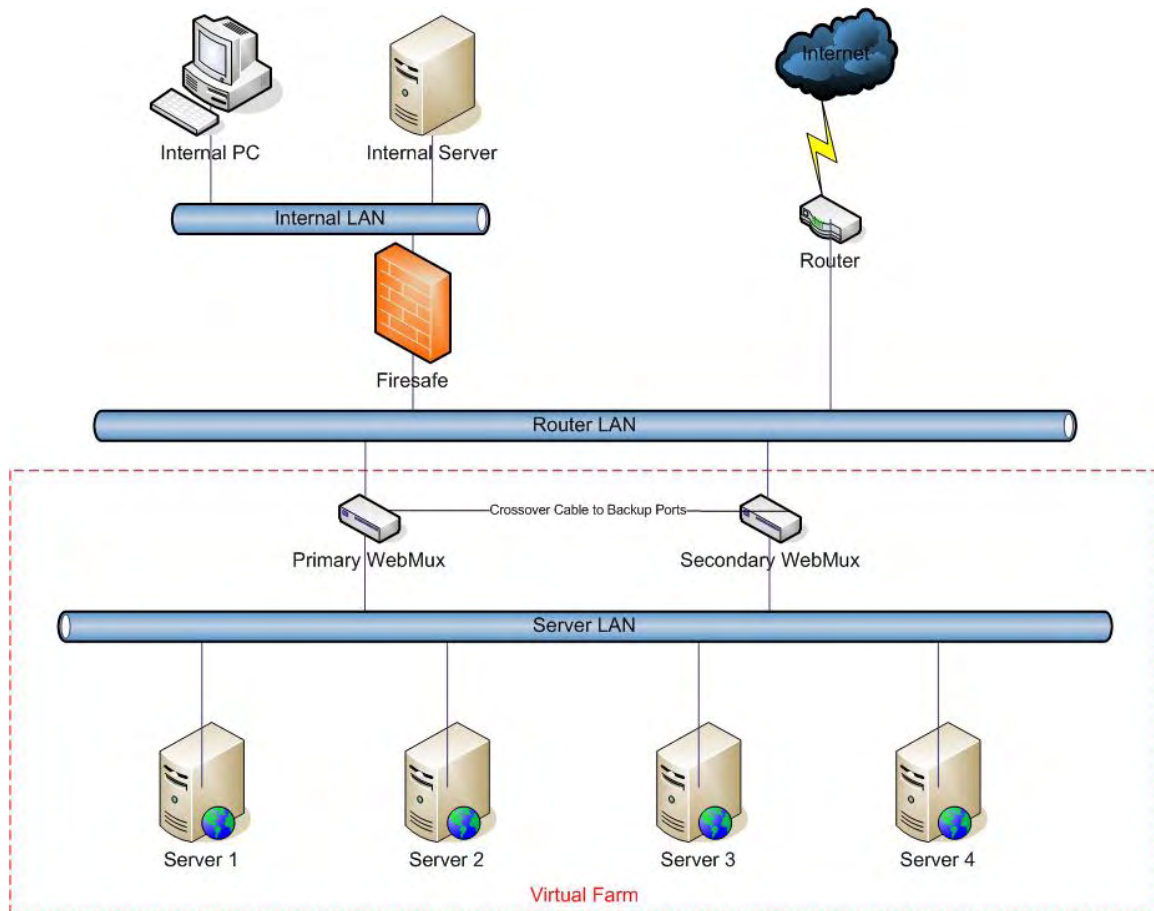**** *With CAI-RSA7000 option card*

Trunking

WebMux™ model 680PG uses Link Aggregation Control Protocol (LACP) to trunk multiple network channels together to achieve greater throughput. This requires multiple connections between the WebMux™ unit and the Router and Server LANs, by connecting multiple ports on the WebMux™ to multiple ports on the Router and Server LAN switches, and configuring each switch to trunk the respective ports together.

WebMux™ model 680PG uses ports "LAN 1", "LAN 2", "LAN 3", and "LAN 4" for the Router LAN and "LAN 5", "LAN 6", and "LAN 7" for the Server LAN. One or more ports in each of these two groupings can be used, with the more ports used the greater the possible traffic handling capacity. At a minimum, one port from each group must be connected (e.g. "LAN 1" to the Router LAN and "LAN 5" to the Server LAN) to the respective switch.

To take advantage of WebMux™'s trunking feature, the switches must support LACP protocol, and the protocol must be enabled and the switches properly configured to aggregate the appropriate ports properly. Note: some switches when LACP enabled, they may require turning off STP to avoid network storm.

Network Overview

The WebMux™ has three modes: In-Path, or NAT (Network Address Translation), Out-of-Path mode, and Transparent (NAT Ethernet Bridge) Mode. Each mode has its advantage and disadvantages. Lets look the NAT mode first.

Internal PC   Internal Server

Internal LAN

Firesafe

Router LAN

Crossover Cable to Backup Ports

Primary WebMux   Secondary WebMux

Server LAN

Server 1   Server 2   Server 3   Server 4

Virtual Farm

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 (Internet) connects to the **Router LAN**. This is the network to which the Internet router is connected. The other interface (server) 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 the 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.
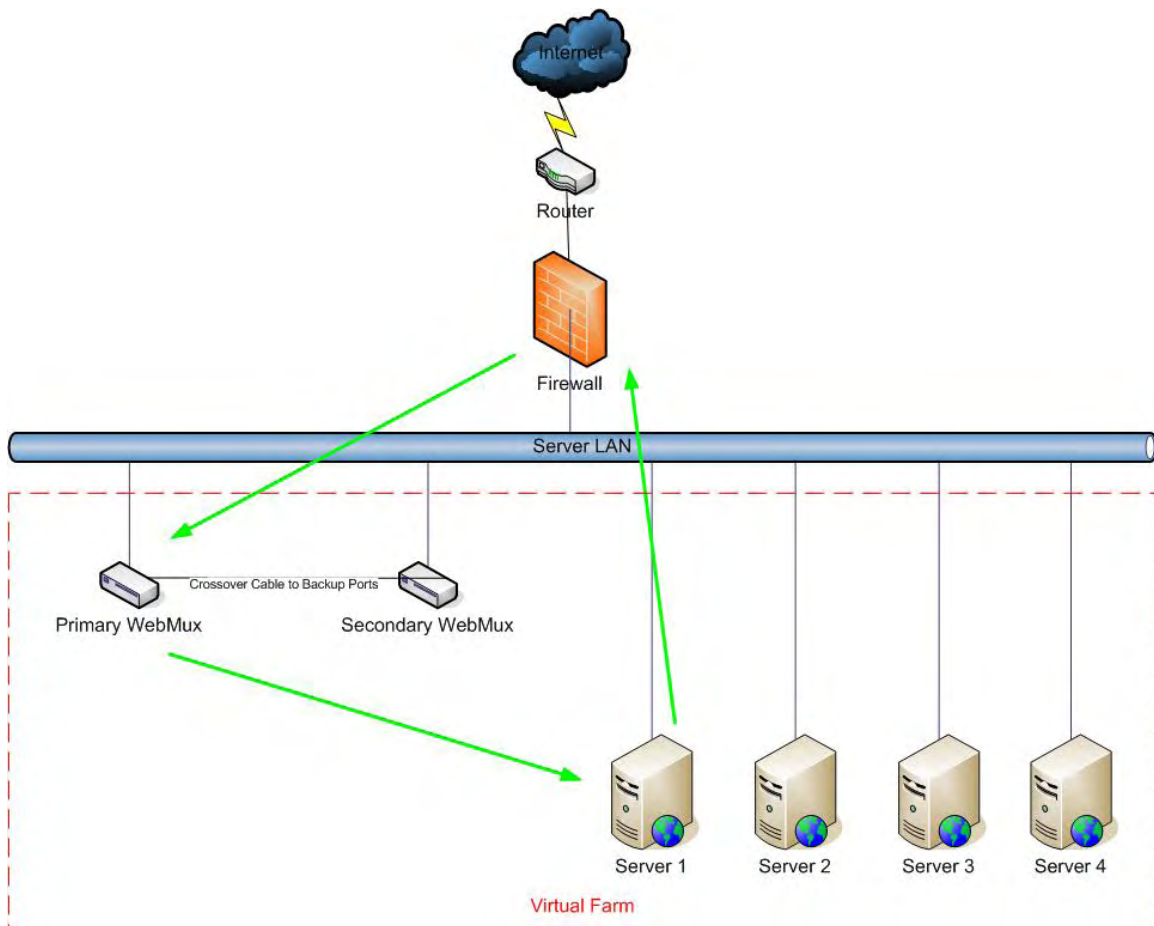
In most situations, the incoming traffic is in small requests, and return traffic from servers back to clients is large amount of data, pictures, or documents. Using out-of-path mode will allow up to 100 times more traffic to be handled by the WebMux™ load balancer. The disadvantage for OOP/direct responding is that the firewall protections built-in to the WebMux™ will no longer function. Users then must provide their own firewall for incoming and outgoing traffic.

Sample Configurations

Single WebMux™

NAT Mode Single WebMux Installation
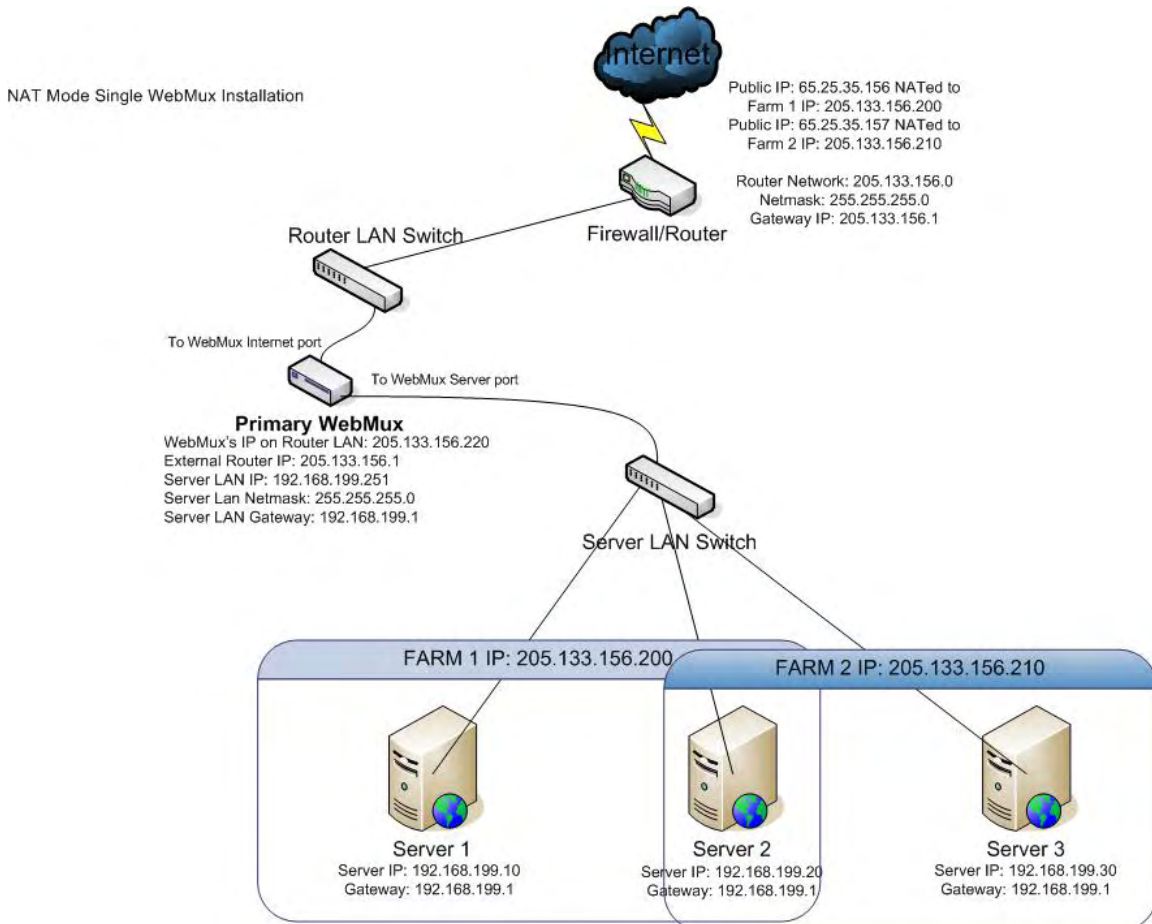
- This installation requires one WebMux™.

- One WebMux™ interface (Internet) connects to the Router LAN. The other interface connects to the Server LAN.

- The WebMux™ translates the Router LAN IP 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 on the Router LAN is 205.133.156.220. 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.

- Changes to the server: change the 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 the WebMux™ can work 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 the WebMux™ interface address must be translated to communicate outbound on all ports.

