

LoadMaster Quick-Start Guide

for the LM-1500, LM-2460, LM-2500, LM-2500 Lite, LM-2860, LM-3620, SM-1020

This guide serves as a complement to the LoadMaster documentation, and is meant to get a new user up and running with basic functionality quickly. It is not a replacement for the full LoadMaster documentation. For concepts and issues not covered in this document, consult the *LoadMaster Installation and Configuration Guide*, located on the enclosed CD.

Table of Contents

What You Will Need.....	2
Network Considerations.....	2
One-armed.....	2
Two-armed.....	3
Default Gateway.....	4
IP Addressing.....	4
Connecting to the LoadMaster.....	5
VGA Console.....	5
Serial Connection.....	5
Initial Setup.....	6
HA Configuration: HA-2 Setup.....	11
Final Step.....	13
Web User Interface (WUI).....	14
Connecting for the First Time.....	14
Configuring a Virtual Service.....	15
SSH Access.....	18
SSL Acceleration/Offloading.....	21
Configuring SSL Virtual Service with Acceleration.....	21
Self-Signed Certificate.....	23



What You Will Need

In order to get started with the LoadMaster, you will need the following items:

- A monitor with standard VGA 15-pin connection and USB keyboard

or

- A serial cable (included), workstation with serial port, and a terminal emulator (such as HyperTerminal for Windows)

In addition, you will also need:

- A LoadMaster with:
 - Power cable
 - Ethernet cable(s)
- An SSH client (such as the freeware PuTTY for Windows)
- A standard browser, such as Internet Explorer, Firefox, Mozilla, or Apple Safari

This document also assumes you are familiar with the basics of TCP/IP networking, web serving, and fundamental network topology.

Network Considerations

Before setting up the LoadMaster, take a moment to consider how the LoadMaster will fit into your network. Generally, there are two main implementations of the LoadMaster in a given network environment: One-armed configuration and two-armed configuration. (There are also variations of those implementations, such as Direct Server Return, which are covered in the *LoadMaster Installation and Configuration Guide*.)

One-armed

In a one-armed configuration, the virtual servers and the real servers are on the same subnet. The LoadMaster connects to the Layer 2 network through one interface, eth0 (referred to as the Network side, versus the Farm side for eth1).



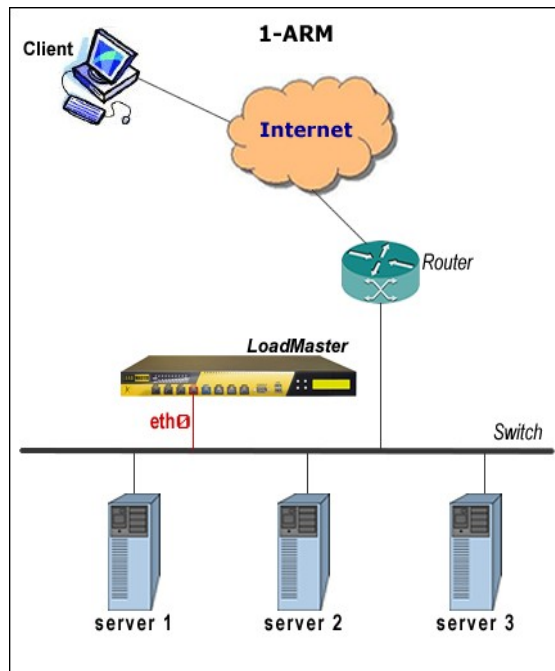


Figure 1: One-armed Configuration

If you already have a firewall in place performing NAT, a one-armed LoadMaster configuration may be preferable. In that instance, the real servers would be on a public DMZ network or a non-routed IP space (such as a 192.168.0.0 or 10.0.0.0 network) and the firewall provides NAT (Network Address Translation) from publicly accessible space.

Two-armed

In a two-armed scenario, the virtual servers and the real servers are on two different subnets. The LoadMaster connects to two networks, one for the virtual servers (usually the public Internet), and one network for the real servers (called the Farm network).



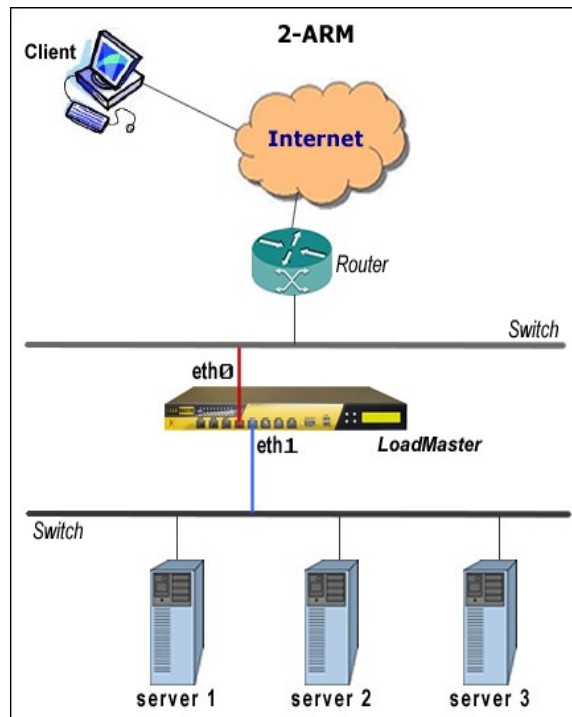


Figure 2: Two-armed configuration

Default Gateway

Another consideration in setting up a LoadMaster is the default gateway on the servers themselves (sometimes referred to as the default route). In a one-armed configuration, it is necessary to have the LoadMaster as the default gateway. There are some situations where the LoadMaster doesn't need to be the default gateway, but those have various limitations in terms of logging on the real servers. In a two-armed configuration, it is necessary to have the LoadMaster as the default route.

Management IP Addressing

If you're implementing the LoadMaster in a standalone configuration (a single LoadMaster), then you'll need a single dedicated IP address for every interface that you utilize. If you're implementing the LoadMaster in a redundant HA configuration (when two units are utilized, one active and one standby for redundancy), you'll need *three* IP addresses for each network interface utilized. In this scenario, each LoadMaster will have its own IP address, and there will be a shared IP address between them, hence the three IP addresses. This is only for management purposes. You will add additional IPs later for virtual services.

In HA configurations, the shared IP address on the subnet of the real servers will be the real server's default gateway address.

Table 1 and Table 2 show the IP addressing scheme for both a standalone and HA



configurations for a two-armed configuration with the Network side (eth0) on a subnet of 192.168.0.0/24, and the Farm side (eth1) on a subnet of 192.168.1.0/24.

