



LOADMASTER

INSTALLATION AND CONFIGURATION GUIDE

DOCUMENT VERSION 1.0

RELEASE 6.0-28a

Revised: March 2012

World Headquarters:

KEMP Technologies, Inc.
12 Old Dock Road
Yaphank , NY 11980
U.S.A.

+1 (631) 345 5292

EMEA Headquarters:

KEMP Technologies Ltd.
Mary Rosse Centre
Holland Road, National Tech. Park
Limerick, Ireland

+353 (61) 260 101

Copyright Notices

Copyright © 2002-2012 KEMP Technologies, Inc.. All rights reserved.. KEMP Technologies and the KEMP Technologies logo are registered trademarks of KEMP Technologies, Inc..

KEMP Technologies, Inc. reserves all ownership rights for the LoadMaster product line including software and documentation. The use of the LoadMaster Exchange appliance is subject to the license agreement. Information in this guide may be modified at any time without prior notice.

Microsoft Windows is a registered trademarks of Microsoft Corporation in the United States and other countries. All other trademarks and service marks are the property of their respective owners.

Limitations: This document and all of its contents are provided as-is. KEMP Technologies has made efforts to ensure that the information presented herein are correct, but makes no warranty, express or implied, about the accuracy of this information. If any material errors or inaccuracies should occur in this document, KEMP Technologies will, if feasible, furnish appropriate correctional notices which Users will accept as the sole and exclusive remedy at law or in equity. Users of the information in this document acknowledge that KEMP Technologies cannot be held liable for any loss, injury or damage of any kind, present or prospective, including without limitation any direct, special, incidental or consequential damages (including without limitation lost profits and loss of damage to goodwill) whether suffered by recipient or third party or from any action or inaction whether or not negligent, in the compiling or in delivering or communicating or publishing this document.

Any Internet Protocol (IP) addresses, phone numbers or other data that may resemble actual contact information used in this document are not intended to be actual addresses, phone numbers or contact information. Any examples, command display output, network topology diagrams, and other figures included in this document are shown for illustrative purposes only. Any use of actual addressing or contact information in illustrative content is unintentional and coincidental.

Portions of this software are; copyright (c) 2004-2006 Frank Denis. All rights reserved; copyright (c) 2002 Michael Shalayeff. All rights reserved; copyright (c) 2003 Ryan McBride. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE ABOVE COPYRIGHT HOLDERS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the above copyright holders..

Portions of the LoadMaster software are copyright (C) 1989, 1991 Free Software Foundation, Inc. -51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA- and KEMP Technologies Inc. is in full compliance of the GNU license requirements, Version 2, June 1991. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Links to the source files are located on the [Product Matrix](#) page and the [Support](#) page of the KEMP website.

Portions of this software are Copyright (C) 1988, Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Portions of this software are Copyright (C) 1998, Massachusetts Institute of Technology

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Portions of this software are Copyright (C) 1995-2004, Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Portions of this software are Copyright (C) 2003, Internet Systems Consortium

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

TABLE OF CONTENTS

LOADMASTER APPLICATION	9
PREFACE.....	9
THE LOADMASTER DOCUMENTATION	9
TYPOGRAPHICAL CONVENTIONS	9
APPLICABLE PRODUCTS	9
1. INTRODUCTION TO KEMP TECHNOLOGIES AND THE LOADMASTER PRODUCTS	10
1.1 KEMP TECHNOLOGIES.....	10
1.2 THE LOADMASTER PRODUCTS.....	10
1.3 LOADMASTER LOAD BALANCER FEATURES.....	11
2 LOADMASTER NETWORK TOPOLOGIES	12
2.1 ONE-ARMED BALANCER.....	12
2.2 TWO-ARMED BALANCER	13
2.3 HIGH AVAILABILITY (HA) CONFIGURATION.....	14
2.4 DIRECT SERVER RETURN – DSR CONFIGURATION EXAMPLE	17
3 SCHEDULING METHODS	18
3.1 ROUND ROBIN.....	18
3.2 WEIGHTED ROUND ROBIN	18
3.3 LEAST CONNECTION.....	18
3.4 WEIGHTED LEAST CONNECTION	18
3.5 AGENT BASED ADAPTIVE BALANCING.....	19
3.6 FIXED WEIGHTED	20
3.7 SOURCE IP HASH	20
4 PERSISTENCE	21
4.1 INTRODUCTION TO PERSISTENCE	21
4.2 HOW DO I KNOW IF I NEED PERSISTENCE?	22
4.3 TIMEOUT.....	22
4.4 LAYER 7 PERSISTENCE METHODS.....	23
4.4.1 <i>Server Cookie Persistence</i>	23
4.4.2 <i>Active Cookie Persistence</i>	23
4.4.3 <i>Server Cookie or Source IP Persistence</i>	23
4.4.4 <i>Active Cookie or Source IP Persistence</i>	23
4.4.5 <i>Hash All Cookies Persistence</i>	23
4.4.6 <i>Hash All Cookies or Source IP Persistence</i>	24
4.4.7 <i>Source IP Address Persistence</i>	24
4.4.8 <i>Super HTTP</i>	24
4.4.9 <i>URL Hash</i>	24
4.4.10 <i>HTTP Host Header</i>	24
4.4.11 <i>Hash of HTTP Query Item</i>	24
4.4.12 <i>Selected Header</i>	25
4.5 PERSISTENCE AND HTTPS/SSL.....	25
4.6 PORT FOLLOWING	25
5 APPLICATION FRONT END.....	26
5.1 INTRUSION PREVENTION SYSTEM	26
5.1.1 <i>Intrusion Handling</i>	27
5.1.2 <i>Detection level</i>	27
5.1.3 <i>Warnings</i>	27
5.1.4 <i>Intrusion Alerts</i>	27
5.1.5 <i>SNORT Configuration</i>	27

5.2	CACHING	28
5.2.1	<i>Flushing Cache</i>	28
5.2.2	<i>Maximum Cache Size</i>	28
5.3	DATA COMPRESSION	29
6	SSL ACCELERATION/OFFLOADING	30
6.1	SELF-SIGNED VERSUS CA SIGNED CERTIFICATES	30
6.2	CERTIFICATE BASICS.....	31
6.3	OPERATIONAL DIFFERENCES	31
7	RULE BASED CONTENT SWITCHING	32
7.1	TERMINOLOGY.....	32
7.2	LIMITATIONS TO CONTENT SWITCHING	33
7.3	USING CONTENT SWITCHING.....	33
8	HEALTH CHECKING	34
8.1	OVERVIEW	34
8.2	SERVICE AND NON-SERVICE BASED HEALTH CHECKING.....	35
9	SNMP SUPPORT.....	38
10	LOADMASTER SOFTWARE UPGRADES	39
10.1	ONLINE UPGRADES.....	39
11	USER MANAGEMENT.....	40
11.1	ROLES/PERMISSION.....	40
11.1.1	<i>Real Servers</i>	40
11.1.2	<i>Virtual Services</i>	40
11.1.3	<i>Rules</i>	40
11.1.4	<i>Certificate Creation</i>	40
11.1.5	<i>3rd Party Certificates</i>	40
11.1.6	<i>Certificate Backup</i>	40
11.1.7	<i>Allowed Network</i>	40
11.1.8	<i>All Permissions</i>	40
11.1.9	<i>GEO</i>	40
12	BONDING AND VLAN	41
12.1	OVERVIEW	41
12.2	PRE-REQUISITE (SWITCH COMPATIBILITY)	41
12.2.1	<i>Switch configuration</i>	41
12.3	BONDING/TEAMING (802.3AD/ACTIVE-BACKUP)	41
12.4	VLAN TAGGING	42
13	MISCELLANEOUS	43
13.1	IPV6 SUPPORT	43
13.2	REMOTE SYSLOG SUPPORT.....	43
13.3	HOW TO GET A LICENSE	43
13.3.1	<i>Get a 30 day evaluation license</i>	43
13.3.2	<i>Get a full LoadMaster license</i>	44
13.3.3	<i>Get full High Availability LoadMaster cluster licenses</i>	44
13.3.4	<i>Upgrading the evaluation license to a full single or HA license</i>	44
13.4	BACKUP AND RESTORE	44
13.5	INTEROPERABILITY BETWEEN L4 / L7 VIRTUAL SERVICES	45
13.6	LOG INFORMATION.....	45
13.7	DEBUGGING UTILITIES.....	45
13.7.1	<i>Disable All Transparency</i>	45