Redundant Installation

NAT Mode with Redundant WebMux Installation
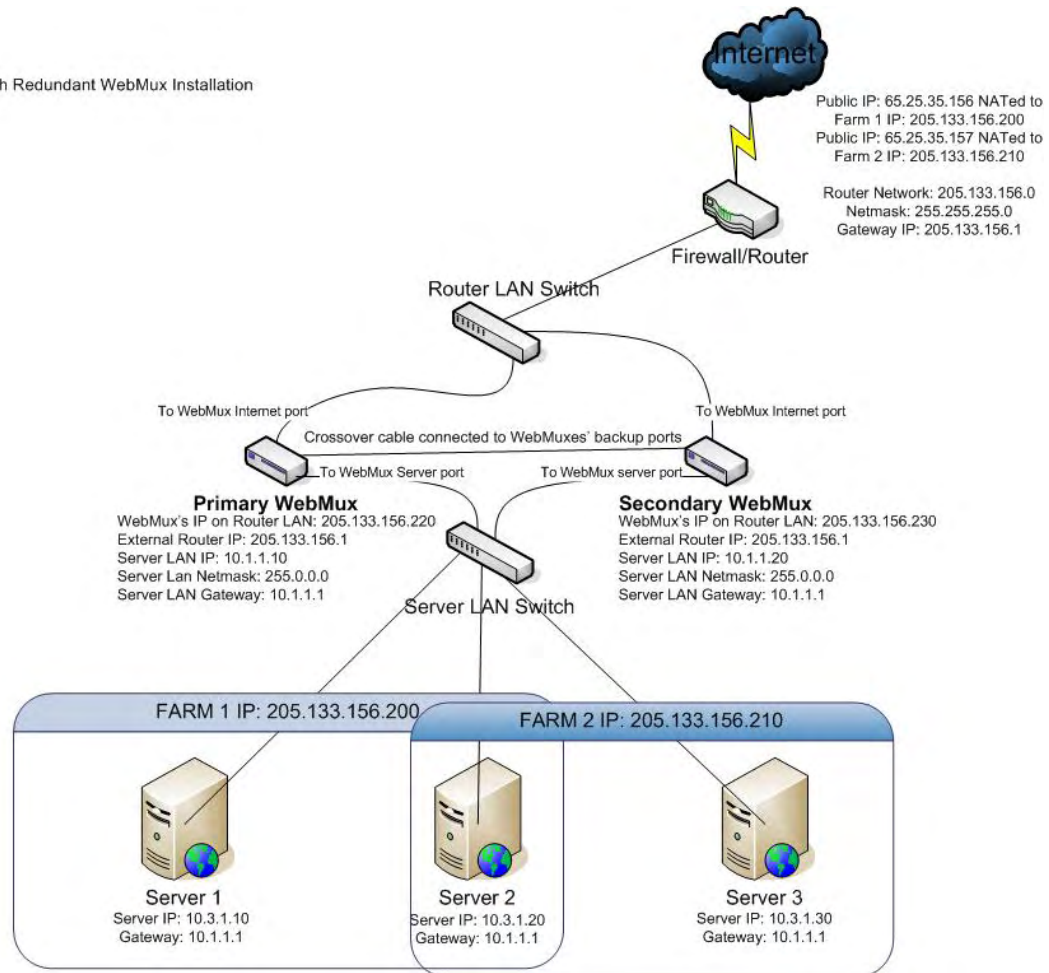
- The installation requires two WebMuxes. One will be the primary, and the other the secondary. They connect together with the Ethernet cable that is either cross-over or through a hub. The primary redundant interface IP address is 192.168.255.253; the secondary redundant interface IP address is 192.168.255.254. 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 Router LAN IP addresses to an internal non-routable class A address. In this example, the subnet-mask is

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.

- Changes to the servers: change default the 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 the WebMux™ can work 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 the 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 (OOP)

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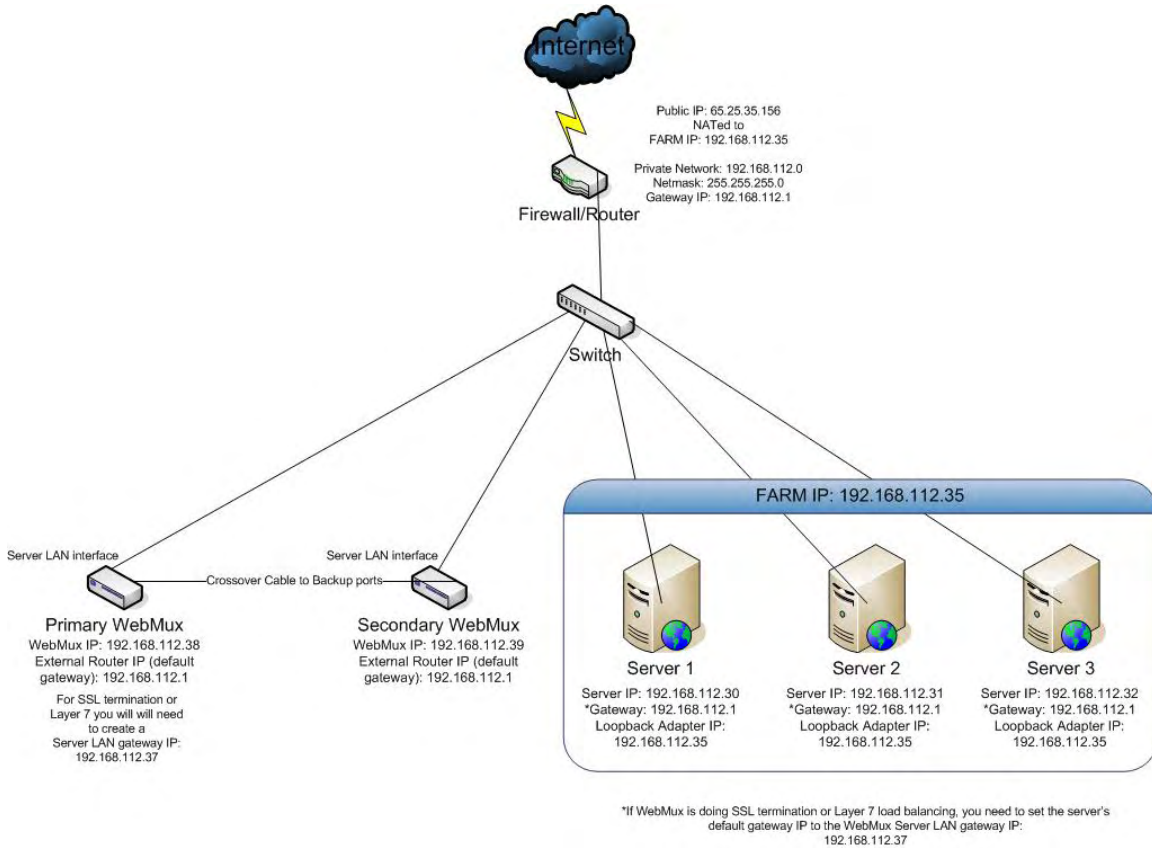
The above diagram is an example about how to configure the WebMux™ in out-of-path mode without changing the IP addresses of the web servers and other servers that already exist on the network. This is particularly helpful when the changing of an existing network of servers causes problems.

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 the server LAN cable is connected, since there is only one network in direct routing mode. The 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. The two WebMuxes are connected to each other through a cross-over Ethernet cable.

Two simple changes must be made to each server in the farm. 1) Have a new loopback adapter installed and have its address set to the farm address. Do not set the gateway on the loopback 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. In other words, the loopback adapter cannot have the gateway specified. Please refer to Appendix 1 and 2 for more details on how to configure the loopback adapter on servers. In case the server is running Windows 2003, the route created during adding loopback adapter cannot be deleted; please make sure the 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 the 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.

> **NOTE:** Under normal Out-of-Path operations, you will only need to set the external gateway IP address for the WebMux™ . However, if you are going to have the WebMux™ do SSL termination or Layer 7 load balancing, you must set a server LAN gateway IP in the WebMux™ and have the servers' default gateway point to that IP address.

Installation without IP Address Change (TM)

Transparent Mode:
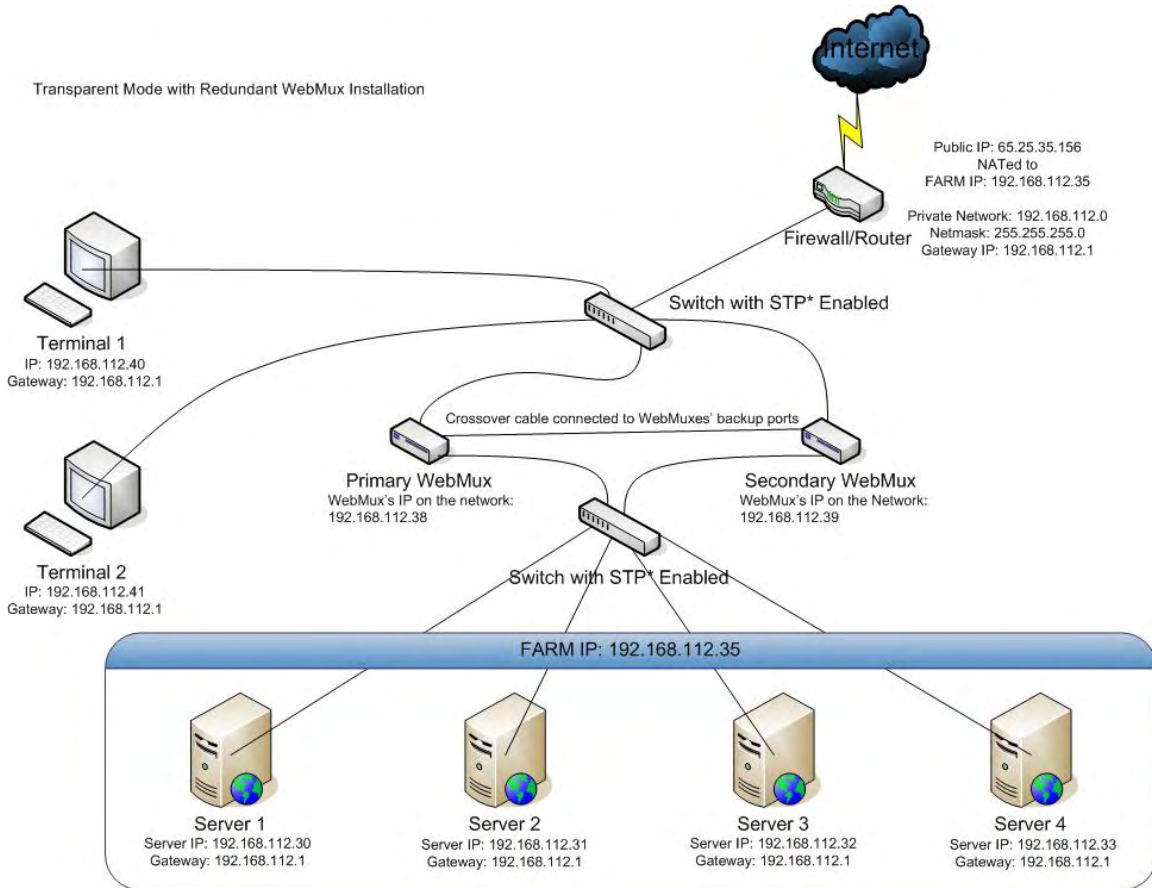
Transparent Mode is another WebMux™ configuration that allows you to keep the existing IP addresses of your servers. Like Out-of-Path mode, the servers and the WebMux™ will be on the same IP network. However, physically, the servers will be connected to the WebMux™ in the same way they would be for NAT mode, on the server LAN port. The "internet" port on the WebMux™ is connected towards the Firewall/Router. In this mode, the WebMux™ functions as an Ethernet bridge. Anything connected to its back interface (server LAN) is on the same network as its front interface (internet/router LAN). If you look at the diagram above, you will see that the terminals are on the same network as the servers, even though the servers are "behind" the WebMux™. The terminals can communicate with the servers IP directly as if the WebMux™ was not there, and vise versa.

When creating a farm, choose a unique farm IP address in the network, and then add the server IP address under that farm. Load balancing occurs when the "Farm IP" is accessed instead of the servers' actual IP.

There are no configuration changes that need to be made on the servers, only the way they are physically connected to the network.

This diagram also gives an example of a redundant WebMuxTM setup. In this case, if the switches have Spanning Tree Protocol (STP) it is necessary to disable STP protocol, due to LACP may conflict with STP protocol.

During a failover situation, you may immediately notice that the backup becomes unreachable even though the indicator lights show that it is active. This is a temporary situation as the switches detect new bridge priorities. This failover time usually takes about 1-30 seconds, depending the switch. This also happens when the primary comes back online and the secondary returns back to standby mode.