<i>Network Segment</i>	<i>Interface</i>	<i>Subnet</i>	<i>IP Address</i>
Network side	eth0	192.168.0.0/24	192.168.0.10
Farm side	eth1	192.168.1.0/24	192.168.1.10

Table 1: Standalone IP addressing

<i>Network Segment</i>	<i>Interface</i>	<i>Subnet</i>	<i>IP Address</i>
Network side	eth0	192.168.0.0/24	Shared: 192.168.0.10 HA-1: 192.168.0.11 HA-2: 192.168.0.12
Farm side	eth1	192.168.1.0/24	Shared: 192.168.1.10 HA-1: 192.168.1.11 HA-2: 192.168.1.12

Table 2: HA IP addressing

Again, these are the for the management IP addresses, that act as default gateways for real servers and as access IPs for administration. IPs for virtual services are added later through the WUI.

Connecting to the LoadMaster

For the initial setup of the LoadMaster, configuration must be done one of two ways: Through the serial console, or with a standard monitor and USB keyboard. Both result in the same configuration procedure, so whatever method suits your needs best will work. (Note: If your 1500-1U unit does not have a VGA port, you will need a serial connection.)

VGA Console

You can make the initial configuration with the LoadMaster through a standard monitor (with 15-pin VGA connector) and a USB keyboard. Simply plug the display and keyboard in and power the LoadMaster on.

Serial Connection

A serial connection is also an option. For this you'll need a serial cable (included with the LoadMaster) and a terminal emulation program to connect through the serial port on a workstation. For Windows users, a commonly used terminal emulation program is HyperTerminal, and is generally included with Windows (located under Programs,



Accessories, Communications).

In Linux, a popular terminal program is minicom, which is included in many distributions or easily obtained.

You'll need to set your terminal emulation program with the following settings:

- Speed: 115200 (note, HyperTerminal defaults to 2400, and many others default to 9600)
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None

Below is how the configuration would look under HyperTerminal:

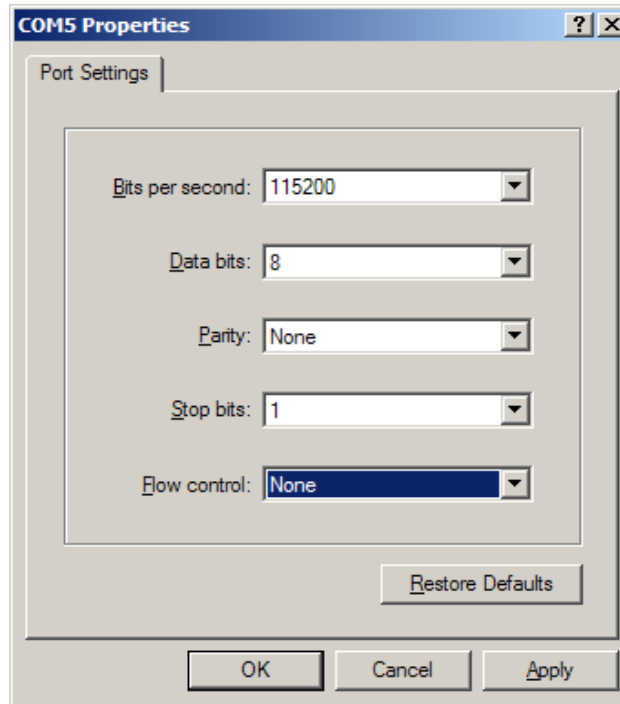


Figure 3: HyperTerminal COM Port Properties

Initial Setup

HA Note: If you've purchased an HA configuration, first setup the system that came with the HA-1 licensing, and the HA-2 system second.

Whether you're connected through a monitor and keyboard or through the serial port, you'll be presented with a login screen:



LoadMaster from KEMP Technologies
(c) 2002-2004 Brain Force Software GmbH
Version 3.1-57

lb100 login:

Log into the LoadMaster with the username “**bal**”, and password of “**1fourall**”.

If the LoadMaster was shipped from the factory with the license installed, you'll be presented with a textual menu (Figure 4). Select option one for “Quick Setup”.

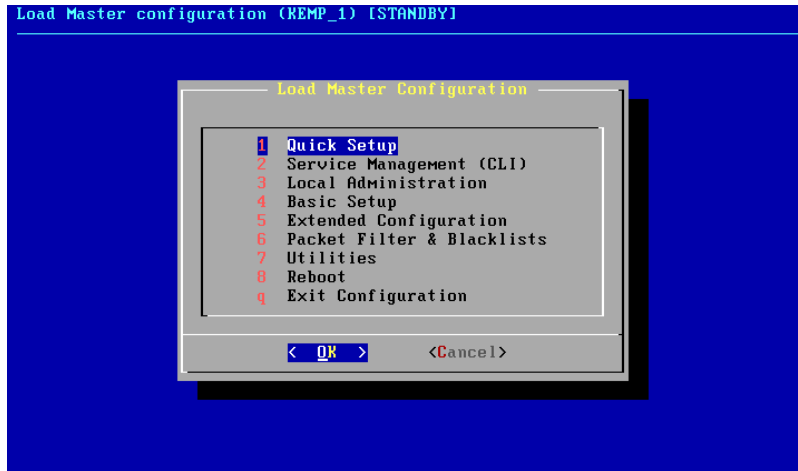


Figure 4: First Login Menu

If the license was not pre-installed, enter the license information as requested, and the Quick Setup will be started automatically.

The first screen the Quick Setup will ask you for is the IP address of the Network-side interface (Figure 5). This is the interface where the virtual servers will reside. If you are using a one-armed configuration, this will be the only interface you'll configure. For two-armed, you'll also configure the Farm-side interface (eth1) in a later step.



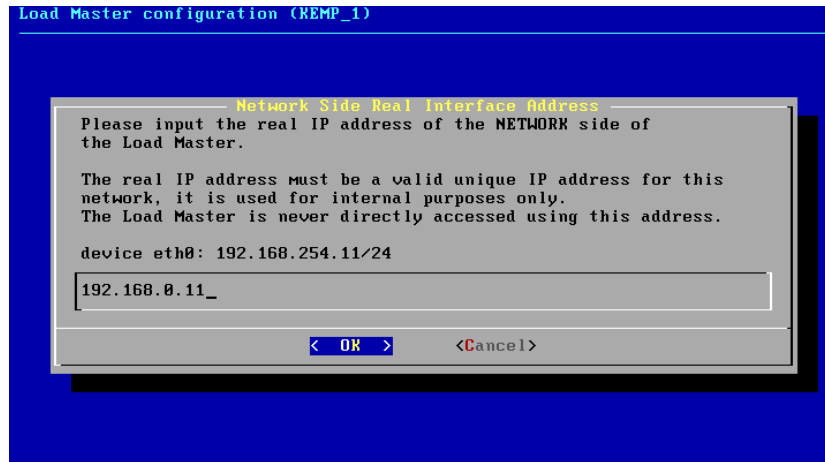


Figure 5: Network-side IP Configuration

You'll then be asked for the netmask. You can enter the netmask in one of two formats: Either the conventional four-octet method, such as 255.255.255.0 for a Class C, or the CIDR format, where the Class C would be represented as /24.