13.7.2	<i>Enable L7 Debug Traces</i>	45
13.7.3	<i>Perform a PS</i>	45
13.7.4	<i>Perform a l7adm</i>	45
13.7.5	<i>Ping Host</i>	45
14	VARIOUS NETWORKING ISSUES	46
14.1	S-NAT.....	46
14.2	DEFAULT GATEWAY AND ROUTES.....	46
14.3	NON-LOCAL REAL SERVER SUPPORT	48
15	GETTING STARTED	49
15.1	THE LOADMASTER HARDWARE APPLIANCE	49
15.2	CONNECTING THE LOADMASTER HARDWARE	49
15.2.1	<i>Connection of eth0</i>	49
15.2.2	<i>Connection of eth1 and eth2</i>	49
15.3	SETTING UP THE SOFTWARE	50
15.3.1	<i>Console</i>	50
15.3.2	<i>Browser</i>	50
15.4	LOGIN AND LICENSE KEY	51
15.5	HA SETUP	51
16	FAST TRACK	52
16.1	HOW TO LOGIN	52
16.2	CREATE A SIMPLE VIRTUAL SERVICE	52
16.3	VIRTUAL SERVICE TEMPLATES	54
16.4	CREATE A VIRTUAL SERVICE WITH CONTENT RULES	54
16.4.1	<i>Setting up Content Rules</i>	54
16.4.2	<i>Configuring Virtual Services for Content Switching</i>	56
16.5	CREATE AN SSL ACCELERATED VIRTUAL SERVICE.....	57
16.5.1	<i>Adding an SSL Virtual Service</i>	57
16.5.2	<i>Adding an SSL Certificate</i>	58
16.5.3	<i>Checking Certificate Installations</i>	60
16.5.4	<i>Intermediate Certificates</i>	61
16.5.5	<i>Installing Intermediate Certificates</i>	61
16.5.6	<i>IIS Certificates</i>	62
16.5.7	<i>Re-encrypt SSL</i>	62
16.5.8	<i>Certificate Signing Request</i>	62
16.5.9	<i>Backup/Restore Certificates</i>	62
16.5.10	<i>SSL Ciphers</i>	63
16.5.11	<i>Web User Interface Root Certificate Installation</i>	63
16.6	LOAD BALANCING MICROSOFT TERMINAL SERVICES.....	63
16.7	CONFIGURING PORT FOLLOWING	65
16.7.1	<i>Create the Virtual Service for HTTP</i>	65
16.7.2	<i>Create the Virtual Service for HTTPS/SSL Offloading</i>	66
16.7.3	<i>Configure Port Following for HTTPS VS</i>	66
16.7.4	<i>Configure Port Following for HTTP VS</i>	67
17	FULL WEB USER INTERFACE (WUI) MENU TREE	68
17.1	HOME.....	69
17.2	VIRTUAL SERVICES.....	70
17.2.1	<i>Add New VS</i>	70
17.2.2	<i>View/Modify Existing VS (HTTP Service)</i>	70
17.3	BASIC PROPERTIES SCREEN.....	71
17.3.1	<i>Service Name</i>	71
17.3.2	<i>Alternate Address</i>	71

17.3.3	<i>Service Type</i>	71
17.3.4	<i>Activate or Deactivate Service</i>	71
17.4	STANDARD OPTIONS SCREEN.....	72
17.4.1	<i>Extra Ports</i>	72
17.4.2	<i>Force L7</i>	72
17.4.3	<i>L7 Transparency</i>	72
17.4.4	<i>Persistence Options</i>	72
17.4.5	<i>Scheduling Methods</i>	73
17.4.6	<i>SSL Properties Screen</i>	74
17.4.7	<i>Advanced Properties Screen</i>	75
17.4.8	<i>View/Modify Existing (Remote Terminal Service)</i>	77
17.4.9	<i>Real Servers</i>	78
17.4.10	<i>Add Real Server</i>	78
17.4.11	<i>Real Server Check Parameters</i>	78
17.5	STATISTICS.....	80
17.5.1	<i>Global Statistics</i>	80
17.5.2	<i>Real Server Metrics</i>	81
17.5.3	<i>Virtual Service Metrics</i>	81
17.6	ENABLE/DISABLE REAL SERVERS.....	82
17.7	RULES & CHECKING.....	83
17.7.1	<i>Content Rule Management</i>	83
17.7.2	<i>Header Modification</i>	84
17.7.3	<i>Adaptive Parameters</i>	84
17.7.4	<i>Service (Health) Check Parameters</i>	85
17.8	CERTIFICATES.....	86
17.8.1	<i>SSL Certificates</i>	86
17.8.2	<i>Intermediate Certificates</i>	86
17.8.3	<i>Certificate Signing Request</i>	87
17.8.4	<i>Backing Up and Restoring Certificates</i>	88
17.9	SYSTEM CONFIGURATION.....	90
17.9.1	<i>Interfaces</i>	90
17.9.2	<i>Local DNS Configuration</i>	93
17.9.3	<i>Route Management</i>	93
17.9.4	<i>Access Control</i>	93
17.9.5	<i>System Administration</i>	94
17.10	USER MANAGEMENT.....	94
17.11	UPDATE LICENSE.....	95
17.11.1	<i>System Reboot</i>	95
17.11.2	<i>Backup/Restore</i>	96
17.11.3	<i>Date/Time</i>	97
17.12	LOGGING OPTIONS.....	97
17.12.1	<i>Log Files</i>	97
17.12.2	<i>Debug Options</i>	98
17.12.3	<i>Syslog Options</i>	99
17.12.4	<i>SNMP Options</i>	99
17.12.5	<i>Email Options</i>	101
17.13	MISCELLANEOUS OPTIONS.....	103
17.13.1	<i>Remote Access</i>	103
17.14	L7 CONFIGURATION.....	104
17.14.1	<i>Network Options</i>	106
17.15	AFE CONFIGURATION.....	107
17.16	HA PARAMETERS.....	108
APPENDIX A. THE LOADMASTER SETUP QUESTIONNAIRE.....		111
SINGLE LOADMASTER BALANCER SOLUTION.....		111