Configuring the WebMux™

Before you Start

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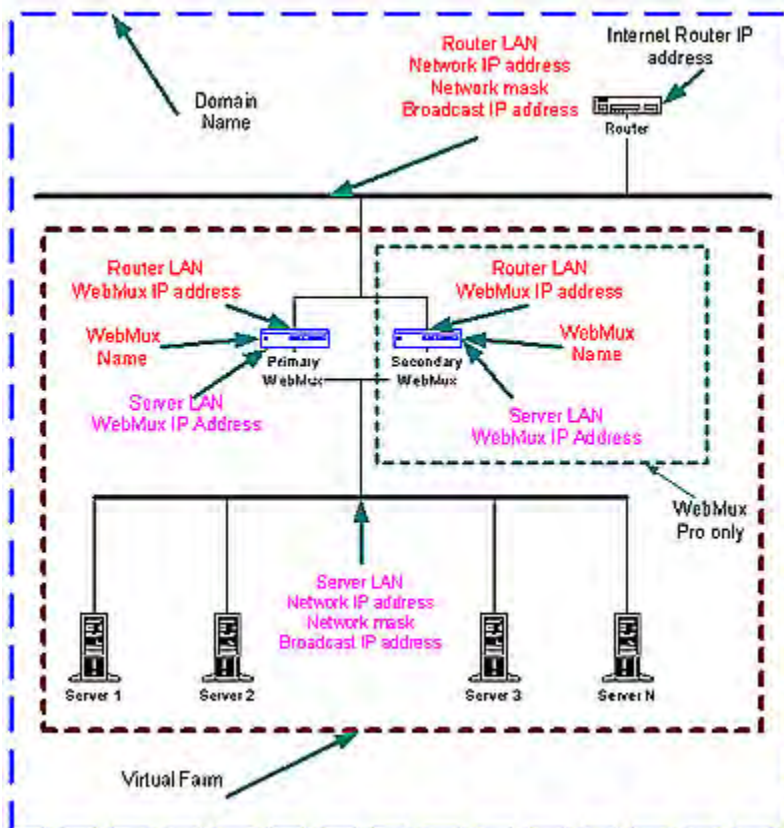
Network Terminology

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.you.com is one virtual server farm; https://www.me.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 that the 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 the WebMux™ and real servers together is called **Server LAN**.

WebMux has three mode, NAT mode, OOP mode, and transparent mode. In NAT mode, only the 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**. We talk other modes in details at later chapters.

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 the 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 and Transparent mode).

- 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.**
NOTE: The IP addresses in the following examples are general examples and are not meant for literal use in an actual setup.

- Turn on the WebMux™. Turn on the power toggle switch ("PWR ON") on the back of the WebMux.

Initial Configuration

The initial WebMux^{TM} configuration is performed in two steps:

- First, connect the 680P WebMux^{TM}'s configuration ("CONSOLE") port to a computer via a cross-over serial cable to set the IP address for the WebMux, communication parameter is 9600 8N1
- Then, connect to the WebMux^{TM} via a web browser to perform the rest of the initial configuration using WebMux^{TM}'s Management Console

Initial setup through Serail/Browser Console

In the initial WebMux setup, you will need to enter the following information, which varies based on the networking mode:

- WebMux^{TM}'s host name
- WebMux^{TM}'s domain name
- WebMux^{TM}'s networking mode (NAT, Transparent, or Out-of-Path)
- For NAT mode, the WebMux^{TM} proxy IP address and net mask for the Router LAN and the WebMux^{TM} IP address, net mask, and gateway for the Server LAN
- For OOP mode, the WebMux^{TM} IP address, net mask, and gateway for the Server LAN
- The server gateway (used if Layer 7 load balancing is being done)

- Whether the WebMux^{TM} is running in a solo configuration or with a backup unit
- If WebMux^{TM} is running with a backup unit, whether the WebMux^{TM} being configured is the primary or backup unit
- The HTTP and HTTPS ports used for WebMux^{TM}'s Management Console

Using a web 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 ebmux_manage_port is 24, your URL will be
http://192.168.12.1:24/cgi-bin/rec
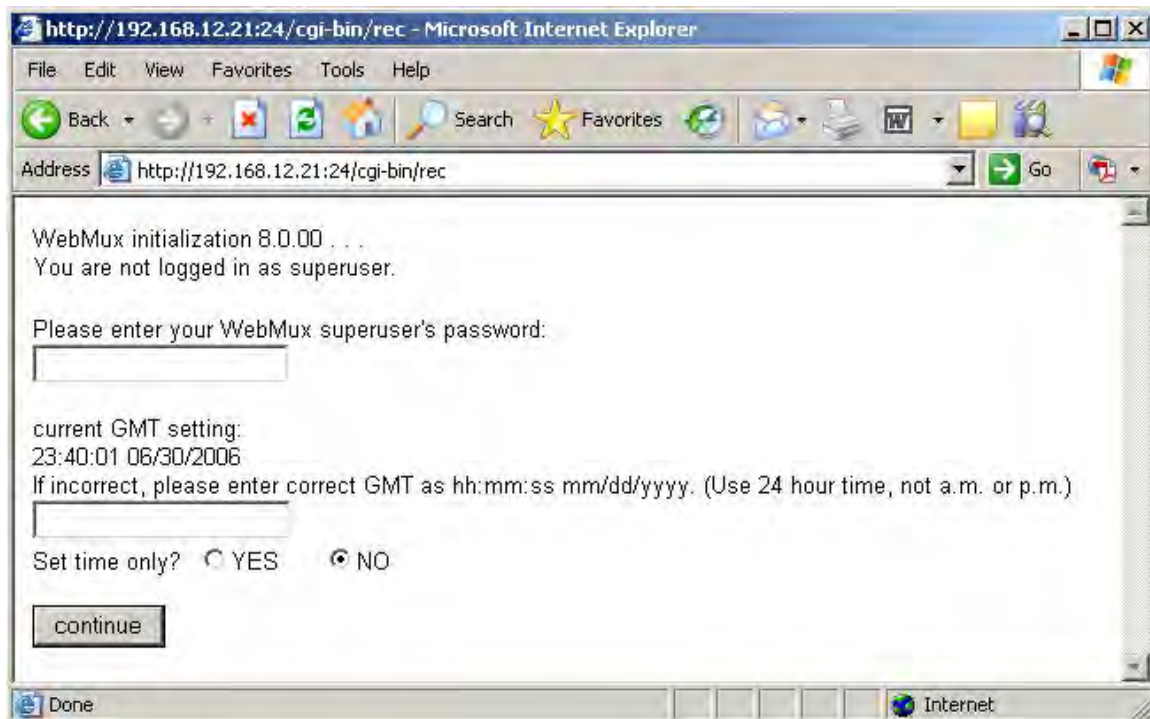
The first screen asks for the superuser's password. The default superuser's password is "superuser",

The next question on the screen asks to set the time in the WebMux™. The WebMux™ uses its clock to set the cookie for the management browser. When a WebMux™ manager is logged in for more than 8 hours without activity, the 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 in to the WebMux™. This section on the "rec" screen will allow the manager to correct the clock, if it is off. After entering proper password and setting the clock information (optional), the "continue" button will bring up this screen:

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

WebMux's name without the domain name
Enter the host name of the WebMux™. This host name is for identification purposes. You may call it webmux1, webmux2, etc.

WebMux's domain name
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.

dispatch method

This specifies WebMux™'s networking mode. Select either "NAT", "Transparent", or "OOP" from the listbox.

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. Transparent mode causes WebMux™ to behave as an Ethernet Bridge. Out-of-Path provides better performance when huge amounts of data need to go back to clients (up to 100X more than on the specification chart); it also does not require a change to the server IP address.

IP address of external router used by WebMux (all modes)

This is the common setup for NAT, Transparent, and Out-of-Path modes. This is an address on the firewall or router local interface. 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, the WebMux™ does check the connectivity to the incoming side on this gateway or through this gateway to the ISP side routers. However, for SSL termination or Layer 7 load balancing, servers need to route traffic back to the WebMux™ via the server LAN gateway (previously mentioned). The WebMux™ then forwards it to the client through the external gateway.

WebMux's address on router's network used as servers' proxy address (NAT mode only)

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). For redundant setup, secondary WebMux™ uses the same IP address for this entry as the primary one. This address floats between primary and secondary WebMuxes.

network mask on this network (NAT mode only)

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

WebMux's fixed IP address on the server's network (all modes)

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™ to check the network and server health 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. 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 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.

network mask on this network (all modes)

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 255.255.255.0.2

Remake password file with default passwords?

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

WebMux administration HTTP port

This is the 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.

WebMux administration HTTPS port

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.

Is this WebMux a primary (or solo) WebMux?

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.

Is this WebMux running solo without a secondary?

If the Primary WebMux™ is running in a standalone configuration (see sample configuration – Standalone WebMux™.), answer Yes. If you plan to add 2nd WebMux™ in the future, you may answer NO, even there is only one WebMux at

the time.   When you add second WebMux™ later on, WebMux™ will automatically detect the backup and start functioning.

IP address on WebMux on server's network used by servers as their router (required for NAT and Transparent mode, optional for OOP mode)

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.

This is an optional configuration that is used only if you are going to do SSL termination or Layer 7 load balancing. Keep in mind this is an IP address assigned to the Server LAN network interface. Be sure to use a unique IP address or duplicate IPs on the network will occur. Enter 0.0.0.0 if not needed.

In the single WebMux™ setup, this address CANNOT be the same as the WebMux™ IP interface address on the Server LAN.

Reinitalize configuration with admin entries only?

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

Reboot immediately after submitting this form?

This is the end of initial configuration. Most of the setup or changes require a reboot to take effect. Select 'Yes' to make the WebMux™ reboot or 'No' to defer the reboot until the 'Submit' button is pressed.

Submit when satisfied or cancel and log out.

Press the 'Submit' button to submit changes, which may cause the WebMux to reboot, or 'Cancel' to cancel the settings specified in the current form.

Management Console

After setting the IP address for the WebMux™, the user should be able to connect a web browser to the WebMux™ to perform the rest of the initial setup and to configure the WebMux™. The web browser does all of the WebMux™ configuration and management except for setting the initial IP address – once the IP address is set, the Management Console can be used for everything else.

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 **https***://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 http instead of https on the URL line if you decide to use port 24 for unsecured communications. (The port number can be changed per your specification, under "setup" in "main management console" section).
- The following login page will appear.

NOTE: In order to 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; allows viewing only.

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 **superuser** 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.
If only HTTPS management login is allowed, go to "setup" and make the first port number for HTTP/HTTPS management port to 0:35

Main Management Console
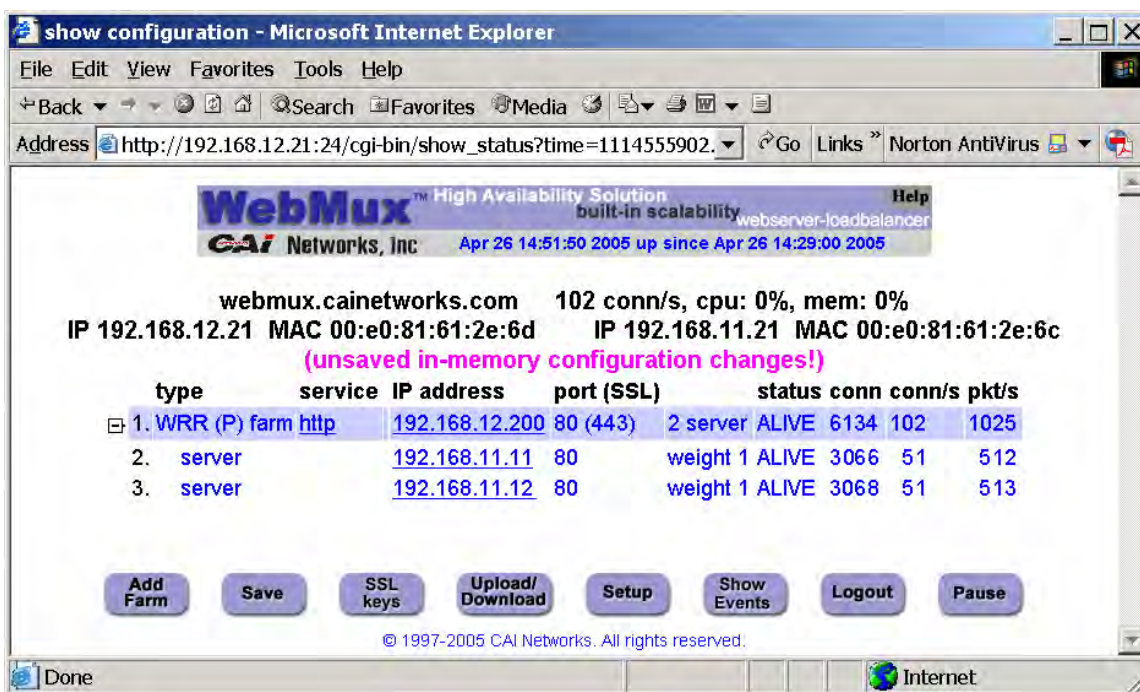
Once logged in to the Management Console, this main screen will show. To continue configuring the WebMux™ , the normal steps are:

Click on the "Setup" button to change administration and setup related information;
Click on "SSL keys" button to manage SSL keys, if SSL termination is desired;
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.