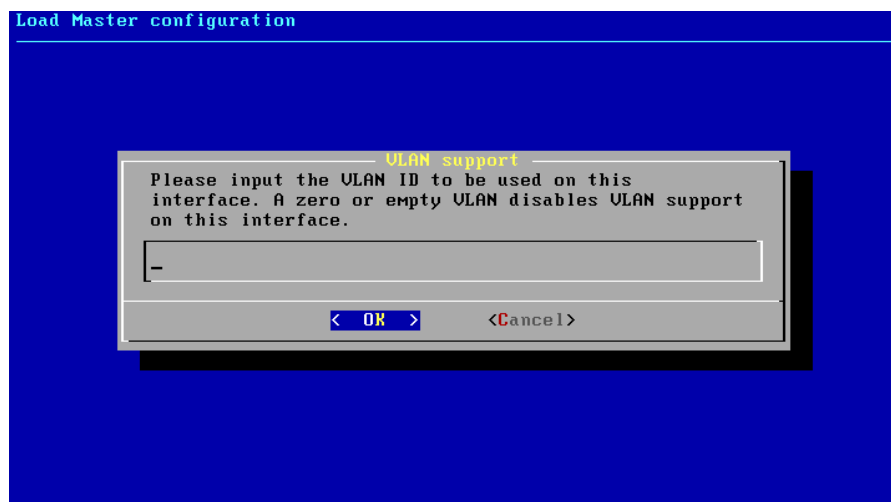


Figure 6: Quick Start VLAN Configuration

Next (Figure 6), the Quick Setup asks for the a VLAN ID. Leave this entry blank. The LoadMaster will function fine on a network with or without VLANs with this option blank. It is only when the switch port that the LoadMaster is connected to is specifically configured for 802.1Q VLAN tagging that a value for this option is required, and that is not a common (or recommended) configuration.

If you've purchased and HA configuration, you'll then be asked for the shared IP address (Figure 7).



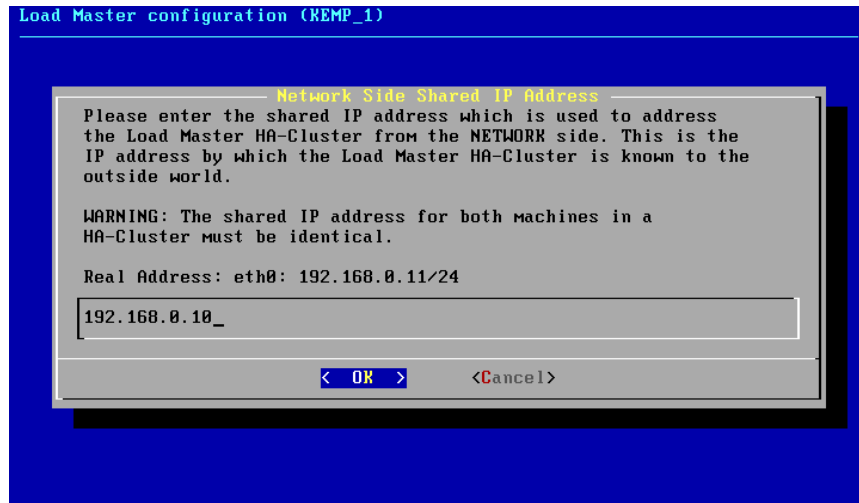


Figure 7: Shared IP Address

The shared IP address is the IP you'll use to connect to the LoadMaster for the web user interface (HTTPS). The shared IP will be held by the active unit in the HA pair (and changes on the WUI made on the active unit will be duplicated on the standby unit automatically).

You'll be asked for the same information for the Farm side interface (eth1). If you're not using the Farm side interface (such as a one-armed configuration), leave the field blank, and Quick Setup will skip the Farm side configuration (Figure 8). If you are using the Farm side, input the information just as you did for the Network side.

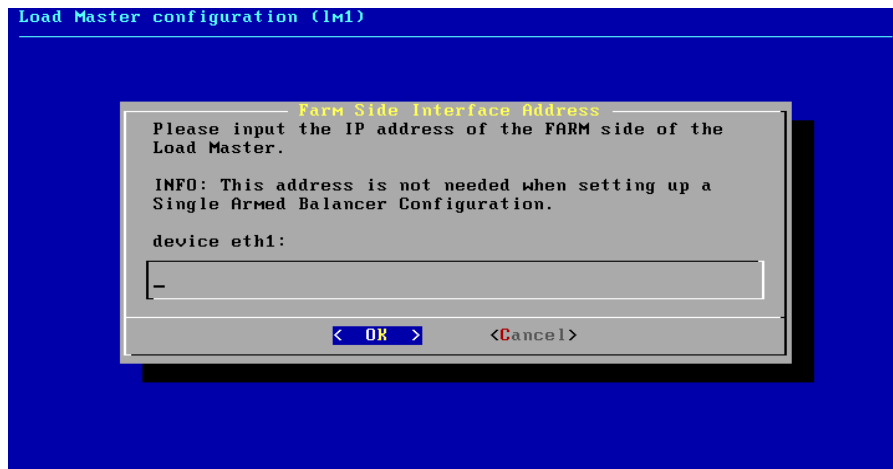


Figure 8: Farm-side (eth1) IP Address

Next (Figure 9), choose a hostname for the LoadMaster. You can use your own naming convention for this. In this example, the LoadMaster is given the name “lm1”.



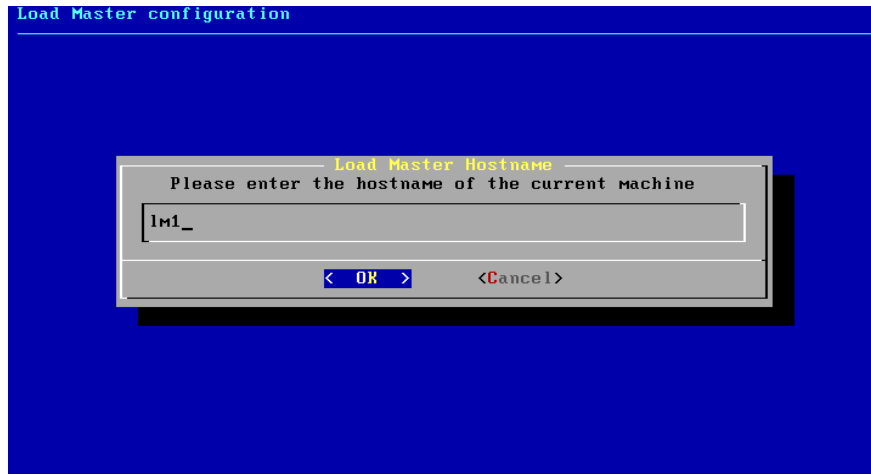


Figure 9: Hostname Configuration

If you've got an HA configuration, the Quick Setup will also ask you for the name of the secondary unit. In this example (Figure 10), it will be named lm2.