HIGHLY AVAILABLE DUAL LOADMASTER BALANCER SOLUTION	112
APPENDIX B: LOADMASTER CONSOLE OPERATION.....	113
QUICK SETUP	113
CONSOLE MAIN MENU	114
CONFIGURATION MENU BASICS.....	114
SERVICE MANAGEMENT (CLI)	114
LOCAL ADMINISTRATION.....	115
BASIC SETUP	116
EXTENDED CONFIGURATION	118
PACKET FILTER & ACCESS CONTROL LISTS	121
UTILITIES	121
REBOOT	123
EXIT LOADMASTER CONFIG.....	123
TOP LEVEL COMMANDS	124
HEALTH CHECK COMMAND LEVEL.....	126
RULES COMMAND LEVEL.....	127
RULE EDIT COMMAND LEVEL	127
VIRTUAL SERVICE (VIP) COMMAND LEVEL.....	128
REAL SERVER COMMAND LEVEL.....	131
APPENDIX D. EXAMPLE OF A CONTENT RULE	133
APPENDIX E. ERROR CODES	134
GENERAL MESSAGES.....	134
L7: CONNECTION TIME OUT MESSAGES	134
HA MESSAGES	135
ENHANCED MESSAGES	135
APPENDIX F. CONFIGURING REAL SERVERS FOR THE DSR CONFIGURATION	137
CONFIGURING A VIP ON THE LOOPBACK INTERFACE ON LINUX.....	137
DSR CONFIGURATION ON WINDOWS	138
CONFIGURING A VIP ON THE LOOPBACK INTERFACE ON WINDOWS SERVER 2000	141
CONFIGURING A VIP ON THE LOOPBACK INTERFACE ON WINDOWS SERVER 2003	142
CONFIGURING A VIP ON THE LOOPBACK INTERFACE ON WINDOWS SERVER 2008 R2.....	142
TO REACH THE DEVICE MANAGER IN WINDOWS XP	143
TO REACH THE DEVICE MANAGER IN WINDOWS 7	143
APPENDIX G: HEADERS ADDED BY LOADMASTER WHEN 'CLIENT CERTIFICATES AND ADD HEADERS' OPTION IS SELECTED	148
APPENDIX H: API FOR AGENT BASED ADAPTIVE BALANCING	150
GLOSSARY	152
INDEX	154
DOCUMENT HISTORY.....	155

LoadMaster Application

Preface

Thank you for purchasing a KEMP Technologies LoadMaster! We know you will find this product meets all your Application Delivery needs. We wish you much success with your KEMP LoadMaster and remember, help is just a phone call away thanks to the first year maintenance included with your LoadMaster product.

The LoadMaster Documentation

The KEMP Technologies LoadMaster documentation library comprises:

- *LoadMaster Installation & Configuration Guide* – (this document) which describes the main features of the LoadMaster Load Balancer, the setup of the LoadMaster hardware (if applicable) and the Web User Interface (browser driven).
- *LoadMaster Quick Start Guide* – as the name suggests, it offers a quick way to have the LoadMaster up and running for those Users who are familiar with load balancing.
- *LoadMaster SSL Quick Start Guide* – a quick way to configure the LoadMaster for SSL support.
- *Load Balancing Microsoft Terminal Services Guide* – shows how to set up a Virtual Service to balance Microsoft Terminal Servers.
- *LoadMaster Deployment Guide for MS Exchange 2010* – detailed configuration for the LoadMaster Exchange product.

The above documents, and more, are located at: <http://www.kemptechnologies.com/us/loadmaster-documentation.html>.

Typographical Conventions

Screenshots and photographs may be design models and may not correspond exactly to currently shipping components, and, they may not include all available options.

Applicable Products

This software releases is applicable to the following LoadMaster products; 2000, 2200, 2500, 2600, 3500, 3600 and 5500 hardware appliances, plus the VLM-100, VLM-1000, VLM-Exchange and VLM-DR virtual products.

1. Introduction to KEMP Technologies and the LoadMaster Products

1.1 KEMP Technologies

KEMP Technologies leads the industry in driving the price/performance value proposition for application delivery and load balancing to levels that our customers can afford. Our products' versatile and powerful architecture provide the highest value, while enabling our customers to optimize their businesses that rely on Internet-based infrastructure to conduct business with their customers, employees and partners.

Most load balancing/SSL accelerator vendors have abandoned the entry-level market in favor of high-priced appliances and switches. This has left a large void in the load balancing and content switching market. First-time buyers are not able to find adequate, high-value products that met their needs, and that are priced within their financial means.

That has all changed with KEMP Technologies' introduction of the LoadMaster. The LoadMaster integrates powerful, stable, fully-featured load balancers with layer-7 content switching, SSL acceleration and security. KEMP Technologies has created an ideal family of products for customers looking for the best value proposition application delivery.

KEMP Technologies' market focus includes small-to-medium sized businesses, Fortune 1000 enterprises, remote enterprise branch offices and managed service providers, who view end-user satisfaction and IT web and application infrastructure reliability and optimization as mission-critical to their long-term success.

These companies are burdened with the risk of networked applications not meeting end-user expectations - a detriment to their brand equity, revenue, and market share.

KEMP Technologies delivers website integrity by providing end-user customers and subscribers with access to applications and content – with availability all the time. KEMP products enable network administrators to gain the control and predictability of their IT infrastructure to insure the highest levels of web and application integrity.

KEMP Technologies products optimize web and application infrastructure as defined by high-availability, high-performance, flexible scalability, security and ease of management. They maximize the total cost-of-ownership for web infrastructure, while enabling flexible and comprehensive deployment options.

1.2 The LoadMaster Products

KEMP Technologies' LoadMaster family of affordable, yet feature rich application delivery controllers and server load balancer appliances automatically and intelligently manage user traffic and applications, to deliver website integrity for small-to-medium sized businesses (SMB) and managed service providers.

KEMP products optimize web infrastructure as defined by high-availability, high-performance, flexible scalability, ease of management and secure operations - while streamlining IT costs. LoadMaster simplifies the management of networked resources, and optimizes and accelerates user access to diverse servers, content and transaction-based systems.

For SMB organizations, KEMP streamlines user access to websites to improve customer satisfaction. Managed service providers use KEMP's purpose-built products to enable fast time-to-market and cost-effective operations for new and existing managed services.

If your website or intranet is critical to you organization, an accessible, secure and continuously operating site is the key to your success. With a powerful ADC or load balancer from KEMP Technologies, you'll be providing your business with a high-value, reliable infrastructure appliance that will significantly improve your web server performance, reduce costs and increase your customer's web experience.

1.3 LoadMaster Load Balancer Features

The LoadMaster load balancer provides the following features with the Balancer Operating Software and the Web User Interface:

The LoadMaster load balancer provides the following features with the LoadMaster Operating Software and the Web User Interface:

- Balancing Methods
- Persistence
- Application Front End
- SSL Acceleration/Offloading
- Rule Based Content Switching
- Health Checking
- SNMP Support
- User Management
- IPv6 Support
- Bonding and VLAN

These features are described in more detail in the following chapters.

2 LoadMaster Network Topologies

2.1 One-Armed Balancer

If a one-armed configuration is selected then the following is true:

- Only the eth0 Ethernet interface will be used (for both in and outbound traffic)
- Real Servers and Virtual Services will be part of the same logical network – sometimes called flat-based - this implies that both have public IP addresses if used for services within the Internet.
- S-NAT does not make sense for one-armed configurations.
- Does not automatically imply the use of Direct Server Return (DSR) methods on the Real Servers
- IP Address transparency will function properly if clients are located on the same logical network as the LoadMaster in a DSR configuration. IP Address transparency is NOT supported when clients are located on the same logical network as the LoadMaster in a NAT configuration.

The one armed solution may be set-up in both a Single and HA configuration.