We will discuss those buttons and related features in great details in later sections. Other buttons on the main management console screen are:

Save
On main management console, click Save button will cause WebMux save its configuration. Changes made to the "Farm" and "Server" will take effect immediately without save. The changes however are not saved permanently to the solid state storage 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 the user to save and restore the WebMux™ configuration to and from their management workstation. See later chapter for details.

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

Show Event
This button will display all the events since the WebMux's 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/ Resume
The status screen automatically refreshes frequently to provide most up to date status. You can use the Pause button to freeze the auto refresh.

After the Pause button is 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
Clicking on the service type on each farm will allow you to change the timeout value of layer 7 testing for each different service. Please note this change is global and 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 the web server does not respond to the WebMux™ protocol chat within 5 seconds, the 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 is not really dead but for some reason not responding to the checking request, the WebMux™ will false alarm. To avoid this, the user can change the timeout value to a larger value. Many times, servers can not resolve the IP address for the back end of the WebMux™ IP address and could cause the server to not respond to the 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 into management console as superuser, click on the setup button, you will come to this screen:

Allowed remote host IPs:

The WebMux™ management console and diagnostic 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. From version 6.4.00, 192.168.12 will be allowed for class C allowed host. 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. If wrong IP addresses are entered, management console login might not be possible. Use the push button controls on the WebMux™ to clear the allowed host list. This field is blank by default.

IPv6 96-bit Address Prefix:

In Out-of-Path mode, you will see the option to create an IPv6 address prefix. The IPv4 addresses will be appended to this prefix. For example, if you assigned 192.168.12.21 for the WebMux's server LAN ip and you assigned fec0:: as the

IPv6 prefix, the WebMux's complete IPv6 address will be fec0::192.168.12.21 (or fec0::c0a8:c15). See also Appendix 8 for extra info on using IPv6.

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 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 the WebMux™ to relay messages are 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

UDP syslog server IP address notification:
The WebMux™ can be configured to send syslog messages to a remote syslogd server. Enter the syslogd server IP address to use this feature. The syslogd server must be configured to accept remote UDP syslog connections. The facility for WebMux™ syslog messages is LOCAL6.

The notification levels of the syslog messages are as follows:

Level	Search Key	Description
INFO	STATS	Status messages
NOTICE	LOGIN	Successful browser login/logout (exludes timeout logout)
NOTICE	SETUP	Significant access and changes to setup and configuration items.
NOTICE	EVENT	Same as pager/mail messages
WARNING	LOGIN	Unsuccessful browser login

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 the WebMux™ acting as a router 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. Only apply for the NAT mode (or for Out-of-Path mode that requires the WebMux™ to do the SSL termation or Layer 7 load balancing. Normally, it this is optional for Out-of-Path mode).

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 the WebMux™ is 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 to any port that is not being load balanced, if so desired. The font push buttons can also change this.

WebMux™ https control port:
Since the WebMux™ is 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 to any port that is not being load balanced, if so desired. The front push buttons 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 sent through multiple cache servers; it is possible the requests for one HTML page are 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 the 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 this 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 the 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. The 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 the WebMux™ through ARP and TCP Connection; however, most Cisco DSL modems will only talk to the WebMux™ through Ping. The change to this verification method will take effect after the WebMux™ has been 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. When farm listing turning red, it is an indication that this address failed check.

Persistence Timeout:
The WebMux™ will keep track the browser connections if the persistent farm is defined and accessed. Within the timeout time period, the 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:
The 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 the WebMux™ to allocate 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:
The 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, the WebMux™ may not be able to get around checking all the servers in few seconds. In concurrent mode, the WebMux™ will start multiple protocol scanners to chat with servers concurrently. Concurrent mode uses more memory and may have other side effects. For most setups, sequential scan is recommended.

URL for Custom Service Check:
Sometimes the WebMux™ built-in server health check is not enough for special needs. When one ASP/JSP server's output depends on the database server and the database server connection is down, one might want to reduce the incoming traffic to the server, suspend new traffic to the server, or totally redirect incoming traffic to a different server. To accomplish that, the WebMux™ allows a farm being set using a "custom defined 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 with one of the allowed responses. 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 is considered dead. The custom defined service also allows for CGI code responses that allow the server to change its own weight and announce such change to a remote syslog daemon. Please see appendix 5 for a sample code and a list of allowed responses.

UDP NTP Time Server IP Address:
Since version 5.4, the 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, the WebMux™ will pretend the server is sending TCP Reset to the client, thus freeing all the TCP_WAIT state connections. Default setting is "Yes" to conserve resources.

Reboot:
Changes to "TACACS+ server configuration", "server gateway address", "server farm network mask", "WebMux™ http control port", "WebMux™ https control port" "WebMux diagnostic ports", "least significant bits", "forwarding policy", "front network verification", and "persistence timeout" requires a reboot for the new configuration to take effect. You can use the Reboot button to reboot the WebMux™ remotely.   Reboot button does require confirmation before proceeding with reboot.

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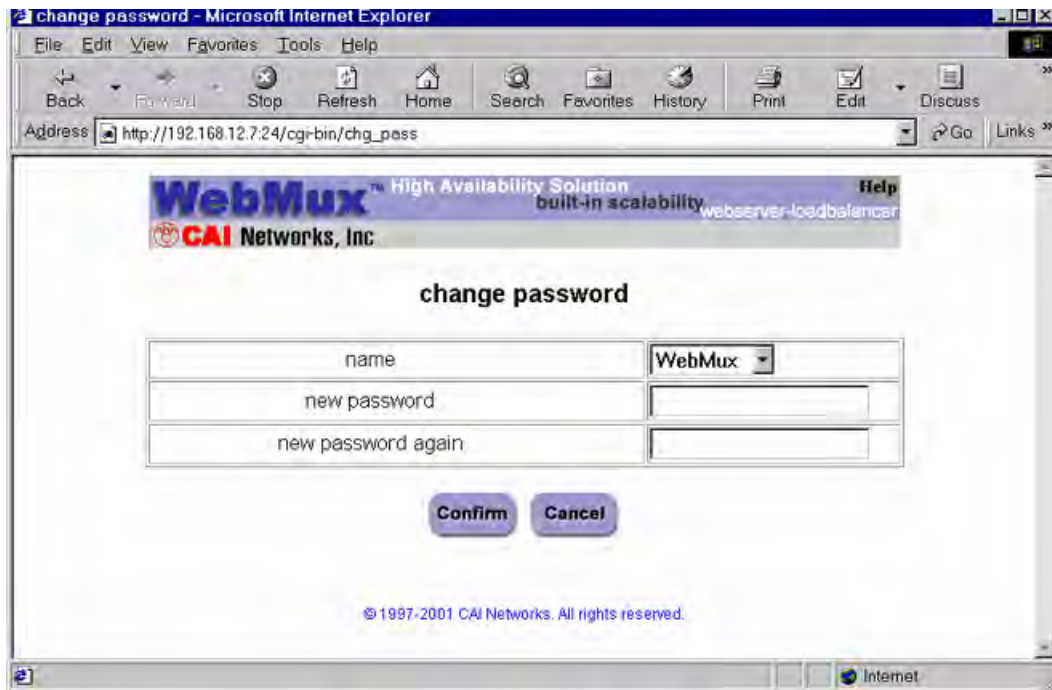
Name:
Select the login name for which the password is to be changed.

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.

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 the WebMux™ internally uses GMT time zone, not your local time zone, per W3C/HTTP protocol. If the timezone is not set correctly, the browser access could be denied due to "cookie" time out. If the UDP NTP server is set up correctly, there is no need to set the clock anymore, since the 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: It is recommended 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 the 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.

Add Farm

Click Add Farm to add a virtual site for the services you want to provide. The "ADD FARM" screen will appear:

By default, the SSL termination is NOT on.

During "Add Farm" action, first select "add HTTP farm", then click on the "Select SSL Termination". Choosing from any key other than "none" will enable SSL termination on the HTTP farm. All the HTTPS incoming traffic will be sent terminated to farms on HTTP port (80). Please set the port to a clear port, since after the WebMux™ terminates the SSL traffic, only clear traffic will go to servers.

When the servers return traffic back, the WebMux™ will re-encrypt the data and send encrypted back to client. If you are using out-of-path mode, please make sure your servers' gateway points to the WebMux™ server LAN gateway IP address; so that the WebMux™ has the chance to re-encrypt the data before replying back to clients.

One can also block not encrypted incoming traffic, so that only encrypted traffic can reach to your server. This might be useful, when you only want encrypted traffic reaching to your servers.

If you like to track on your server if the incoming traffic was HTTPS or HTTP, you may turn on "tag SSL terminated HTTP traffic". By change that to "Yes", decrypted traffic will have the added MIME header "X-WebMux-SSL-termination: true". You can write script on your server to identify if the original traffic was HTTPS or HTTP, and then properly redirect the traffic to the HTTPS.

SSL Keys
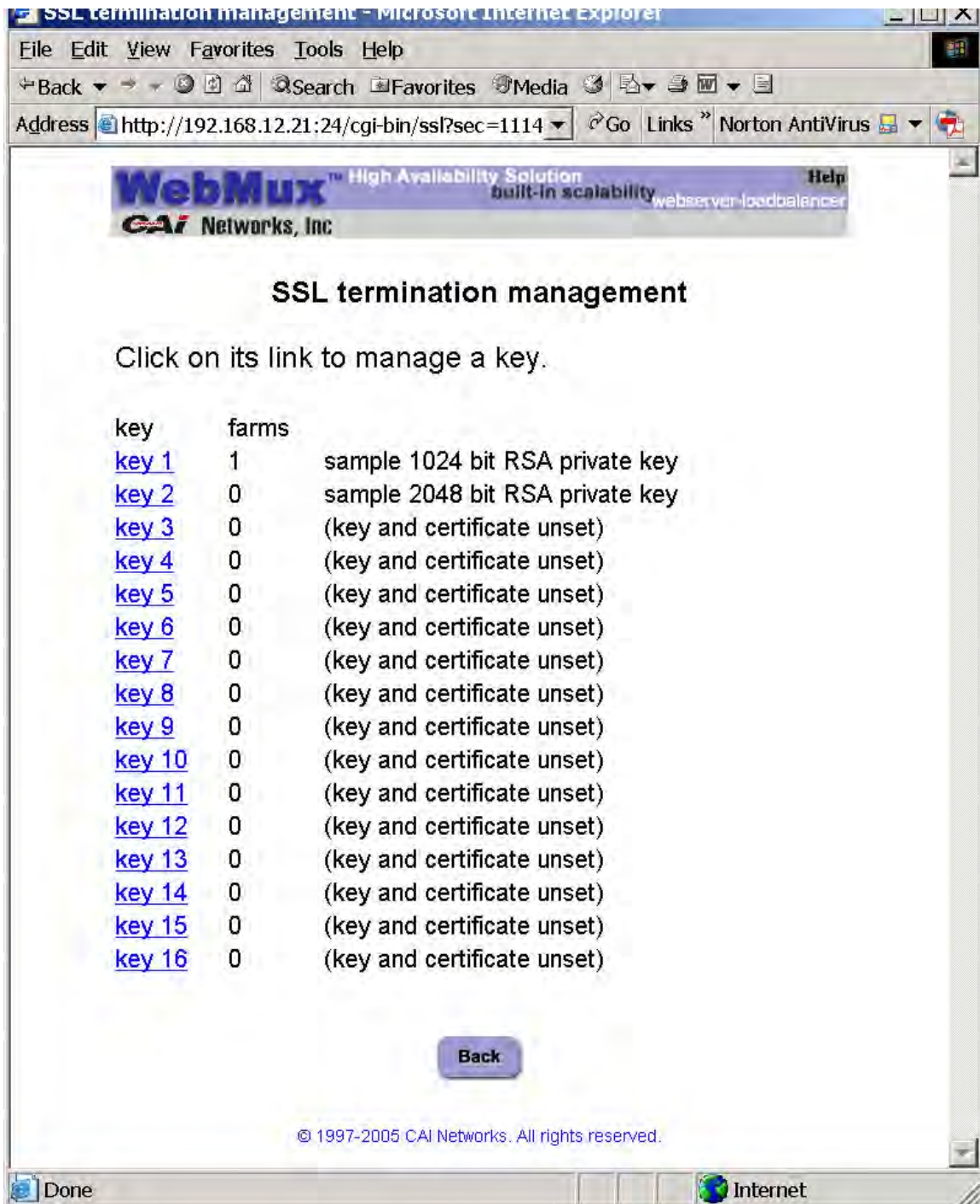
WebMux™ supports SSL V2, SSL V3, and TLS V1 with RSA key length from 512, 1024, and 2048. For each WebMux™, one can have 32 SSL certificates: Any key can be active or not active. The first line of the private key is the comment. See included two sample keys for details. If there is no comment line in the key, it will be blank. If there is no key, it will display "(key and certificate unset)".