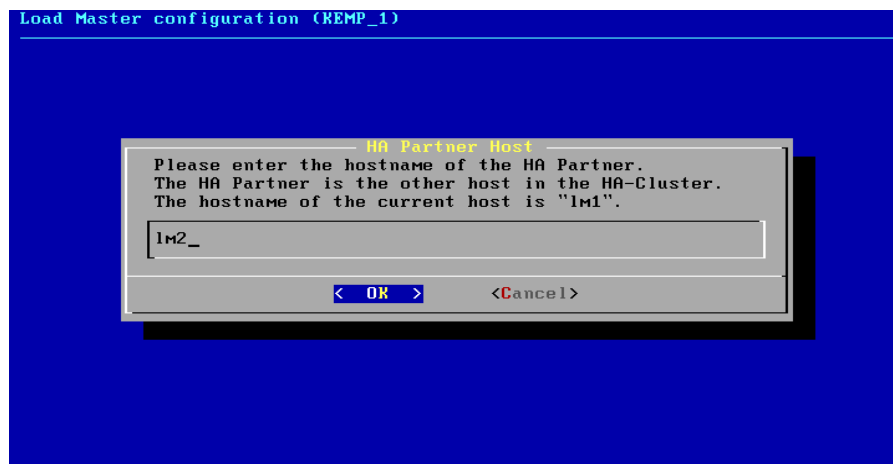


Figure 10: HA-2 name

For the "Name Server IP Addresses" screen (Figure 11), give the LoadMaster at least one IP address of an accessible nameserver.



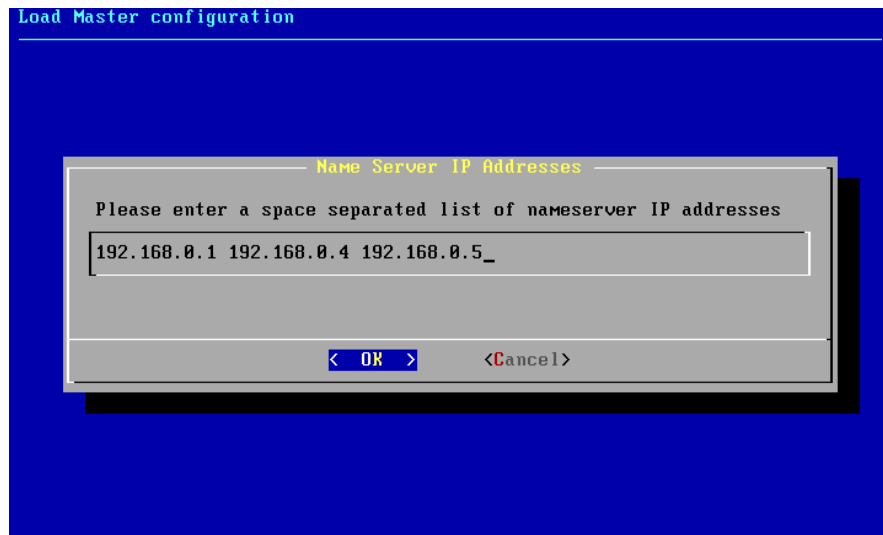


Figure 11: Name Server IP Entry

You'll next be asked for a list of search domains. You can enter in domains, or you can leave this blank.

Enter the default gateway that the LoadMaster will use to access the Internet (Figure 12). This will be on the Network-side interface, eth0. This is the same regardless of a one-armed or two-armed configuration.

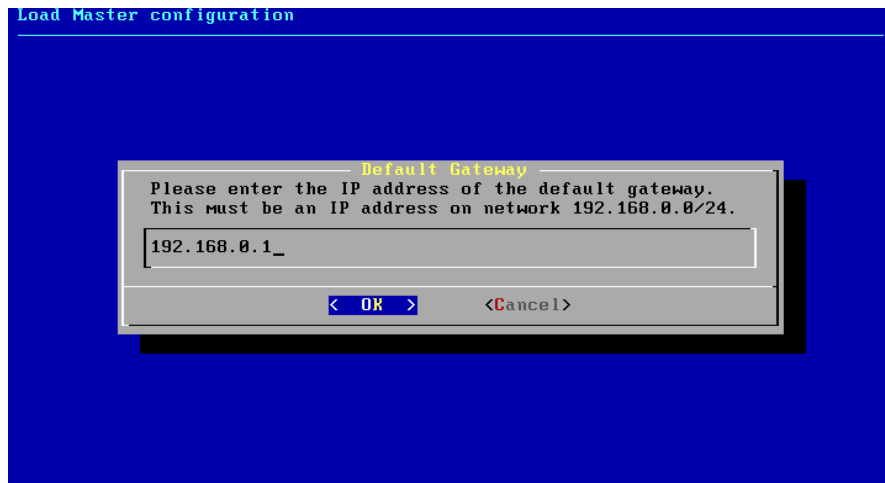


Figure 12: Default Gateway Configuration

When you've completed these steps, you'll presented with the main menu, shown in Figure 1 earlier.

Should you ever need to go through the Quick Setup Menu again for any reason, select option 1: Quick Setup, and the system will take you through the steps you just completed again.



HA Configuration: HA-2 Setup

If you're only using a standalone setup, then you can skip this section and move onto the “Final Step” section. If you do have an HA configuration, make sure that when you power up the HA-2 unit that there is network connectivity on the Network side interface (eth0) between both systems. This is critical for syncing the configuration between the two systems.

Once the HA-1 licensed system is configured, power up the HA-2 unit and log in as you did for the HA-1 system. As with the HA-1 unit, you may be prompted for the license (a printout of the license will be included with the HA-2 system) and then dropped into the Quick Setup directly, or you'll need to select it from the menu. Either way, in the first step you'll be asked for the Network side IP address (Figure 13):

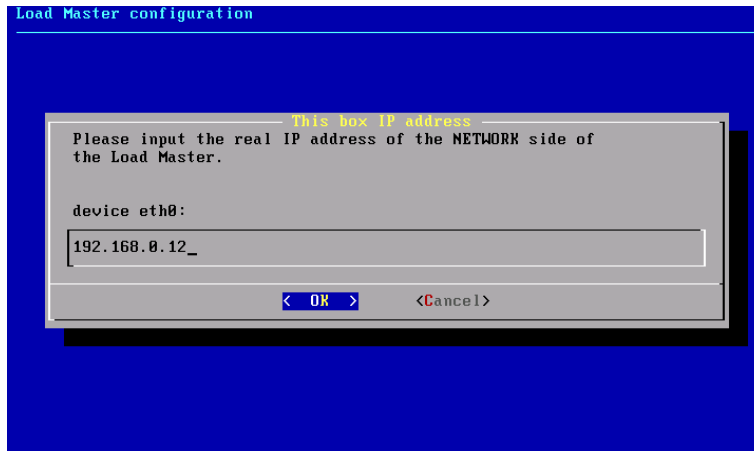


Figure 13: HA-2 Network Configuration

Enter the real IP address of the HA-2 unit. This IP address should be separate from the HA-1 unit. You'll then be asked for the netmask and VLAN as you were for HA-1.