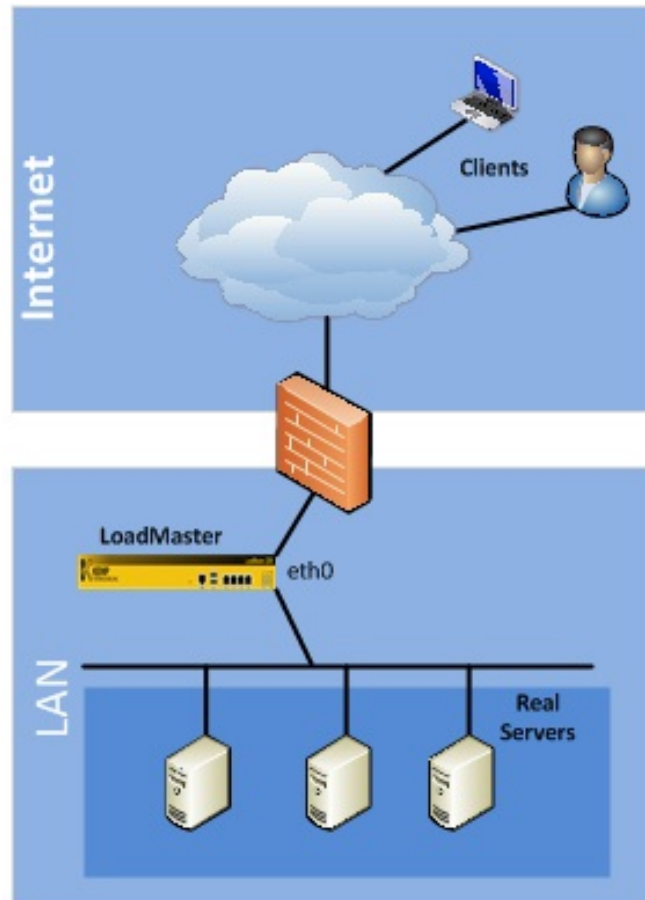


Figure 2-1 LoadMaster single, 1-arm configuration

2.2 Two-Armed Balancer

An example of a two-armed LoadMaster site may look as follows.

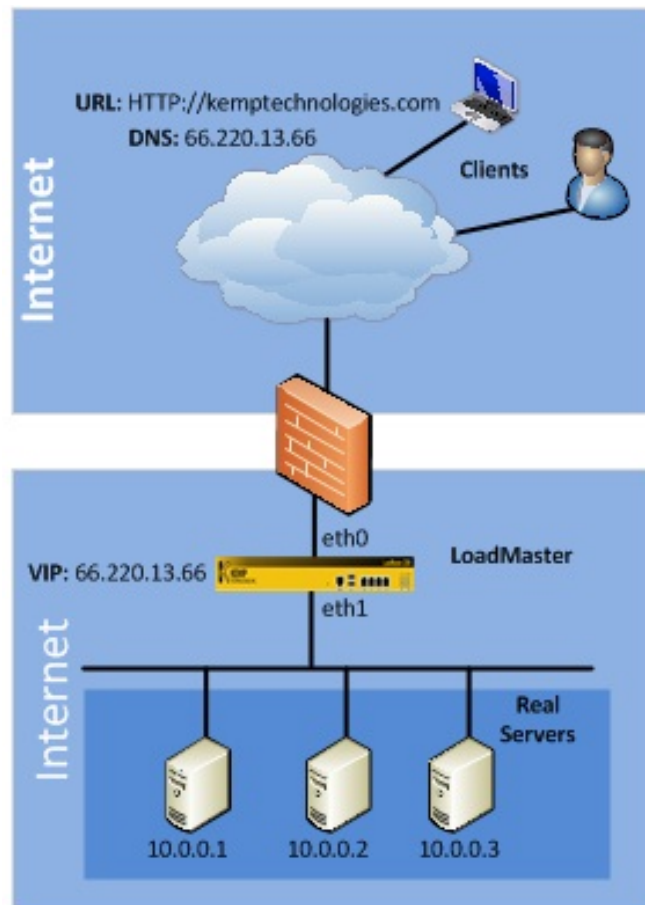


Figure 2-2: LoadMaster single, 2-arm configuration

The system has been configured as follows:

- A Virtual Service (VS) has been created on the LoadMaster with an IP address 66.220.13.66 for an HTTP service.
- The VS has been configured to balance the incoming traffic across the Real Servers (RS) (server 1, 2 and 3).
- A web User requests the URL “http://www.kemptechnologies.com”.
- The URL will be resolved by the DNS into IP address 66.220.13.66.
- The request will be routed to the LoadMaster, which offers this IP address as an IP-alias of its network interface eth0.
- The LoadMaster is connected to the server farm subnet 10.0.0.0 via its network interface eth1.
- The LoadMaster knows that in this subnet are three Real Servers are assigned to the requested address 66.220.13.66 and able to deliver the required content.

The LoadMaster uses the load balancing method you configured, e.g. weighted round robin, to send the request onto one of the three Real Servers.


Other items to note regarding the two-armed configuration are:


- Both eth0 (net side) and eth1 (farm side) interfaces are used. Additional ports go to the farm side for Multi-Armed configurations
- Implies that the LoadMaster (eth0) and server farm(s) are on separate logical networks, sometimes referred to as a NAT based topology.
- The server farm(s) may make use of non-routable (RFC1918) IP addresses
- S-NAT may be useful in such a configuration
- IP Address transparency will function properly if clients are located on the same logical network as the LoadMaster in both NAT (common) and DSR (uncommon) configurations.
- Virtual Services may be created on any of the Ethernet interfaces.
- Real Servers may exist on either the eth0 or up to the ethX network. However, placing Real Server on eth0 in a two-armed configuration is not recommended.

Leveraging one port and configuring the “Additional Subnet” feature qualifies as two-armed.

2.3 High Availability (HA) Configuration

The High Availability feature of the LoadMaster guarantees the availability of your server farm. HA is achieved by a hot-standby, failover mechanism. Two identical LoadMaster units are integrated into the network as a cluster. One machine serves as the active LoadMaster and the second one remains in a standby, idle state, always prepared to take over the activities from the active server. This cluster appears as a single logical unit to the Internet side and to the server farm side connections.

 With an HA cluster, each network interface has an individual IP address and one shared IP address – shared with the partner unit. The shared IP address is identical for both LoadMaster appliances, though it is associated with only the active LoadMaster at any given time.

 If the LoadMaster is to be used as the Default Gateway in the server interface, it must be set to the shared IP address since this would be available.

During normal operation each node periodically sends health check messages over the eth0 and eth2 connections to verify the availability of the peer appliance. In the event the active LoadMaster should fail, the standby appliance will become active and take over the task of balancing.

The topology for HA single arm looks like this:

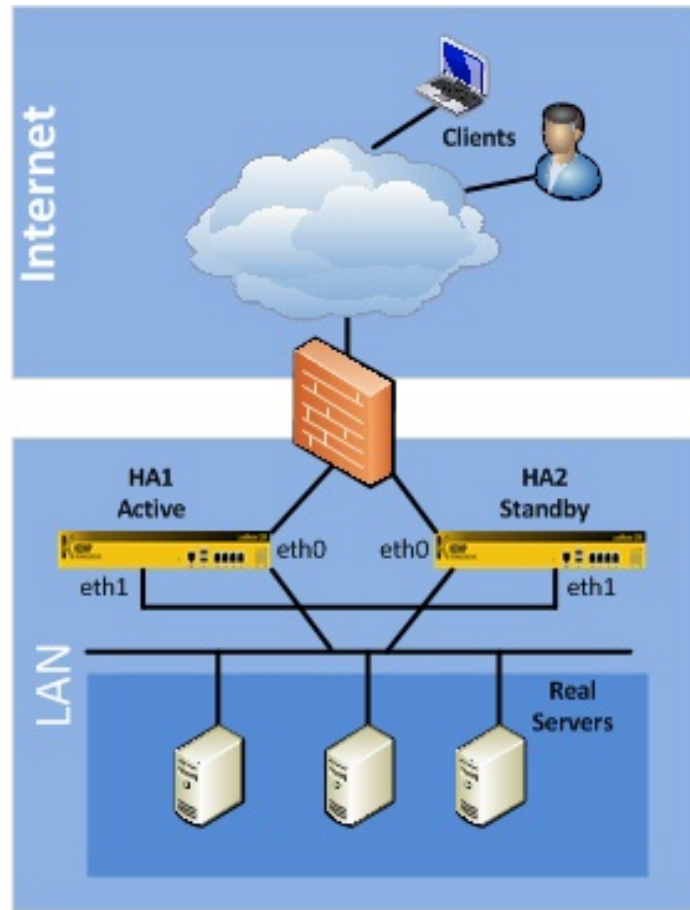


Figure 2-3 : LoadMaster HA, 1-arm configuration

LoadMasters, HA1 and HA2, use eth0 to connect to the network (firewall) and to the servers, and, have one shared IP address between the two ports. Whereas eth1 on each unit is directly connected via a patch cable - the port is auto-sensing so it makes no difference if the cable is straight or reversed- and is used exclusively for additional HA health checking.