Key length can be different from 512 to 2048. RSA key length 1024 also called 128bit strong encryption. You can click "manage key1" or "manage key2" to generate keys, copy and paste signed certificates:
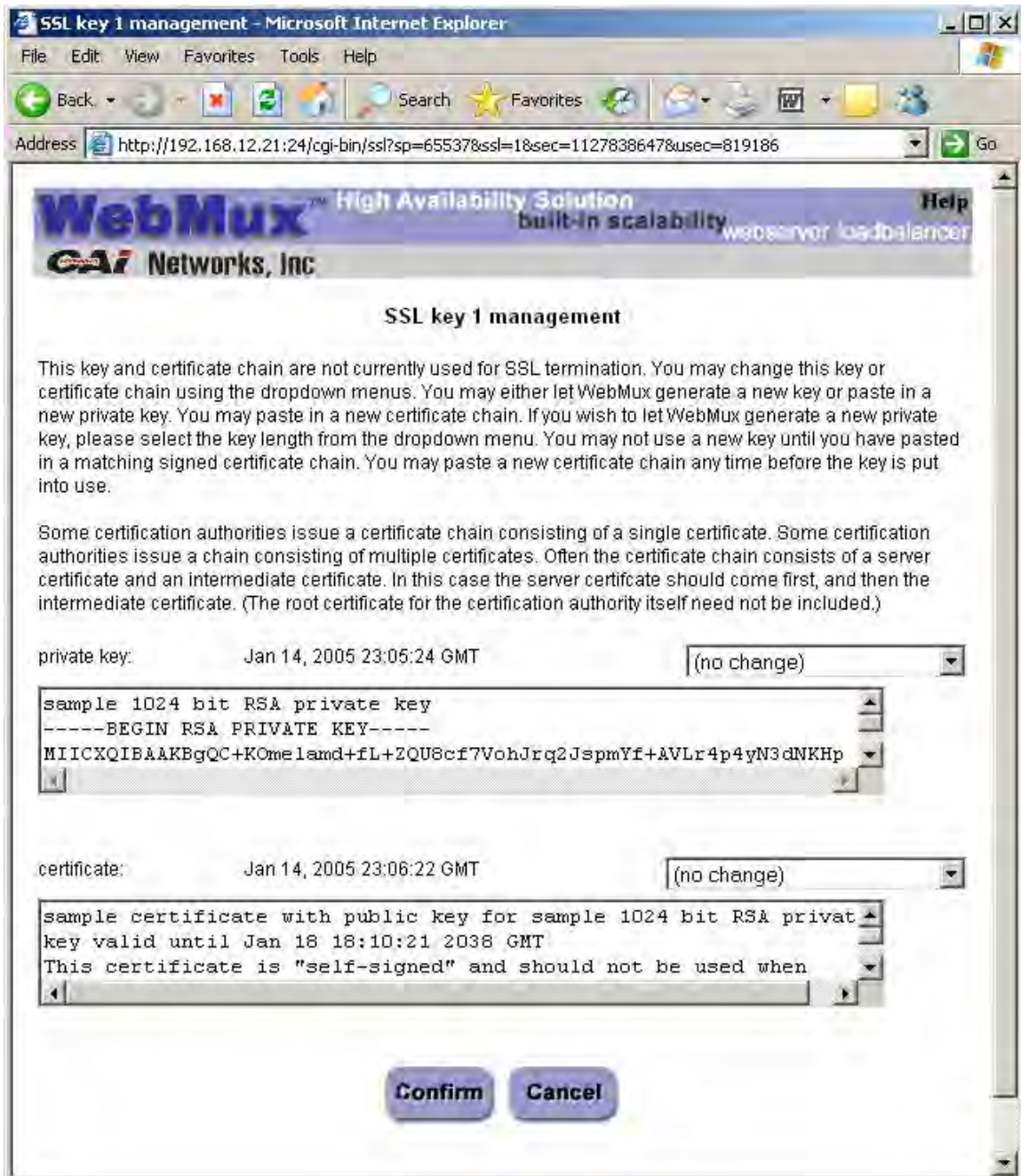
You can view, copy and paste keys into the two windows. You should backup your private key and save in a secure place. Each private key and public key pair must match to be able to work properly.

If you plan to generate new keys, click on the drop down box above the private key window to select key length, and then click on the "Confirm" button. This process is also known as "generate a CSR" – Certificate Signing Request. It is the process that you generated a key pair and send the public key to CA for "signing". Once your public key signed and pasted into the key management screen, all the browsers over Internet will accept it without complaint during its life signed in the key. You can visit www.thawte.com or www.verisign.com for more information.

Enter all the information necessary. Click on "Confirm" button to complete the key generation. You will be taken back to the dialog boxes that will display the newly created private and public keys.

You will then copy and save both private and public keys, submit the public key to the CA of your choice to sign. Once they send you back the signed public key, you will need to paste that into this certificate dialog box, select "using new key pasted in" and click on confirm button to save it into the WebMux™.

There should be 3 certificates. The one whose identity is your e-mail address is the site certificate. The one whose subject and issue are identical is the CA root. The 3rd one is called intermediate certificate. Please paste your site certificate first, followed by your intermediate certificate.
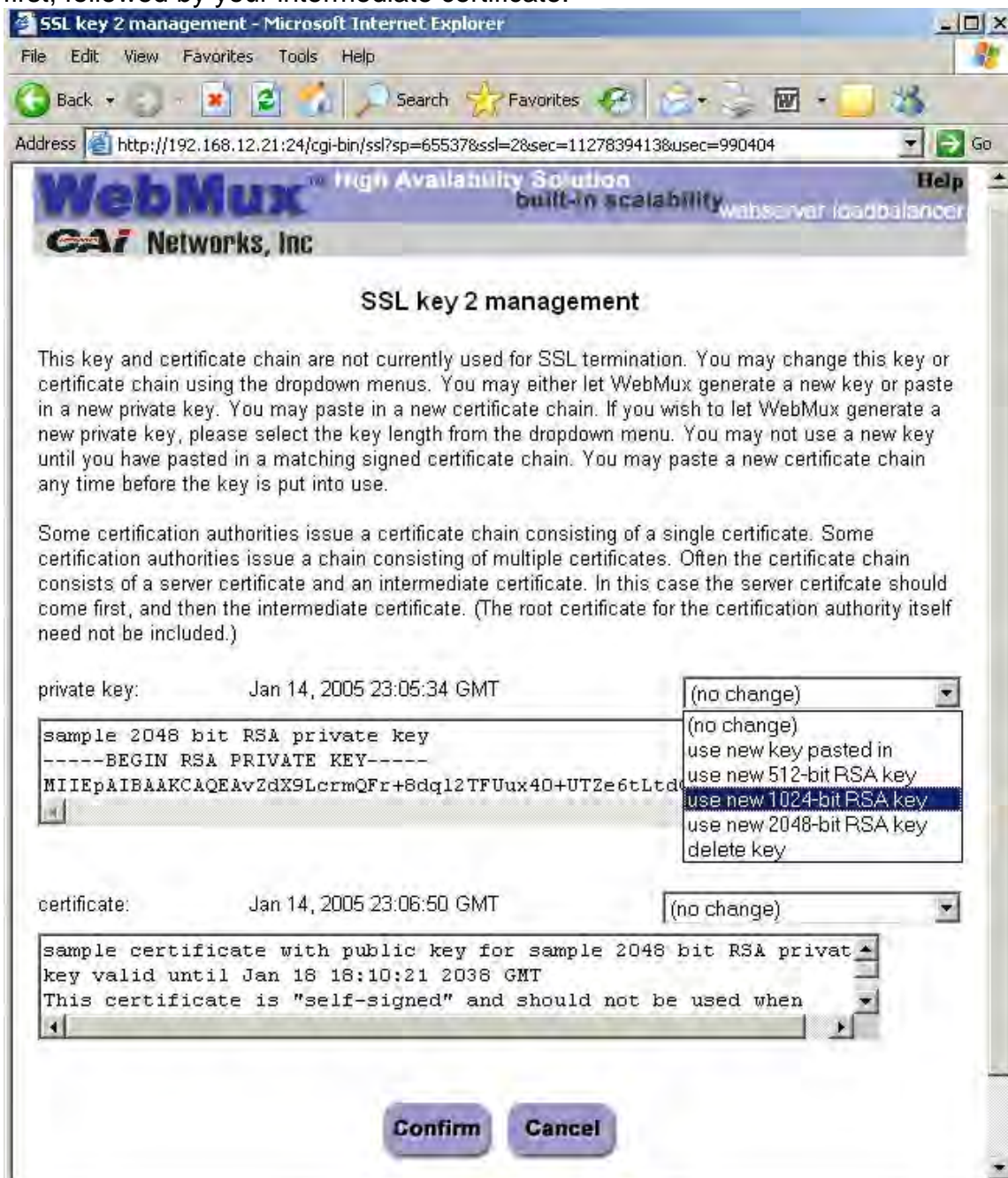
If you have existing signed keys from a Windows IIS server or a Linux server, you can transfer them into the WebMux™ and continue using them until they expire. Please contact us for how to convert your existing keys.

Upload/Download
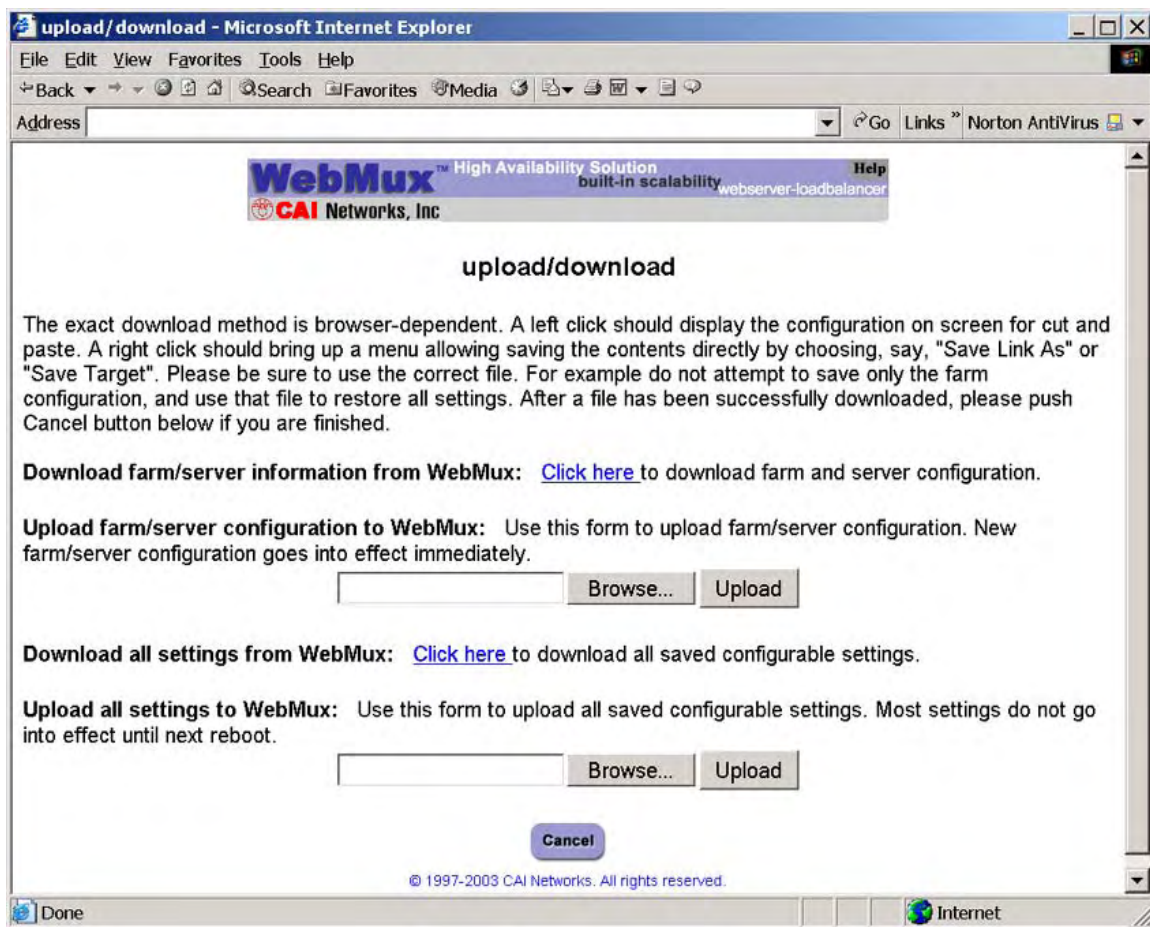
Download:
This feature allows the SAVED (not necessarily the active) configuration to be saved at the Administrative Browser workstation. Click on the **Click Here** to display the configuration. Choose 'File->Save As' from the browser menu to save it as a text file. Changes can be made to this file 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 the WebMux™ with a new unit, you could save the configuration and upload all settings to the WebMux™ , so that you do not need to go

through step by step configuration (requires both WebMuxes on the same firmware revision).