You'll then be asked for the *partner* IP address, the real IP address of HA-1 on the Network (eth0) interface (Figure 14). Note: This is not the shared IP address, but the real IP of the HA-1 system.



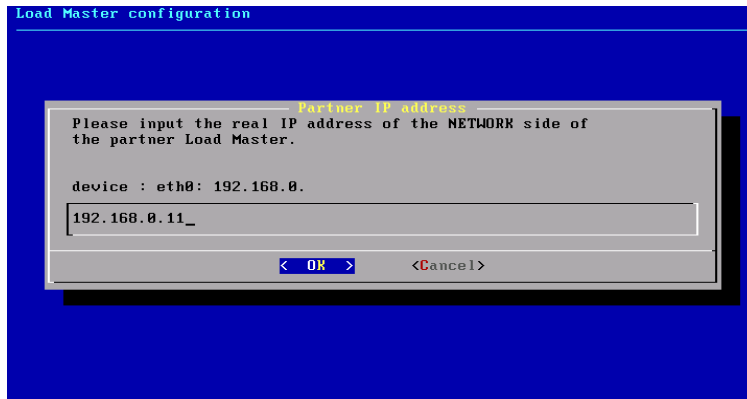


Figure 14: HA-2 Partner IP address

The HA-2 unit will now retrieve the configuration from the HA-1 unit, and if all goes well, you'll see the confirmation message in Figure 15.

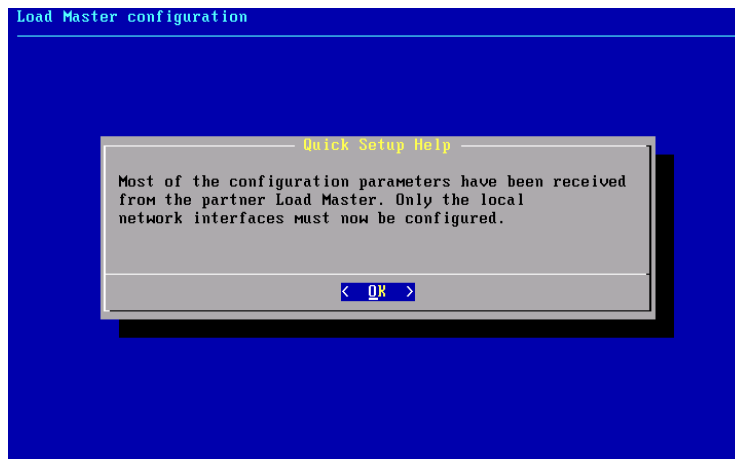


Figure 15: Configuration Retrieval

The next prompt will be for the Farm side network configuration. If you're doing a second network (two-armed), then enter the IP information as you did for the Network-side interface. Otherwise, leave the field blank when asking for the farm side IP.

The system will then ask you if you wish to activate the changes. Select yes, and the Quick Setup is complete.

Final Step

The final step in the initial setup is to change the default password of "1fourall" so that the system can be accessed and configured remotely.



YOU MUST CHANGE THE DEFAULT PASSWORD BEFORE YOU CAN ACCESS THE LOADMASTER REMOTELY. IN HA CONFIGURATIONS, PASSWORDS MUST BE CHANGED ON BOTH SYSTEMS

To change the default password, select “3: Local Administration”, then “Set Password”.

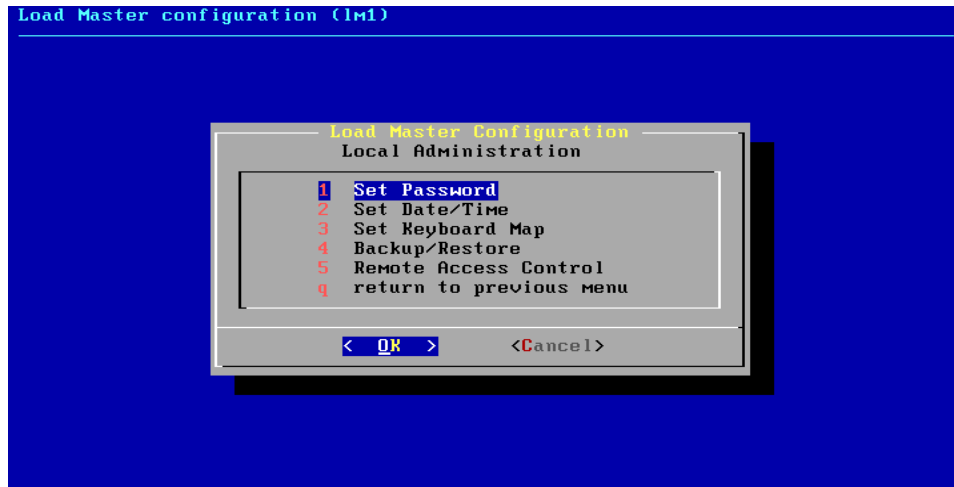


Figure 16: Set Password

You'll then be prompted to change the password. The requirement to change the default password is a security feature of the LoadMaster. The password must be changed on both the HA-1 and HA-2 units in the case of an HA configuration.

Web User Interface (WUI)

Configuration of the Virtual Services is typically done through the WUI (Web User Interface). The WUI interface utilizes HTTPS (Secure HTTP), so all passwords and information exchanged is encrypted over the network.

Connecting for the First Time

To access the WUI, put the IP address of your LoadMaster (either the Network or Farm interface IP address, whichever you have access to from your subnet) into the browser as an HTTPS URL. For example, if the IP address you have configured is 192.168.0.10, then the URL would be <https://192.168.0.10>.

When the URL comes up, you'll get some variation of security warning (Figure 17), depending on your browser (this warning is from Internet Explorer 6.0):





Figure 17: HTTPS Security Alert in IE

There is no cause for concern. What this alert means is that the LoadMaster is signing its own SSL certificate, instead of relying on a certificate issued by a trusted certificate authority (CA), such as Verisign or Thawte. Since this is an internal network device that you've setup, this is not an issue. This is only for your administration purposes, and no one accessing the load balanced sites on the LoadMaster will see that alert. You may see this alert every time you log in, depending on your browser.

(Note: If you use the SSL offloading/acceleration functionality of the LoadMaster or load balance SSL servers behind the LoadMaster for a public website, you'll be able to install certificates from a CA for those sites onto the LoadMaster.)