The topology for HA dual arm looks like this:

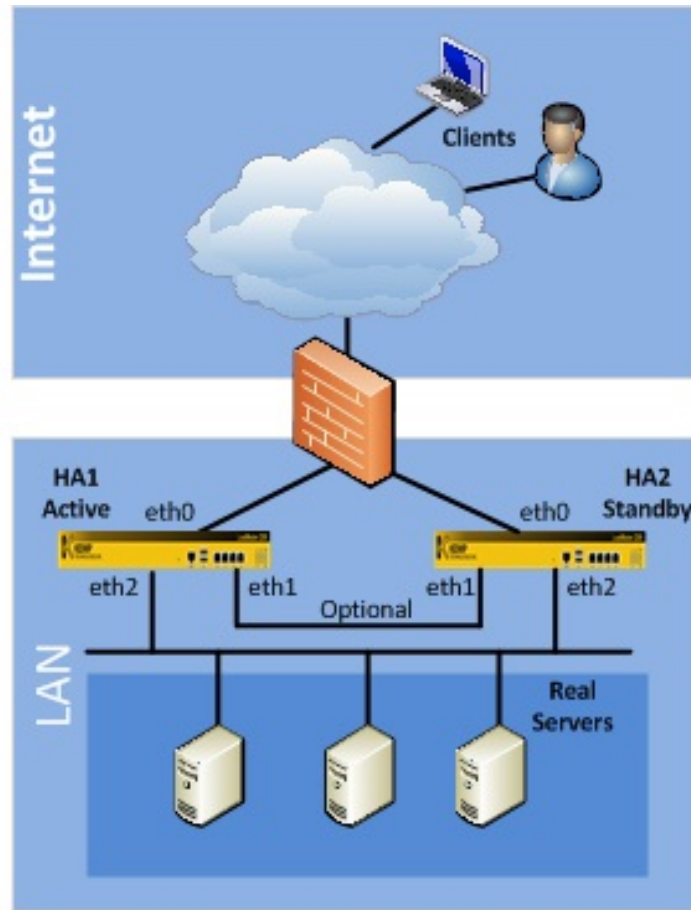


Figure 2-4 : LoadMaster HA, 2-arm configuration

Both HA1 and HA2 use eth0 to connect to the network (firewall) and eth2 for connection to the servers. The two eth0 ports have one shared IP address and the two eth2 ports have a different shared IP address. Health checking between the two LoadMasters occurs between both eth ports. Optionally, eth1 on each unit may be directly connected via a patch cable for added HA health checking though it is quite unnecessary since there is already 2 health check routes between the HA pair.

⚠ Both HA1 and HA2 must be on the same subnet with the same default gateway and be located within the same physical site. They must not be separated by an intra-site link and must use the same gateway to return traffic.

Running HA spanned across multiple subnets will not provide hardware redundancy in the event of a failure of the link between them. If traffic balancing between multiple sites is required, either the LoadMaster DR or the GEO LoadMaster, KEMP's DNS-based appliances that employ health checking to avoid site outages, would be the correct solution.

2.4 Direct Server Return – DSR Configuration Example

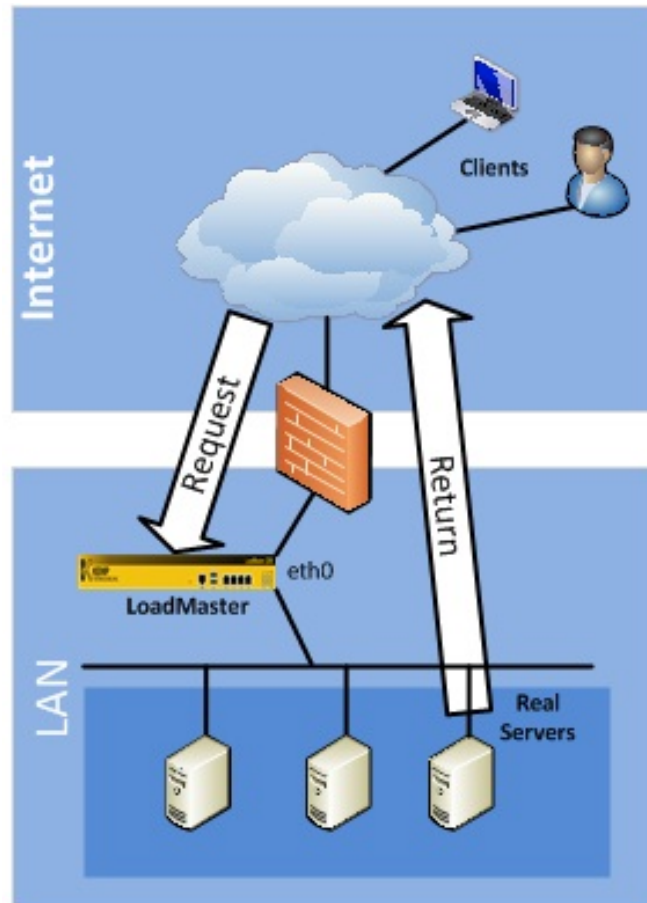


Figure 2-5 : LoadMaster DSR, single, 1-arm configuration

- 1 – Incoming request intercepted by LoadMaster
- 2 – Routed to Server 1
- 3 – Response from Server 1
- 4 – Response goes directly to Client without LoadMaster

This feature should be implemented only if the Real Servers need to respond to the clients directly, without going through the LoadMaster. In this configuration the Real Servers must have a path to the clients without going through the LoadMaster (e.g., an additional router in parallel with the LoadMaster).

⚠ The only persistence option supported in a DSR configuration is Source IP. NO Layer 7/Application features can be used with DSR. Also, DSR may be used only in a 1-ARM configuration due to routing issues caused on the RS with the loopback interface in a 2-ARM solution.

DSR uses a combination of MAT (MAC address translation) and a modified RS configuration. The RS is configured with an IP address as normal but it is also given the IP address of the VIP. Normally you cannot have two machines on a network with the same IP address. To get around this, the VIP address on a Real Servers must be configured so that the server does not respond to arp requests on the VIP address.

For further information on how to configure Real Servers (both Linux and Windows) please refer to **Appendix F. Configuring Real Servers for the DSR Configuration**

3 Scheduling Methods

There are several load balancing methods provided by the LoadMaster, which are known as "Scheduling Methods" or "algorithms":

3.1 Round Robin

With this method incoming requests are distributed sequentially across the server farm (cluster), i.e. the available servers.

If this method is selected, all the servers assigned to a Virtual Service should have the similar resource capacity and host identical applications. Choose round robin if all servers have the same or similar performance and are running the same load. Subject to this precondition, the round robin system is a simple and effective method of distribution.

However, if the servers have different capacities, the use of the round robin system can mean that a less powerful server receives the next inquiry even though it has not yet been able to process the current one. This could cause a weaker server to become overloaded.

3.2 Weighted Round Robin

This method balances out the weakness of the simple round robin: Incoming requests are distributed across the cluster in a sequential manner, while taking account of a static "weighting" that can be pre-assigned per server.