More about Add Farm

Farm IP address:

This is the IP address of the new farm.

For SSL terminated traffic, each farm must have its own IP address.

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.mydomain.com, the farm IP address will be the IP address for www.mydomain.com from your DNS record. If the IP address of www.mydomain.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.

Since version 4.0.3, we also introduced "label" concept for the farms and servers. Once the label is specified, the 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. Since version 5.6, the name label is also being used to check HTTP layer 7 protocols as part of the 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, the WebMux™ considers that server dead. For both IIS and Apache servers doing virtual hosting, the 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 the WebMux™ for your intranet, then the farm IP address will be the IP address of the original web or application server. The web or application servers must be changed their IP addresses so that the WebMux™ can translate farm IP address to the server IP address. You can use the WebMux™ Router LAN IP address as your farm address to save IP address. You can add multiple farms to this IP address, as long as the port number is different.

In the NAT (not TM) mode, the WebMux™ acts as a firewall also, all ports except farm port(s) are blocked. All servers behind the WebMux™ can reach to the outside through the WebMux™ . From outside, the traffic can be seen all come from the WebMux™ router LAN IP address, or proxy address. If a WebMux™ is placed behind a firewall, please add a rule on firewall for WebMux router LAN address to anywhere/anyport. All farm IP addresses should have rules to allow incoming traffic mapped to the address and port number, as well as return traffic for each farm IP address from any port to anywhere.

In Transparent (TM or bridge) mode, there is no firewall protection from WebMux. All servers talk to each other freely cross WebMux. Only the farm IP/port address is being load balanced using any selected scheduling method.

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. If you enabled SSL termination (see last chapter), select port 80 for the farm and servers in the farm. The WebMux™ will terminate all SSL (on port 443) traffic and send them to port 80(DO NOT select port 443 if you enabled SSL termination). For example, if you have five port-80 farms and your WebMux™ only allows one certificate, the WebMux™ will use same certificate for all five farms.

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. The 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 health check (TCP)	User Specify
Generic no health check (UDP)	User Specify
Generic no health check (TCP/UDP)	User Specify

Custom Defined TCP Services	80 or User Specify
Custom Defined UDP Services	User Specify
Custom Defined TCP/UDP Services	User Specify
Custom Defined Paired HTTP and HTTPS (TCP) Service	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
- Layer 7 HTTP URI load directing
- Layer 7 HTTP URI load directing with cookies
- Layer 7 hashed URI load directing

Layer 7 scheduling methods can only be used with the HTTP – Hypertext Transfer Protocol (TCP) service. These scheduling methods allow you to direct traffic to a specific group of servers depending on a match pattern that is compared to the URI in the client's GET request header.

Layer 7 HTTP URI load directing with cookies allows the WebMux™ to direct traffic from the same client to the same server in the farm. This scheduling method also compares the match pattern against the host MIME header. In other words, a host name can be specified as a match pattern. Also, if the server generates a cookie, the WebMux™ will generate its own cookie to keep track of which client session belongs to which server. These are useful for shopping cart services, for example, so that a client will be directed to the same server and keep their shopping cart items valid. The WebMux ™ 's cookie expire time matches the MAX_AGE setting specified in the cookie generated by the servers. When MAX_AGE is not defined, the cookie expire time is 30 minutes.

Layer 7 hashed URI load directing does a mod function on the URI string as part of its load balancing mechanism.

SSL Termination:

Selecting an SSL key in this section will enable SSL termination for this farm.

The HTTP service and POP3 service terminate to ports 443 and 995, repectively, and will allow you to choose any port for the clear traffic to the servers.

When using the generic or custom services, specifying the clear traffic port for the service in the "port number" section causes the WebMux to automatically assume the secure port for the following services:

Clear Traffic Port	Secure Port	Service
80	443	HTTP
110	995	POP3
23	992	Telnet
25	465	SMTP
119	563	NNTP
143	993	IMAP
194	994	IRC
389	636	LDAP

Modify Farm

Modify farm can be invoked from the main management console screen by clicking on the farm IP addresses or labels.
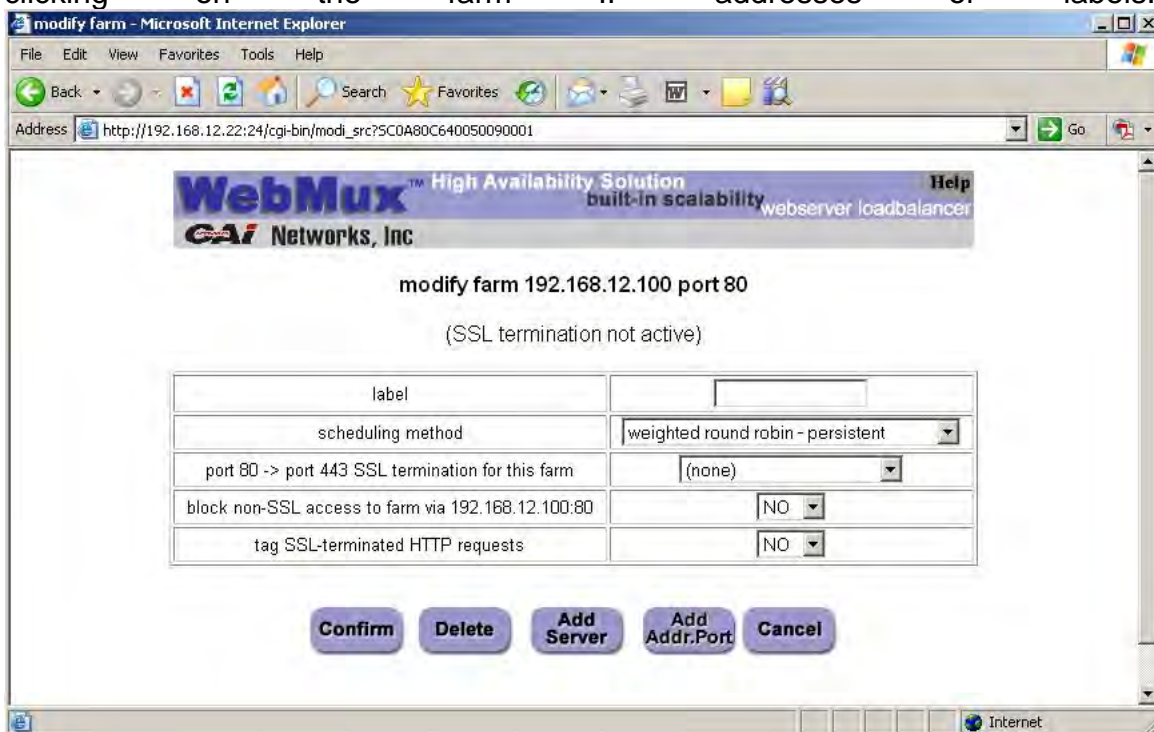
Farm IP address and port number:
These numbers are displayed here for reference purposes. These fields are set in the "Add Farm" screen. Once set, they are not changeable. If they must be changed, delete the farm and then add a new one.

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
- Layer 7 HTTP URI load directing
- Layer 7 HTTP URI load directing with cookies (this method also checks the host MIME header against the specified match pattern)

Key Selection:

You can change the SSL certification/key pair used for this farm. All current connection for this farm will be reset if the key changes.

Block Clear Port:

If you do not want to allow non-encrypted traffic going to server, change the "No" to "Yes".

Tag SSL-terminated HTTP requests:

If SSL termination is active for this farm, choosing "Yes" for this option will add a "X-WebMux-SSL-termination: true" MIME header in the decrypted http request.

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.

Since version 4.0.3, the WebMux™ allows adding a label next to each server's IP address. The purpose of labeling a server is only to help identify 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 setting 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 completed.
- **Favorite Active** – The server will be put into services immediately after it is added. If a Favorite Active server failed, once it is operational, the 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.

Add Address/Port

Click this button using MAP ^{tm} feature to create additional IP address/port protocol combinations for the farm. To use MAP ^{tm} feature, a farm will treat all the related IP address and ports as one, so any port in the MAP failed, the whole server will be taken out from services. The same client will also be send to the same server no matter which port it access within that MAP ^{tm}.
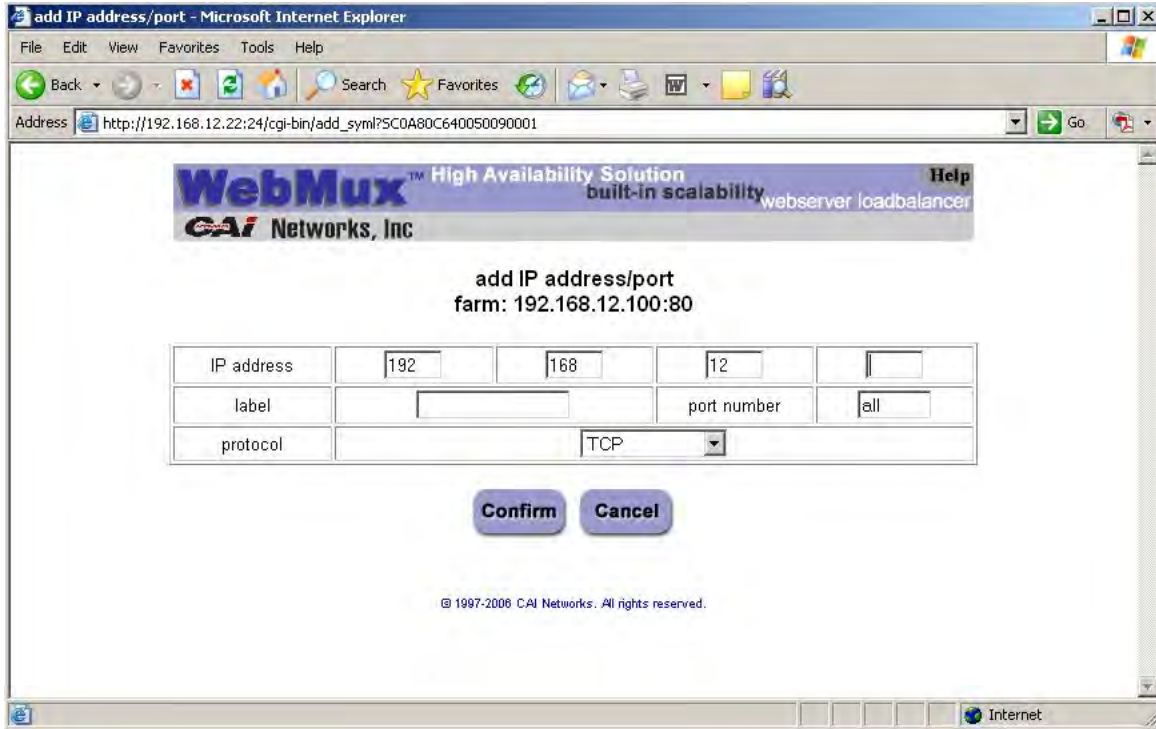
Farm IP and Port:
These numbers are displayed here for reference purposes. These fields are set in the "Add Farm" screen. Once set, they are not changeable. If they must be changed, delete the farm and then add a new one.

IP Address:
Add an IP address to the current farm configuration. The IP address can be the same as long as the port number does not duplicate any existing IP/port combinations.

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.

Port Number:

You can specify a port number that doesn't duplicate any existing IP/port combinations. A port number of "all" will enable all port ranges, but excluding any already existing ports associated with the specified IP address. *Please see the note at the end of this section regarding the behaviors of the additional IP/port in conjunction with SSL termination.*

Protocol:

You can choose TCP, UDP, or combined TCP/UDP.

NOTE: If your farm is already SSL terminated and you create an additional IP/port combination using the main farm IP and specifying the same secure port (or "all"), the SSL termination by the WebMux will be bypassed and SSL will be done directly by the server.