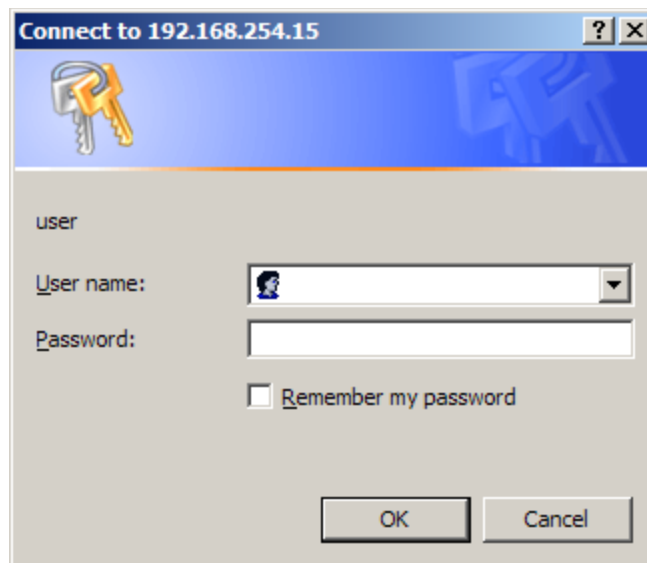


Figure 18: Authentication Request for LoadMaster Administration



Once you click “Yes”, you’ll be presented with authentication screen (Figure 18). For the username, use “bal”, and use the password that you’ve changed from “1fourall”.

REMEMBER: IF YOU DID NOT CHANGE THE DEFAULT PASSWORD, YOU WILL NOT BE ABLE TO LOG IN REMOTELY

Configuring a Virtual Service

Now that you’re in the WUI, you can create a Virtual Service. From the main menu (shown below) select the “Virtual Services” tab from the top (Figure 19).

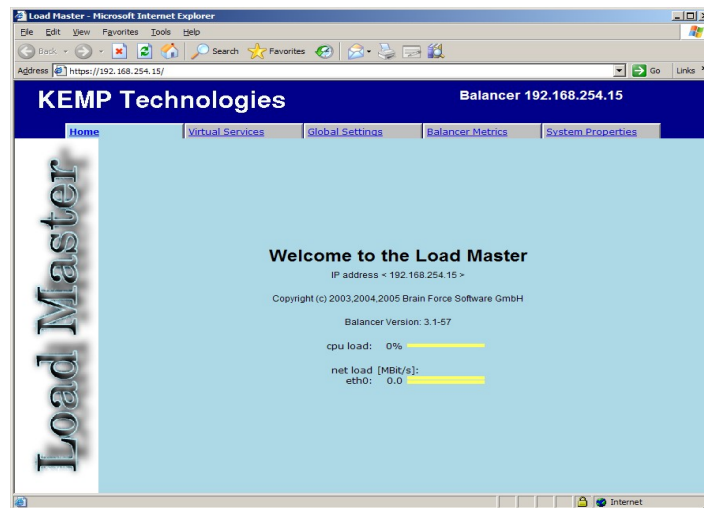


Figure 19: LoadMaster WUI Main Menu

You’ll see a button for “add virtual service”. Click there, and you’ll be presented with several configuration fields (Figure 20): IP address, port, and protocol (TCP or UDP). The IP address will be how users will access your load balanced servers, and it should be on a subnet that is accessible to the Internet (or Intranet) either directly or by NAT from a firewall. If this is to be a standard web server, the port should be 80, and the protocol should be TCP.

Virtual Address	<input type="text" value="192.168.254.200"/>
Port	<input type="text" value="80"/>
Protocol	<input type="text" value="tcp"/>
<input type="button" value="Add this Virtual Service"/> <input type="button" value="Cancel"/>	

Figure 20: Adding a Virtual Service



In this example, I've used the IP address of 192.168.254.200, port 80, protocol as TCP. Now that you've configured the Virtual Service, you'll need to add some real servers for the Virtual Service to forward traffic to.

Under “Real Servers for this Virtual Service” (Figure 21), click on “Add New...” to add a real server.

Properties for Virtual Service tcp/192.168.254.200:80

Activate or Deactivate Service	<input checked="" type="checkbox"/>
Real Server Check Protocol	HTTP
Service nickname (optional)	
Content Switching and Persistence Options	Persistence Mode: NONE
Content switching:	disabled
Port Following	Disabled
Scheduling Method	round robin
SSL Acceleration	Enabled: <input type="checkbox"/>

Real Servers for this Virtual Service

Add New ...

Operation	IP Address	Port	Forwarding method	Weight	Status
-----------	------------	------	-------------------	--------	--------

Figure 21: Properties for new Virtual Service

**Add a new Real Server to Virtual Service
192.168.254.200:80:tcp**

Please Specify the Parameters for the Real Server

Real Server Address	192.168.254.100
Port	80
Forwarding method	nat
Weight	1000

Add This Real Server Cancel

Figure 22: Adding a Real Server to new Virtual Service

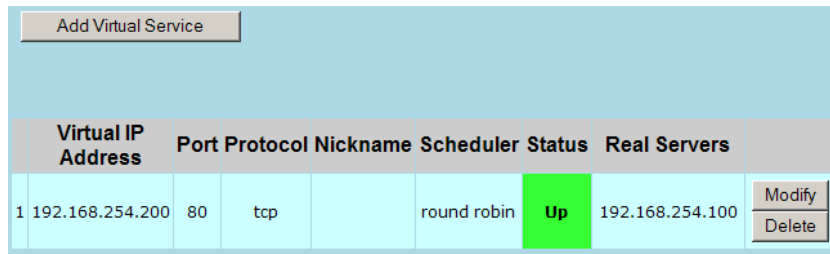
In the example above (Figure 22), I've added the real server IP address of 192.168.254.100, which is on the same subnet as my Virtual Service 192.168.254.200,



meaning this is a “one-armed” configuration. (*Again, make sure the default gateway for your web server is that of the LoadMaster.*)

Although only one real server is required for the Virtual Service to respond, more would be required of course for scaling and redundancy. You can add more at this point, or you can go back later and add/remove real servers as required.

Click on the Virtual Services tab up at the top, and you'll see a list of all your configured virtual servers. If any of the web servers are responding, you should see a green “Up” under the status (Figure 23).



Virtual IP Address	Port	Protocol	Nickname	Scheduler	Status	Real Servers	
1 192.168.254.200	80	tcp		round robin	Up	192.168.254.100	Modify Delete

Figure 23: Virtual Services Listed

At this point, you should be able to bring the Virtual Service up in your browser. In my case, I've configured the real server as a FreeBSD system with a fresh install of Apache, and I can see the default page below (Figure 24).