The administrator simply defines the capacities of the servers available by weighting the servers. The most efficient server A, for example, is given the weighting 100, whilst a much less powerful server B is weighted at 50. This means that Server A would always receive two consecutive requests before Server B receives its first one, and so on.

3.3 Least Connection

Both round robin methods do not take into account that the system does not recognize how many connections are maintained over a given time. It could therefore happen that Server B is overloaded, although it receives fewer connections than Server A, because the users of this server maintain their connections longer. This means that the connections, and thus the load for the server, accumulate.

This potential problem can be avoided with the "least connections" method: Requests are distributed on the basis of the connections that every server is currently maintaining. The server in the cluster with the least number of active connections automatically receives the next request. Basically, the same principle applies here as for the simple round robin: The servers related to a Virtual Service should ideally have the similar resource capacities.

3.4 Weighted Least Connection

If the servers have different resource capacities the "weighted least connection" method is more applicable: The number of active connections combined with the various weights defined by the administrator generally provides a very balanced utilization of the servers, as it employs the advantages of both worlds.

This is, in general, a very fair distribution method, as it uses the ratio of the number of connections and the weight of a server. The server in the cluster with the lowest ratio automatically receives the next request.

3.5 Agent Based Adaptive Balancing

In addition to the methods above the LoadMaster contains an adaptive logic, which checks the state of the servers at regular intervals and independently of the configured weighting.

For the extremely powerful “agent based adaptive balancing” method the LoadMaster periodically checks the system load on all the servers in the farm: Each server machine should provide a file that contains a numeric value in the range between 0 and 99 representing the actual load on this server (0 = idle, 99 = overload, 101=failed, 102=administratively disabled). The LoadMaster retrieves this file by an HTTP GET operation. It is the server’s job to provide the actual load in the ASCII file. There are no prerequisites, though, how the servers evaluate this information.

Two different strategies are applied, depending on the overall load of the server farm:

During normal operation the scheduling algorithm calculates a weighting ratio out of the collected load values and distributes the connections according to it. So if excessive overloading of a server occurs, the weighting is readjusted transparently by the system. As with the weighted round robin, incorrect distribution can then be countered by assigning different weights to the servers available.

During a period of very low traffic, however, the load values as reported by the servers will not build a representative sample. A load distribution based on these values would result in uncontrolled, oscillating directives. Therefore in such a situation it is more reasonable, to calculate the load distribution based on the static weight ratio. The LoadMaster switches to the weighted round robin method automatically when the load on all servers falls below a limit defined by the administrator. If the load rises above the limit the LoadMaster switches back to the adaptive method.

For further information regarding Adaptive Balancing, please refer to **Appendix G: Headers Added by LoadMaster When ‘Client Certificates and Add Headers’ Option is Selected**

When the Client Certificates and add Headers option is selected in the Client Certificates drop-down while enabling SSL Acceleration, a number of headers are added. The following list describes the headers that are added to the https request by LoadMaster.

```
SSL_CLIENT_A_KEY="rsaEncryption"
SSL_CLIENT_A_SIG="md5WithRSAEncryption"
SSL_CLIENT_I_DN="/C=US/ST=Administrator/L=Limerick, Ireland/O=Kemp
Technologies/OU=Mary Rosse House/CN=MMC CA"
SSL_CLIENT_I_DN_C="US"
SSL_CLIENT_I_DN_CN="MMC CA"
SSL_CLIENT_I_DN_L=" Limerick, Ireland "
SSL_CLIENT_I_DN_O=" Kemp Technologies "
SSL_CLIENT_I_DN_OU=" Mary Rosse House "
SSL_CLIENT_I_DN_ST="Administrator"
SSL_CLIENT_M_SERIAL="05"
SSL_CLIENT_M_VERSION="3"
SSL_CLIENT_S_DN="/C=US/O= Kemp Technologies /OU= Mary Rosse House
/ST=Administrator/L= Limerick, Ireland /0.9.2342.19200300.100.1.1=jar/CN=Kemp
Sales/Email=sales@kemptechnologies.com"
SSL_CLIENT_S_DN_C="US"
SSL_CLIENT_S_DN_CN="Kemp Sales"
SSL_CLIENT_S_DN_Email="sales@kemptechnologies.com"
SSL_CLIENT_S_DN_L="Limerick, Ireland "
SSL_CLIENT_S_DN_O="Kemp Technologies "
SSL_CLIENT_S_DN_OU="Mary Rosse House "
SSL_CLIENT_S_DN_ST="Administrator"
SSL_CLIENT_VERIFY="SUCCESS"
```

```
SSL_CLIENT_V_END="Jan 16 14:30:35 2005 GMT"
SSL_CLIENT_V_START="Jan 18 14:30:35 2000 GMT"

SSL_SERVER_A_KEY="rsaEncryption"
SSL_SERVER_A_SIG="md5WithRSAEncryption"
SSL_SERVER_I_DN="/C=US/ST=Administrator/L=Limerick, Ireland/O=Kemp
Technologies/OU=Mary Rosse House/CN=MMC CA"
SSL_SERVER_I_DN_C="US"
SSL_SERVER_I_DN_CN="MMC CA"
SSL_SERVER_I_DN_L=" Limerick, Ireland "
SSL_SERVER_I_DN_O=" Kemp Technologies "
SSL_SERVER_I_DN_OU=" Mary Rosse House "
SSL_SERVER_I_DN_ST="Administrator"
SSL_SERVER_M_SERIAL="05"
SSL_SERVER_M_VERSION="3"
SSL_SERVER_S_DN="/C=US/O= Kemp Technologies /OU= Mary Rosse House
/ST=Administrator/L= Limerick, Ireland /0.9.2342.19200300.100.1.1=jar/CN=Kemp
Sales/Email=sales@kemptechnologies.com"
SSL_SERVER_S_DN_C="US"
SSL_SERVER_S_DN_CN="Kemp Sales"
SSL_SERVER_S_DN_Email="sales@kemptechnologies.com"
SSL_SERVER_S_DN_L="Limerick, Ireland "
SSL_SERVER_S_DN_O="Kemp Technologies "
SSL_SERVER_S_DN_OU="Mary Rosse House "
SSL_SERVER_S_DN_ST="Administrator"
SSL_SERVER_VERIFY="SUCCESS"
SSL_SERVER_V_END="Jan 16 14:30:35 2005 GMT"
SSL_SERVER_V_START="Jan 18 14:30:35 2000 GMT"
```

Appendix H: API for Agent Based Adaptive Balancing.

3.6 Fixed Weighted

The highest weight Real Server is only used when other Real Server(s) are given lower weight values. However, if highest weight server falls, the Real Server with the next highest priority number will be available to serve clients. The weight for each Real Server should be assigned based on the priority among Real Server(s).

3.7 Source IP Hash

A hash of the source IP is generated and used to find the correct real server. This means that the real server is always the same from the same host.

You don't need any source IP persistence.



This MAY cause real server imbalance.

4 Persistence

4.1 Introduction to Persistence

Persistence – which can also be referred to as “affinity”, “server affinity”, or “server sticky” -- is the property that enables all requests from an individual client to be sent to the same server in a server farm. Persistence is not turned on by default, but it is an option configurable for each Virtual Service.

Without persistence, the LoadMaster will direct traffic according to the load balancing algorithm, such as round-robin, weighted round-robin, etc. (Figure 1).