Also, the health check mechanism for the servers is dictated by the main farm service. For example, if the farm is using the http service and you create an additional IP/port for telnet access, the WebMux will continue to monitor the status of the servers via the http service health check. The telnet service is not monitored. If you require that such additional services be monitored, we recommend that you initially create a farm using custom health checking and create a specific CGI scripting that will monitor your specific services.

Add L7 Server

If setting up a Layer 7 farm, the add server screen will be similar to this:

Two options extra options are available:
- Match Pattern
- Pattern is anchored

Match Pattern:
This is the pattern the URI will be compared to. It is stated in extended regular expressions format. Please refer to Appendix 7 for some examples.

Pattern is Anchored:
Will include checking the portion of the URL right after the "http://".

NOTE: If you chose Layer 7 URI load directing with cookies as the scheduling method, the match pattern is also compared to the host MIME header. In other words, you can use a host name as a match pattern criterion.

Modify Server

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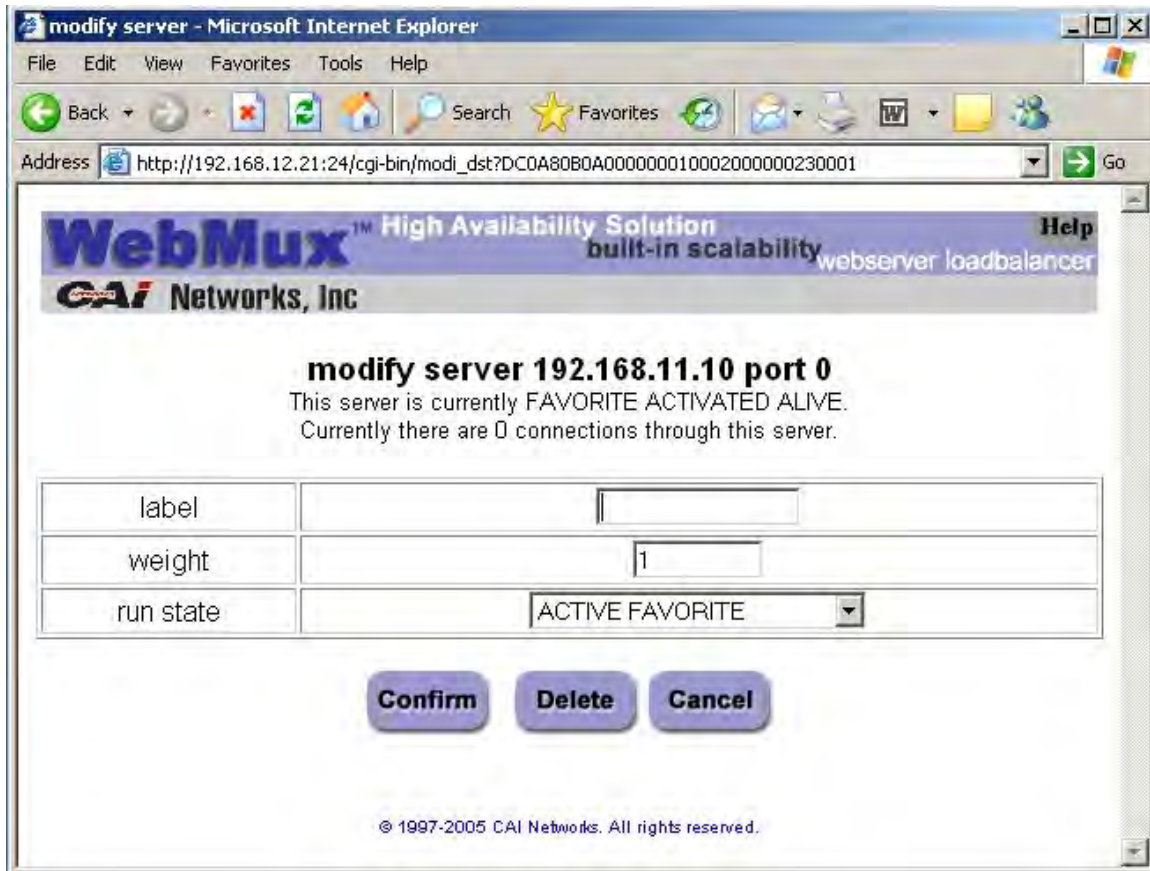
Destination server IP address and port number:

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. Changing the weight to zero will stop the incoming connections while all existing connections continue until time out or connection is terminated by client and server. Although all numbers from 1 to 100 will allow traffic to go through, using a smaller weight number in each server will have the best load distributing result.

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

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, Transparent, or Out-of-Path		
Router LAN Information (NAT ONLY)		
Router LAN WebMux™ Proxy IP Address		
Router LAN Network IP Address Mask		
Server LAN Information (NAT and OOP)		
Server LAN WebMux™ IP Address		
Server LAN Gateway IP Address (optional for OOP)		/////
Server LAN Network IP Address Mask		
Bridge Settings (For Transparent Mode Only)		
WebMux Bridge IP Address		
WebMux Bridge IP Network Mask		
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	Y/N

Sample Configuration Worksheets

Standalone WebMux™ NAT Mode

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, Transparent, 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
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
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.

Standalone WebMux™ Transparent Mode

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, Transparent, or Out-of-Path	Transparent
Bridge Information	
Bridge IP Address	205.133.156.210
Bridge IP Network Mask	255.255.255.0
WebMux™ farm IP Address	205.133.156.200
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**

Out of Path 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, Transparent, or Out-of-Path	Out-of-Path
WebMux™ Server LAN Information	
Server LAN WebMux™ IP Address	10.1.2.254 (any)
Server LAN WebMux™ IP Address Mask	255.255.0.0
Server LAN WebMux™ farm IP Address	10.1.1.200
Server LAN gateway IP address (Necessary for WebMux™ SSL termination and for Layer 7 load balancing. Each server's default gateway needs to be set to this IP)	10.1.1.253
Server Configuration	
Server IP address	No Change
Server NetMask	No Change
Server Default Gateway	No Change
Server Default Gateway (if using WebMux™ for SSL Termination or Layer 7 load balancing)	10.1.1.253
Server add loopback adapter	10.1.1.200
Route Deletion Refer to Appendix 2	10.1.1.200
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 (except if using the WebMux™ for SSL termination or Layer 7 load balancing. See next paragraph). 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.

For SSL termination or Layer 7 load balancing, you must set server LAN gateway IP address and set the servers' default gateway to that IP.

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, Transparent, 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
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

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 67 for how to set the internal clock.

Q. I can't login with my browser because the server does not respond?

R. Your IP address is not on the allowed host list, or the wrong IP addresses were 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 order 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 to quiet the new connections for the server so that it can be taken out of service.

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

For out-of-path mode, a loopback adapter or device in similar function is required. This appendix listed a few different ways to add such a device for different OSes.

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:

For Linux 2.4/2.6 Systems:

Login as root, and add this command to the bootup script:
iptables -t nat -A PREROUTING -d <farm_ip> -j DNAT --to-dest <server_ip>

For IP-based virtual hosting with multiple IPs, repeat the command for each farm IP on all the servers. Don't forget to add the proper farm IP to each virtual host configuration.

With IPv6 addresses, add the IPv6 address of the FARM to "lo" adaptor. Also, be sure that the routing table has an IPv6 entry for the network and a default gateway entry for the real interface of the server. You can check by issuing the "route --inet6" command. See Appendix 8 for other IPv6 related information.

For SUSE Enterprise Linux 9:
You can use YAST to set up a Virtual Interface and add the farm IP.
Login as root, and add this command to the bootup script:
iptables -t nat -A PREROUTING -d <farm_ip> -j DNAT --to-dest <server_ip>

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

For Solaris:
ifconfig lo0:1 FARM_IP_ADDR
ifconfig lo0:1 FARM_IP_ADDR FARM_IP_ADDR
ifconfig lo0:1 netmask 255.255.255.255
ifconfig lo0:1 up
For Apple Servers:
ifconfig lo0 inet farm_ip_addr netmask 255.255.255.255 alias
route delete gateway_ip farm_ip_addr netmask
Where lo0 is the loopback adapter.

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*IIIIIIIIIIII PPPP* - 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*IIIIIIIIIIII PPPP* - 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. The WebMux™ supports virtual hosting by checking the virtual server's response.   There are three different situations for the WebMux™ to handle.

If the service is HTTPS, there is no way to do virtual hosting on the same IP address. 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, the 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 , the WebMux™ actually periodically reads a page from this URL. If server that serves that URL does not response correctly, the WebMux™ will mark that server dead. Since every server in that farm serves all the virtual farms, the 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. The 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.   The 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. The 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, the WebMux™ will excludes that server from serving the farm. If server responses 402, which indicating access is denied for that virtual farm, the 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.

```
#!/bin/bash
echo "Content-type: text/plain"
echo           # blank line
if ps -C sshd &>/dev/null ; then
      echo "OK"        # response from server goes here, see list below.
      echo "SSH service available"
else
      echo "NOT OK"
      echo "SSH daemon not running"
fi
```

The following is a list of valid CGI code responses:

```
OK                - server is alive, no weight change
OVERLOAD          - set weight to 0, to quiesce (same as "WEIGHT=0")
QUIESCE           - set weight to 0, to quiesce (same as "WEIGHT=0")
WEIGHT=n          - set weight to integer n
WEIGHT-=n         - subtract integer n from the weight
WEIGHT+=n         - add integer n to the weight
```

The response must be in all capitals to be recognized. The changes in weight count as an unsaved configuration change. It is not automatically saved.

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.

Appendix 7 – Extended Regular Expressions

Example Patterns:

An item which has the string "Compiler" in it.

```
Compiler
```

Items with various spellings of "Dijkstra" with the j replaced by any character

```
Di.kstra
```

Items with various spellings of "Dijkstra" with the "ijk" replaced by any number of characters

```
D.*stra
```

An item with either "Compiler" or "compiler" in it.

```
[cC]ompiler
```

String like bananas, banananas, bananananas etc.

```
bana(na)+s
```

Items with the strings "regular" and "expression" on the same line with anything or nothing between them

```
regular.*expression
```

Items with either regular or expression (or both).

```
regular|expression
```

Items with either OO or "Object Oriented" or "Object-Oriented" on one line.

```
OO|([oO]bject( |\-)[oO]riented)
```

To search for characters other than letters or digits put a "\" in front of them.

```
S\/SL
```

These examples were taken from the following web page:
http://www.csci.csusb.edu/dick/samples/egrep.html

Appendix 8 – Notes on IPv6

Because IPv6 uses the colon (:) symbol in the address, there are special considerations needed when using the IPv6 address in a web browser because the colon (:) is also used to denote a port number (i.e. 192.168.12.21:24). Because accessing the WebMux's web management requires access to port 24, you cannot simply put the IPv6 address in the address bar of the browser like you would for an IPv4 address. You must enclose the address in brackets ([]). For example, if the IPv6 address of the WebMux is fec0::c0a8:c15, then you would enter http://[fec0::c0a8:c15]:24/cgi-bin/login to get to the web management.

There are also IPv6 versions of some basic networking tools such as ping6, traceroute6, and tcpdump with the IPv6 flag, ip –f inet6, route –inet6, etc. Please be sure that network software/client is indeed IPv6 capable or is the correct IPv6 version to use before assuming that your network is not working.

Also, when adding an IPv6 address to your server's NIC (network interface card), your server's OS might not automatically add a default gateway in its routing table for the IPv6 address. Please double check the routing tables and make sure the proper entries are there. If your servers are not accessible from the outside but are accessible within the subnet, you might want to check and make sure that the default gateway was set up correctly.

Appendix 9 – WebMux SNMP MIB Query ID

.1.3.6.1.4.1.27182.3.1.1.1.11.0
caiWebMuxActive.0
 SYNTAX   INTEGER { true(1), false(2) }
 DESCRIPTION   "Whether this WebMux unit is active."

.1.3.6.1.4.1.27182.3.1.1.1.7.0
caiWebMuxCPUSpeed.0
 SYNTAX   Integer32
 UNITS "MHz"
 DESCRIPTION   "The clock speed of the CPU(s) in this unit."

.1.3.6.1.4.1.27182.3.1.1.1.9.0
caiWebMuxCPUUsage.0
 SYNTAX   Unsigned32
 UNITS "%"
 DESCRIPTION   "The current CPU usage expressed as a
               percentage."

.1.3.6.1.4.1.27182.3.1.1.1.8.0
caiWebMuxCPUs.0
 SYNTAX   Unsigned32
 DESCRIPTION   "The number of CPUs in this unit."

.1.3.6.1.4.1.27182.3.1.1.3.1.9.x.y
caiWebMuxFarmAddressBlockNonSSL.x.y
 SYNTAX   INTEGER { true(1), false(2) }
 DESCRIPTION   "If the value of this object is true(1), then
               connections to the IP address given for this
               row that are not using SSL will not be
               accepted."