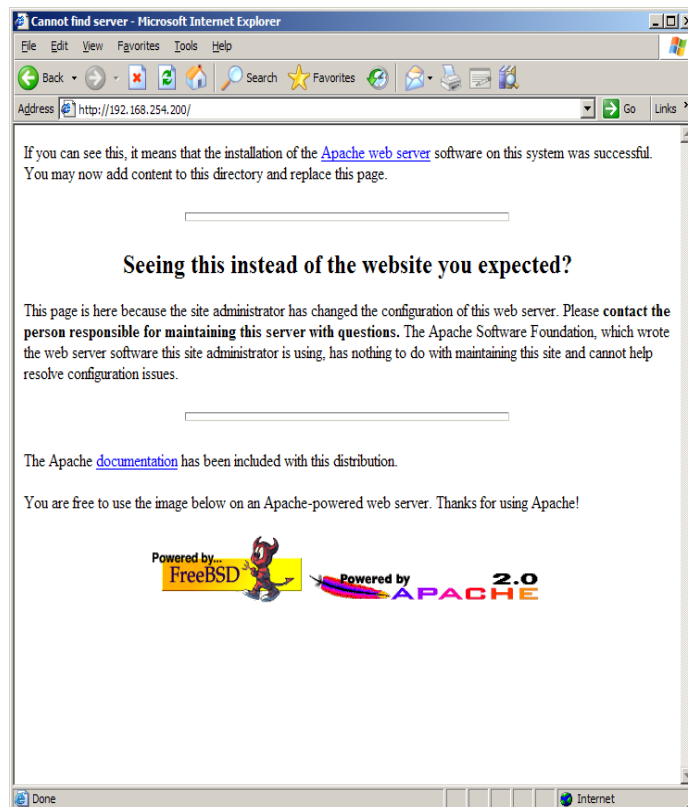


Figure 24: Successful Virtual Service



Note: If you don't get a page, and the virtual servers shows “up”, make sure the default route is pointed towards the LoadMaster. An incorrect default route setting is one of the most common reasons why a page will not load on the LoadMaster. Also, if you are on the same subnet as the real server, you will not be able to view a page.

SSH Access

While the virtual servers, real servers, and load balancing configuration is mainly done through the WUI, certain parameters must be configured through the same console interface that you used to setup the LoadMaster initially. You do not need to be on the LoadMaster with a keyboard and monitor or serial cable, however (although that is always an option). You can access the LoadMaster through SSH, an encrypted protocol similar to telnet.

To access the LoadMaster through SSH, you'll need an SSH client. For Windows, a popular and freeware SSH client is the venerable PuTTY application, which can be found here: <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>. There are also commercial SSH clients for Windows, including Secure CRT (<http://www.vandyke.com/products/securecrt/index.html>).

To use PuTTY to connect the LoadMaster, start PuTTY up and give the IP address of the LoadMaster in the Hostname field. In the example below (Figure 25), the LoadMaster's IP address is 192.168.0.1. The port to connect is TCP port 22 (which is the default for SSH). Then click “Open”.

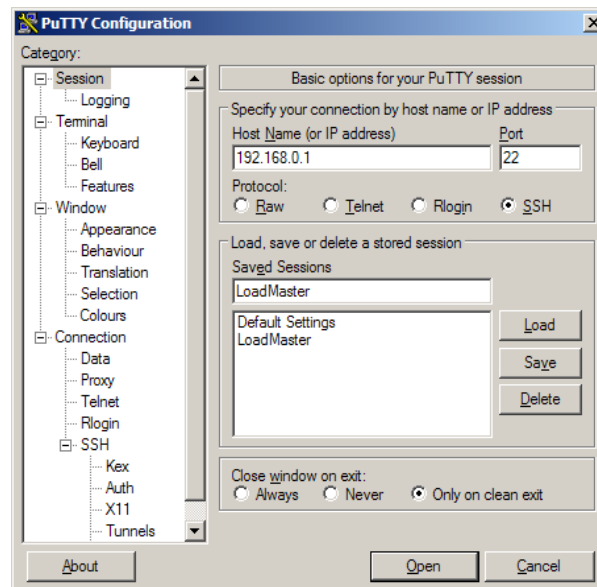


Figure 25: PuTTY Windows SSH Client Screen

The first time you connect to the LoadMaster (or any other SSH-enabled device), you'll



get a security alert similar to Figure 26.

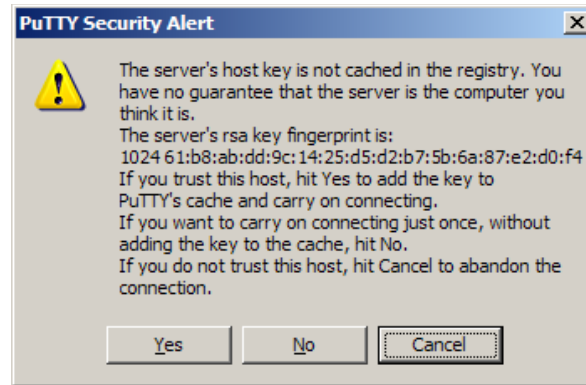


Figure 26: PuTTY Host Key Accept

Select “Yes”, so PuTTY downloads the server's key. Once you do this, you shouldn't be prompted again the next time you log in from this SSH client. (If you use another workstation or SSH client to connect, the first time you connect from there you'll also see that alert).

In the PuTTY window, you'll be asked prompted for “login:”, which you'll give as 'bal', and the password is of course the password you configured. Remember, you will not be able to use the '1fourall' password, you'll need to change it from the VGA/serial console before you can login remotely.

AGAIN: IF YOU DID NOT CHANGE THE DEFAULT PASSWORD, YOU WILL NOT BE ABLE TO LOG IN REMOTELY

Once you're logged in, you should then recognize the menu you're given as the one from the VGA/serial console (Figure 27).

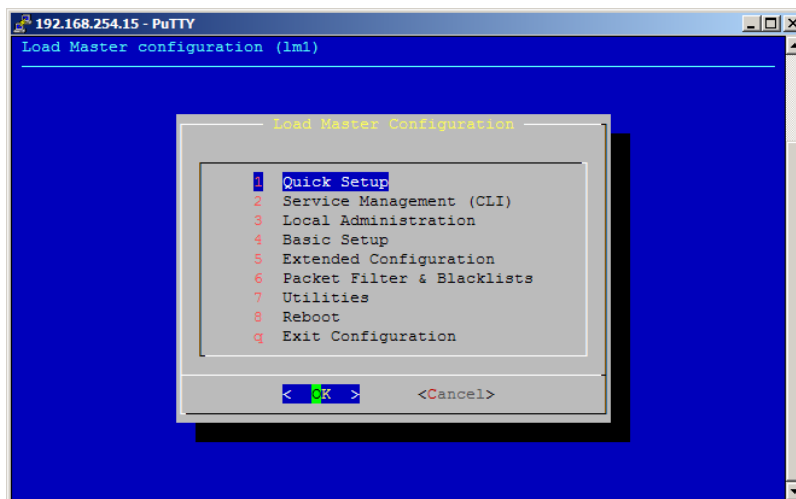


Figure 27: LoadMaster Configuration Main Menu



Most Linux and Unix systems include an SSH client (type `ssh` from the command line).