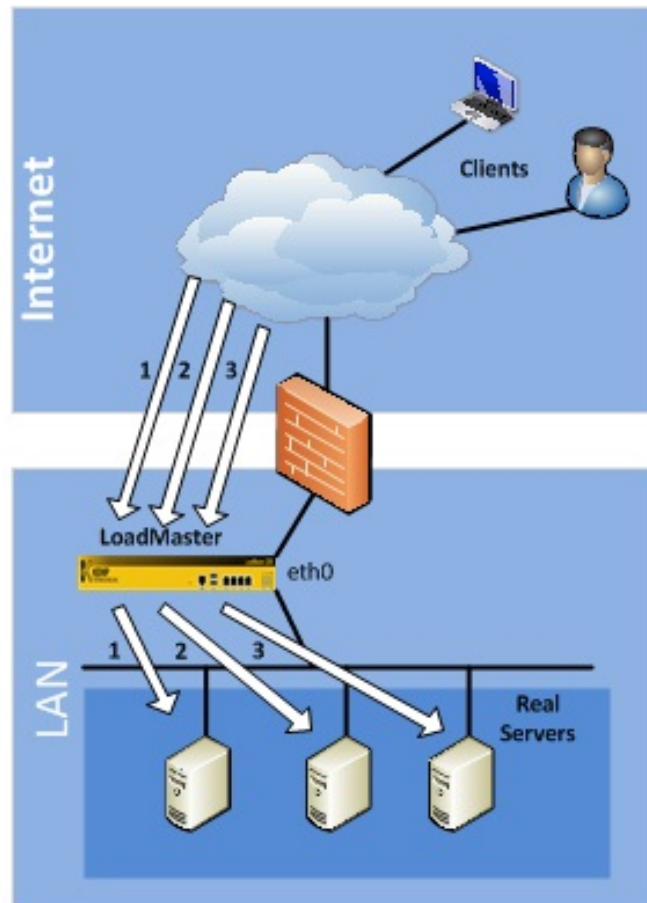


Figure 4-1 : Load Balancing without persistence

With persistence, the LoadMaster will direct new connections according to the load balancing algorithm, but returning connections will go to the same server (Figure 2).

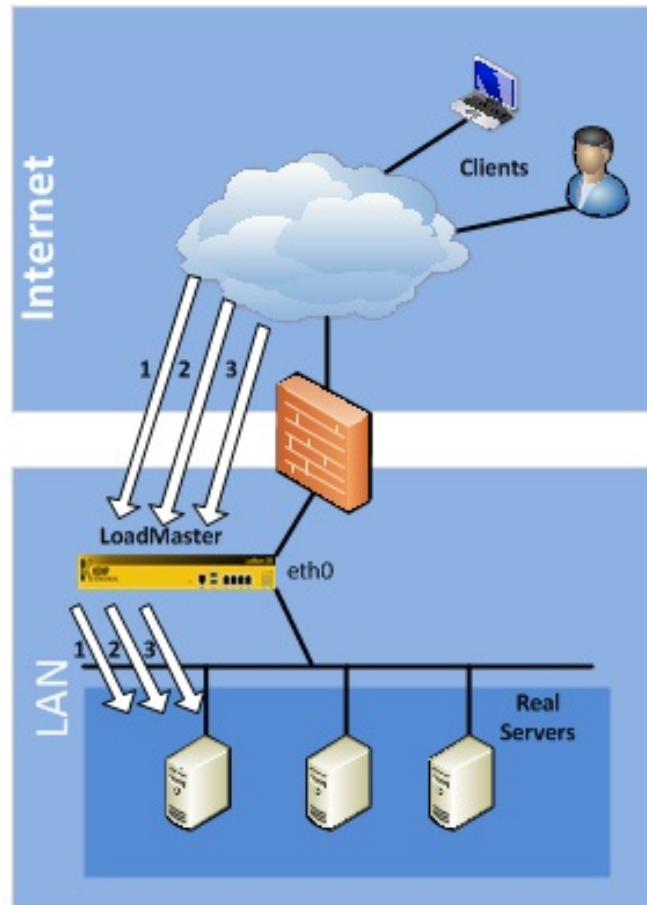


Figure 4-2 : Load balancing with persistence

4.2 How Do I Know If I Need Persistence?

If the site you're running is an interactive site, then chances are you'll need persistence. This is especially true for sites that require some type of login. If the site you're running is static, serving only static text and images, then you may not need persistence. In most cases, persistence can't hurt even if you don't need it.

The session handling mechanism for many website programming languages (ASP, PHP, etc.) are known as “stateful”, there is a unique session established for the user, and that “state” is kept on the same server. This stateful information, which can include everything from login credentials to the content of a shopping cart, is typically not shared among servers, so when using multiple servers it is important to keep an individual user tied to a specific web server for the duration of the interaction, and that is where persistence comes in.

4.3 Timeout

For each persistence method, there is a configurable timeout value that determines how long the persistence for each user is honored, selectable from 1 minute to 7 days.

This timeout clock is started from the **most recent active connection**, and not the initial connection. If a client made requests to the Virtual Server repeatedly within the timeout period, the persistence would be honored indefinitely.

For instance, if a Virtual Service has a timeout value set to 10 minutes, and a user comes in and made several requests in the course of 20 minutes, but the time between connections is always less than 1 minute. If the user goes idle for 20 minutes, then the next connection will be counted as a new session, and may be sent to a different server. If this is not long enough, then the timeout value should be set for a higher amount. In general matching this value to your server timeout value is recommended.

4.4 Layer 7 Persistence Methods

These are methods that look beyond the IP address and port, and provide a range of options to achieve layer 7 persistence.

4.4.1 Server Cookie Persistence

The Server Cookie option is a Layer 7 feature that uses existing cookies generated from the server to determine which server to send users to. This method is sometimes referred to as “passive cookie”, as the LoadMaster does not generate or manage the cookie, it only observes the cookie in the HTTP stream.

With Server Cookie persistence, you’ll need to configure the Cookie Name option so the LoadMaster knows which cookie to refer to. For Server Cookie persistence to work best, the cookie generated by the server should have a unique value for each individual user.

4.4.2 Active Cookie Persistence

The Active Cookie method is a Layer 7 feature that uses cookies like the pervious method, but with Active Cookie the cookies are generated by the LoadMaster, not the server.

When a connection comes into a LoadMaster Virtual Service configured with Active Cookie, the LoadMaster looks for a specific cookie. If that cookie is not there, the LoadMaster inserts it into the HTTP stream with a Set-Cookie directive. Existing cookies are not affected.

As with the Server Cookie persistence method, the value for the LoadMaster-generated cookie is unique to each user, allowing the LoadMaster to differentiate between users.

A benefit of this method is that no cookies need to be managed or generated by the servers, relieving the burden of server configuration. To gain better dispersion per client connection you can enable the “Add Port to Active Cookie” feature in the L7 configuration.

4.4.3 Server Cookie or Source IP Persistence

The Server Cookie or Source IP setting is identical to the Server Cookie setting, but with the additional fall-back method of source IP address. If, for any reason, the expected cookies aren't present (this can happen when a client browser is configured to refuse cookies), then the source IP address will be used to determine persistence.

4.4.4 Active Cookie or Source IP Persistence

The Active Cookie or Source IP setting is identical to the Active Cookie Persistence. If, for any reason, the expected cookies aren't present, then the source IP address will be used to determine persistence.

All things being equal, if you're going to use Layer 7 persistence, this is the recommended method. It requires no configuration on the servers, the LoadMaster manages all persistence-related cookies, and it falls back onto source IP address in cases where cookies are rejected by the client.

4.4.5 Hash All Cookies Persistence

The Hash All Cookies method creates a hash of the values of all cookies in the HTTP stream. Cookies with the same value will be sent to the same server for each request. If the values change, then the connection will be treated as a new connection. The client will then be allocated to a server according to the load balancing algorithm.

4.4.6 Hash All Cookies or Source IP Persistence

Hash All Cookies or Source IP is identical to Hash All Cookies, with the additional feature that it will fall back to Source IP persistence in the event no cookies are in the HTTP string.