.1.3.6.1.4.1.27182.3.1.1.3.1.5.x.y
caiWebMuxFarmAddressIPv4.x.y
 SYNTAX   IpAddress
 DESCRIPTION   "An IPv4 address used to access the service
               provided by this server farm."

.1.3.6.1.4.1.27182.3.1.1.3.1.6.x.y
caiWebMuxFarmAddressIPv6.x.y
 SYNTAX   OCTET STRING (16)
 DESCRIPTION   "An IPv6 address used to access the service
               provided by this server farm."

.1.3.6.1.4.1.27182.3.1.1.3.1.3.x.y
caiWebMuxFarmAddressLabel.x.y
  SYNTAX   OCTET STRING (0..255)
  DESCRIPTION   "The mnemonic label assigned to this address
                and port for a server farm."

.1.3.6.1.4.1.27182.3.1.1.3.1.7.x.y
caiWebMuxFarmAddressPort.x.y
  SYNTAX   Unsigned32 (1..65535)
  DESCRIPTION   "A TCP or UDP port number used to access the
                service provided by this server farm."

.1.3.6.1.4.1.27182.3.1.1.3.1.2.x.y
caiWebMuxFarmAddressRowStatus.x.y
  SYNTAX   INTEGER { active(1), notInService(2), notReady(3), createAndGo(4
), createAndWait(5), destroy(6) }
  DESCRIPTION   "The status of this row. As this table is
                read-only, the value of this object will
                always be active(1) at the present time."

.1.3.6.1.4.1.27182.3.1.1.3.1.8.x.y
caiWebMuxFarmAddressSSLPort.x.y
  SYNTAX   Unsigned32 (1..65535)
  DESCRIPTION   "A port number used to access the
                service provided by this server farm securely
                using the secure sockets layer (SSL)."

.1.3.6.1.4.1.27182.3.1.1.3.1.4.x.y
caiWebMuxFarmAddressService.x.y
  SYNTAX   OCTET STRING (0..255)
  DESCRIPTION   "The type of service provided by this address and
                port for this server farm."

.1.3.6.1.4.1.27182.3.1.1.3.1.10.x.y
caiWebMuxFarmAddressTagSSL.x.y
  SYNTAX   INTEGER { true(1), false(2) }
  DESCRIPTION   "If the value of this object is true(1), then
                HTTP requests to the IP address given for this
                row that are using SSL will have the following
                header line added:"

.1.3.6.1.4.1.27182.3.1.1.2.1.4.x
caiWebMuxFarmConnections.x
  SYNTAX   Counter32
  DESCRIPTION   "The current number of connections being
                serviced by this server farm.

The total number of connections serviced by
this server farm.

XXX delete as appropriate
"

.1.3.6.1.4.1.27182.3.1.1.2.1.5.x
caiWebMuxFarmConnectionsPerSec.x
  SYNTAX   Gauge32
  DESCRIPTION   "The current rate of incoming server
               connections for this server farm."

.1.3.6.1.4.1.27182.3.1.1.2.1.6.x
caiWebMuxFarmPacketsPerSec.x
  SYNTAX   Gauge32
  DESCRIPTION   "The current rate of incoming packets
               for this server farm."

.1.3.6.1.4.1.27182.3.1.1.2.1.2.x
caiWebMuxFarmRowStatus.x
  SYNTAX   INTEGER { active(1), notInService(2), notReady(3), createAndGo(4
), createAndWait(5), destroy(6) }
  DESCRIPTION   "The status of this row. As this table is
               read-only, the value of this object will
               always be active(1) at the present time."

.1.3.6.1.4.1.27182.3.1.1.2.1.3.x
caiWebMuxFarmScheduling.x
  SYNTAX   OCTET STRING (0..255)
  DESCRIPTION   "The load balancing alhorithm used to
               distribute incoming connections amongs the
               servers of this farm."

.1.3.6.1.4.1.27182.3.1.1.1.3.0
caiWebMuxFirmwareDate.0
  SYNTAX   OCTET STRING (8 | 11)
  DESCRIPTION   "The date and time the current firmware
               version was built."

.1.3.6.1.4.1.27182.3.1.1.1.16.1.4.x
caiWebMuxIfCurrentLinkSpeed.x
  SYNTAX   Unsigned32
  UNITS "Mbps"
  DESCRIPTION   "The current link speed of this interface, in
               megabits per seconds (Mbps)."

```
------------------------------------------------------------------------
.1.3.6.1.4.1.27182.3.1.1.1.16.1.x.y
caiWebMuxIfIPv4Address.x
  SYNTAX        IpAddress
  DESCRIPTION   "The IPv4 address of this interface."
------------------------------------------------------------------------
.1.3.6.1.4.1.27182.3.1.1.1.16.1.2.x
caiWebMuxIfIPv6Address.x
  SYNTAX        OCTET STRING (16)
  DESCRIPTION   "The IPv6 address of this interface."
------------------------------------------------------------------------
.1.3.6.1.4.1.27182.3.1.1.1.16.1.5.x
caiWebMuxIfLinkUp.x
  SYNTAX        INTEGER { true(1), false(2) }
  DESCRIPTION   "If this interface is up and running, the
                value of this object will be true(1)."
------------------------------------------------------------------------
.1.3.6.1.4.1.27182.3.1.1.1.16.1.3.x
caiWebMuxIfMaxLinkSpeed.x
  SYNTAX        Unsigned32
  UNITS "Mbps"
  DESCRIPTION   "The maximum link speed of this interface, in
                megabits per seconds (Mbps)."
------------------------------------------------------------------------
.1.3.6.1.4.1.27182.3.1.1.1.5.0
caiWebMuxManufactured.0
  SYNTAX        OCTET STRING (8 | 11)
  DESCRIPTION   "The date and time of manufacture of this
                unit."
------------------------------------------------------------------------
.1.3.6.1.4.1.27182.3.1.1.1.10.0
caiWebMuxMemoryUsage.0
  SYNTAX        Unsigned32
  UNITS "%"
  DESCRIPTION   "The current memory usage expressed as a
                percentage."
------------------------------------------------------------------------
.1.3.6.1.4.1.27182.3.1.1.1.4.0
caiWebMuxModel.0
  SYNTAX        OBJECT IDENTIFIER
  DESCRIPTION   "An object identifier uniquely identifying
                which model of WebMux this is.  The possible
                set of identifiers is given under the
                caiWebMuxFamily sub-tree.  Note that the
                SNMPv2-MIB object sysObjectID.0 will have the
                same value as this object in all cases."
```

.1.3.6.1.4.1.27182.3.1.1.1.1.0
caiWebMuxName.0
  SYNTAX   OCTET STRING (0..255)
  DESCRIPTION   "The assigned name of this WebMux unit."

.1.3.6.1.4.1.27182.3.1.1.1.13.0
caiWebMuxPrimary.0
  SYNTAX   INTEGER { true(1), false(2) }
  DESCRIPTION   "The value of this object is true(1) if this
                WebMux is the primary partner of a redundant
                pair, or is running solo. The value of this
                object is false(2) if this WebMux is the
                secondary partner of a redundant pair."

.1.3.6.1.4.1.27182.3.1.1.1.6.0
caiWebMuxSerialNumber.0
  SYNTAX   OCTET STRING (0..255)
  DESCRIPTION   "The unique serial number of this unit."

.1.3.6.1.4.1.27182.3.1.1.4.1.4.x.y
caiWebMuxServerAddressIPv4.x.y
  SYNTAX   IpAddress
  DESCRIPTION   "The IPv4 address of this server."

.1.3.6.1.4.1.27182.3.1.1.4.1.5.x.y
caiWebMuxServerAddressIPv6.x.y
  SYNTAX   OCTET STRING (16)
  DESCRIPTION   "The IPv6 address of this server."

.1.3.6.1.4.1.27182.3.1.1.4.1.9.x.y
caiWebMuxServerConnections.x.y
  SYNTAX   Counter32
  DESCRIPTION   "The current number of connections being
                serviced by this server.

                The total number of connections serviced by
                this server.

                XXX delete as appropriate
                "

.1.3.6.1.4.1.27182.3.1.1.4.1.10.x.y
caiWebMuxServerConnectionsPerSec.x.y
  SYNTAX   Gauge32
  DESCRIPTION   "The current rate of connections being

serviced by this server."

.1.3.6.1.4.1.27182.3.1.1.4.1.14.x.y
caiWebMuxServerError.x.y
  SYNTAX   Integer32
  DESCRIPTION   "most recent error code for server if available"

.1.3.6.1.4.1.27182.3.1.1.4.1.7.x.y
caiWebMuxServerL7Pattern.x.y
  SYNTAX   OCTET STRING (0..255)
  DESCRIPTION   "The layer 7 pattern to match a request
              against for this server."

.1.3.6.1.4.1.27182.3.1.1.4.1.8.x.y
caiWebMuxServerL7PatternAnchored.x.y
  SYNTAX   INTEGER { true(1), false(2) }
  DESCRIPTION   "If the value of this object is true(1) then
              the layer 7 pattern to be matched has the
              leading '/' included."

.1.3.6.1.4.1.27182.3.1.1.4.1.3.x.y
caiWebMuxServerLabel.x.y
  SYNTAX   OCTET STRING (0..255)
  DESCRIPTION   "The mnemonic label assigned to this server."

.1.3.6.1.4.1.27182.3.1.1.4.1.11.x.y
caiWebMuxServerPacketsPerSec.x.y
  SYNTAX   Gauge32
  DESCRIPTION   "The current rate of packets being sent to
              this server."

.1.3.6.1.4.1.27182.3.1.1.4.1.6.x.y
caiWebMuxServerPort.x.y
  SYNTAX   Unsigned32 (1..65535)
  DESCRIPTION   "The TCP or UDP port number used to access
              the service on the provided address."

.1.3.6.1.4.1.27182.3.1.1.4.1.2.x.y
caiWebMuxServerRowStatus.x.y
  SYNTAX   INTEGER { active(1), notInService(2), notReady(3), createAndGo(4
), createAndWait(5), destroy(6) }
  DESCRIPTION   "The status of this row. As this table is
              read-only, the value of this object will
              always be active(1) at the present time."

.1.3.6.1.4.1.27182.3.1.1.4.1.12.x.y

caiWebMuxServerState.x.y
  SYNTAX   Unsigned32
  DESCRIPTION   "The current state of this server. The bits
                have the following meaning:

                Bit   Meaning
                0x0001 If bit set server is available

                0x0002 If bit set WebMux will send traffic
                    to this server

                0x0020 If bit set always try to use this
                    server if it is available

                0x0040 If bit set, only try to use this
                    server if no other server in the farm
                    is available
                "

.1.3.6.1.4.1.27182.3.1.1.4.1.13.x.y
caiWebMuxServerWeight.x.y
  SYNTAX   Unsigned32 (1..100)
  DESCRIPTION   "The current rate of packets being sent to
                this server."

.1.3.6.1.4.1.27182.3.1.1.1.12.0
caiWebMuxSolo.0
  SYNTAX   INTEGER { true(1), false(2) }
  DESCRIPTION   "The value of this object is true(1) if this
                WebMux is running solo, or false(2) if this
                WebMux is part of a redundant pair."

.1.3.6.1.4.1.27182.3.1.1.1.2.0
caiWebMuxVersion.0
  SYNTAX   OCTET STRING (0..255)
  DESCRIPTION   "The WebMux firmware version running this
                WebMux unit."

Index

H

Hardware Setup · 22, 23
HDD light · 1
health check · 4, 39, 55

I

IPv6 · 5, 34, 82, 90, 91

L

LAN 1 port · 1
LAN 2 port · 1
LAN 3 port · 1
LAN 4 port · 1
LAN 5 port · 1
LAN 6 port · 1
LAN 7 port · 1
LAN 8 Port · 1
Layer 7 · 5, 7, 18, 36, 56, 57, 59, 64, 72, 73
Link Aggregation Control Protocol (LACP) · 9
loopback · 17, 27, 72, 73, 83
Loopback · 81

M

management console · 29, 34, 36, 78
MAP · 6, 62
MIB · 91, 94
MIME · 5, 45, 54, 56, 59, 64
Modify · 29, 58, 65

N

NAT · 5, 9, 10, 23, 26, *See*
netmask · 13, 34, 73
NTP · 40, 42, 55

O

out-of-path · 17, 45, 81
Out-of-Path · 5, 9, 11, 17, 18, 19, 26, 39
OVERLOAD · 87
Overview · 4, 9

P

pager · 5, 33, 35, 84
paging · 35
passwd · 27, 68, 69, 71, 72, 74
Pattern · 64
persistent · 37, 39, 56, 57, 58, 59, 83
Power Cord · 3
Power Indicator · 2
primary · 15
Proxy · 4, 67, 69, 71, 74
public key · 47, 48
PWR light · 2