SSL Acceleration/Offloading

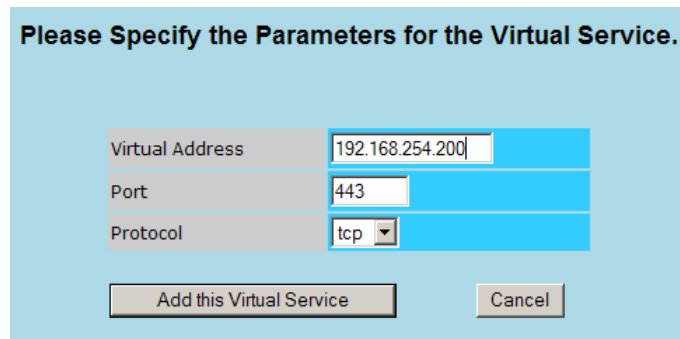
The LoadMaster series of server load balancers also offers the ability to do SSL termination, also known as SSL acceleration (or SSL offloading). This is a process whereby the LoadMaster's configured Virtual Service accepts incoming HTTPS connections and sends regular unencrypted HTTP to the real servers.

There are many advantages to this, with two of the main advantages being that the LoadMaster saves the real server from the SSL processing, as well as the LoadMaster being able to make load balancing and persistence decisions based on the HTTP headers (such as cookies), which it couldn't do if the HTTP header information were encrypted.

SSL Acceleration/Offloading relieves the Real Servers of all CPU-intensive SSL processing. It also enables the LoadMaster to make load balancing and persistence decisions based on unencrypted HTTP header content.

Configuring SSL Virtual Service with Acceleration

Configuration of SSL Acceleration is quite simple. First, setup a new Virtual Service (Figure 28) with the a TCP port of 443 (443 is the default for HTTPS) the same way you setup the first Virtual Service in an earlier section (it can be on the same IP address as a previously configured Virtual Service).



Please Specify the Parameters for the Virtual Service.

Virtual Address	192.168.254.200
Port	443
Protocol	tcp

Add this Virtual Service Cancel

Figure 28: Adding HTTPS Virtual Service

The next screen you will see is the Virtual Service properties page for the Virtual Service you just created (Figure 29).



Properties for Virtual Service tcp/192.168.254.200:443					
Activate or Deactivate Service	<input checked="" type="checkbox"/>				
Real Server Check Protocol	HTTPS				
Service nickname (optional)					
Content Switching and Persistence Options	Persistence Mode: NONE Content switching: disabled				
Port Following	Disabled				
Scheduling Method	round robin				
SSL Acceleration	Enabled: <input type="checkbox"/>				
Real Servers for this Virtual Service					
Add New ...					
Operation	IP Address	Port	Forwarding method	Weight	Status

Figure 29: Properties for SSL Virtual Service

You'll see a checkbox option for SSL Acceleration (Figure 30).

SSL Acceleration	Enabled: <input type="checkbox"/>
------------------	-----------------------------------

Figure 27: SSL Acceleration/Offloading Checkbox

To enable SSL Acceleration/offloading, select that box. The first thing you'll see is an prompt (Figure 31) telling you that there is no SSL certificate for the Virtual Service. This is normal.

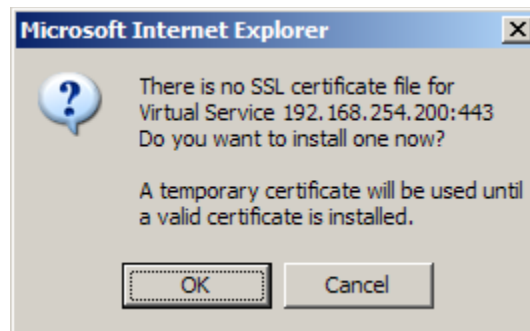


Figure 31: Temporary Certificate Notification

For now, click on “Cancel”, and you'll be setup with a self-signed certificate (you can always go back and add a Certificate Authority-signed certificate later). From there, you can add a real server just as you did with a Virtual Service. You can even add the same real servers that may be setup for other Virtual Services.



Self-Signed Certificate

When dealing with a public SSL-enabled site, you'll likely want to go with an SSL certificate signed by a Certificate Authority. If you've already got an SSL certificate on your web servers, you can use those certificates on the LoadMaster. If not, you'll want to contact a CA and obtain one (which takes some time). In the meantime, you can use a self-signed certificate to test the SSL functionality.

If you've setup an SSL accelerated/offloaded Virtual Service, put the IP address (or hostname is you've setup DNS) into your browser for an HTTPS connection. In my case, I've setup a Virtual Service on 192.168.254.200, so the URL I give my browser is <https://192.168.254.200/>.

When accessing a site with a self-signed certificate, you'll first be presented with a Security Alert on most browsers (Figure 32).



Figure 32: Self-signed Certificate Alert

Selecting yes tells your browser to trust the certificate, even though it's not issued by a trusted certificate authority (such as Verisign or Thawt). The traffic will still be encrypted.



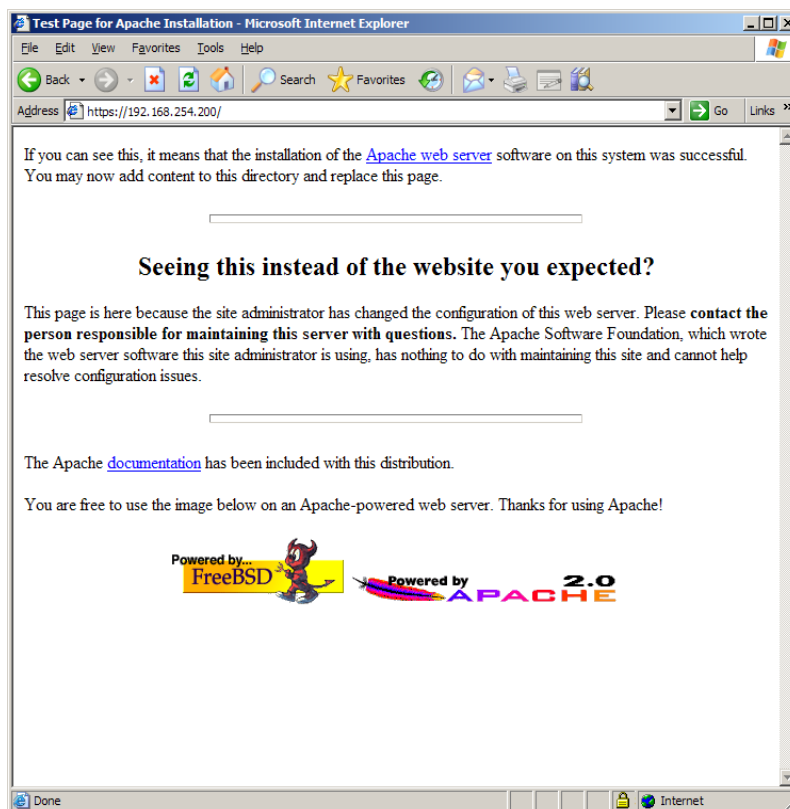


Figure 33: Successfully Served HTTPS/SSL Web Page

Again, if the site doesn't come up right away, make sure the default route for your real servers is set to the IP address of the LoadMaster.

In my example (Figure 33), traffic hitting my Virtual Service on 192.168.254.200 (port 443) comes in as HTTPS encrypted traffic, and is sent to be served by the real server as unencrypted HTTP traffic.