4.4.7 Source IP Address Persistence

Source IP Address persistence uses the source IP address of the incoming request to differentiate between users. This is the simplest method of persistence, and works for all TCP protocols, including those that aren't HTTP related.

Source IP Address persistence is the only persistence option that can be used in conjunction with Content Switching or Direct Server Return deployments.

4.4.7.1 Weakness of Source IP Address

There are situations where Source IP persistence may be undesirable or even ineffective in properly keeping persistence. These situations include:

- When many (or all) users appear to come from a single IP address
- When a user switches IP addresses

The first case is often encountered when a significant number of user requests traverse a single proxy, and thus appear to come from a single IP. With Source IP persistence, this would mean that all of those users would appear as a single user. Another way this might occur is when all of the client requests come over the Internet from a single office. Office routers typically NAT all office systems to one IP address, so again, all users and all requests would appear to be a single user. This can result in uneven load balancing, since new user sessions arriving would all be directed to the same Real Server, without being balanced.

The second case is a largely historical concern, having to do with proxy servers at some of the mega-ISPs (e.g., AOL, Earthlink). In some cases, proxy configuration, or any number of networking issues, might switch IP addresses from time to time. When the IP address changes, the user appears as a different user to SRC persistence.

In each of these cases, Layer 7 persistence would solve the issue, regardless of what IP they came from. However, this only works for the HTTP protocol (and HTTPS/SSL when the session is terminated at the LoadMaster).

4.4.8 Super HTTP

Super HTTP is the recommended method for achieving persistence for HTTP and HTTPS services with the LoadMaster. It functions by creating a unique fingerprint of the client browser and uses that fingerprint to preserve connectivity to the correct Real Server. The fingerprint is based on the combined values of the User-Agent field and, if present, the Authorization header. Connections with the same header combination will be sent back to the same Real Server.

4.4.9 URL Hash

With URL Hash persistence, the LoadMaster will send requests with the same URL to the same server.

4.4.10 HTTP Host Header

With HTTP Host Header persistence, the LoadMaster will send all requests that contain the same value in the HTTP Host: header to the same server.

4.4.11 Hash of HTTP Query Item

This method operates that the named item being inspected is a Query Item in the Query String of the URL. All queries with the same Query Item value will be sent to the same server.

4.4.12 Selected Header

With Selected Header persistence, the LoadMaster will send all requests that contain the same value in the specified header to the same server

4.5 Persistence and HTTPS/SSL

With HTTPS/SSL, there are a few things to consider. If you're not terminating the SSL session at the LoadMaster, then your only options are Source IP Address persistence or SSL Session ID Persistence. Since the stream is encrypted in a non-terminated session, the LoadMaster cannot look at the HTTP headers or other Layer 7 information.

If you are terminating the HTTPS/SSL session at the LoadMaster, then any of the LoadMaster persistence options can be used. Since the HTTPS/SSL session is terminated, the LoadMaster sees all of the unencrypted traffic, and is able to look at the HTTP stream. This is true even when you're terminating the HTTPS/SSL session at the LoadMaster, and then re-establishing an SSL session with the Real Servers.

4.6 Port Following

When using “shopping cart” like services where a user selects items and adds them to a list, any of the previous types of persistency can be used. When the user then decides to pay for the items, this is normally performed using a secure SSL (https) service. When port following is turned on, the Real Server where the “shopping cart” connection is active will be selected for the SSL session. This selection will only occur when a connection is still open from the same client (as determined by the source IP address), and if the SSL service has the same IP address as the “shopping cart” service.

For example, if a connection is made to the HTTP service of www.somewebsite.com, and then a new SSL connection is made to the same address, then the SSL session will be directed to the same Real Server as the original HTTP service.

5 Application Front End

Application Front End is a group of features that revolve around web application delivery and network optimization. The introduction of the LoadMaster Application Front-End Services (AFE) solves very core requirements by providing better bandwidth and server utilization while allowing LoadMaster to remain a transparent load-balancing appliance that is easy to deploy and manage. LoadMaster AFE Services include:

- Intrusion Prevention System (IPS)
- Caching
- Data Compression

Each feature can be deployed per web Virtual Service.

Note: AFE features are license based if you do not have these features please contact your KEMP Sales Representative.

5.1 Intrusion Prevention System

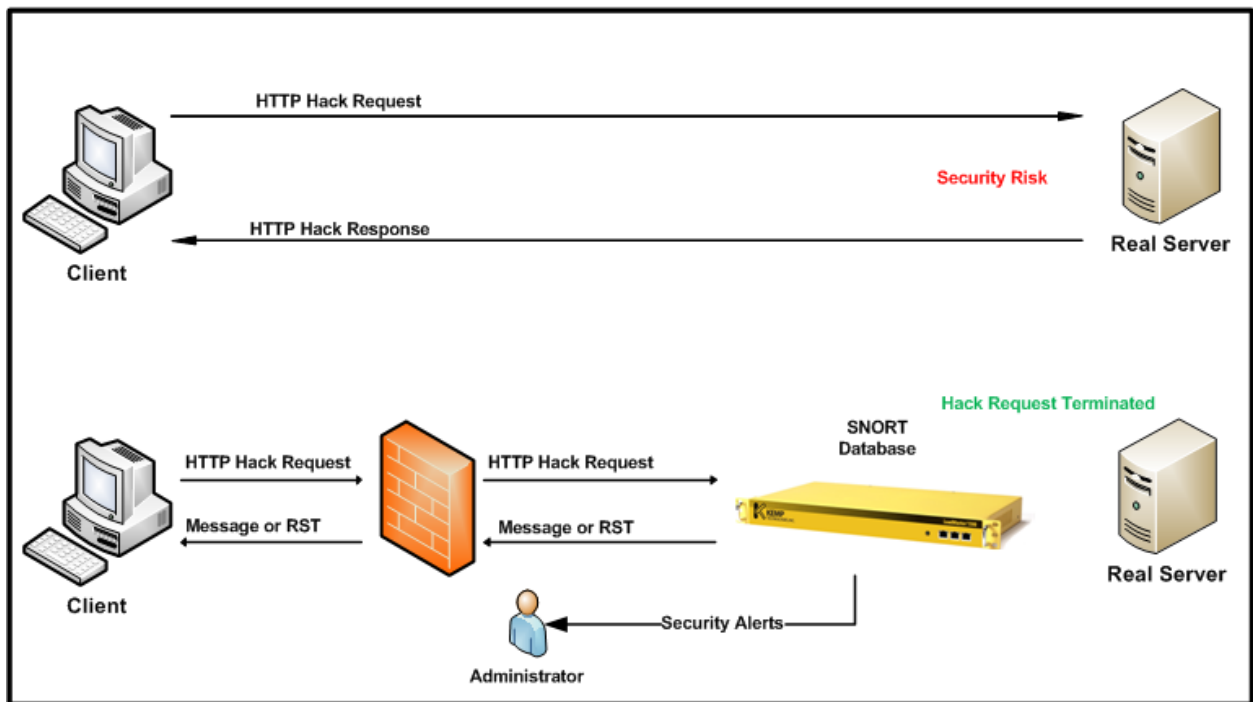


Figure 5-1 Intrusion Prevention

LoadMaster is an established hardened Internet appliance with HTTP intrusion prevention. In addition to Secure Socket Layer (SSL), Denial of Service support offered by LoadMaster the Intrusion Prevention System (IPS) service will provide in-line protection of Real Server(s) by providing real-time mitigation of attacks and isolation of Real Server(s). Intrusion prevention is based on the industry standard SNORT database and provides real-time intrusion alerting.

⚠ The LoadMaster supports SNORT rules version 2.8 and below.

IPS can be enabled per HTTP and off loaded HTTPS Virtual Services.

5.1.1 Intrusion Handling

There are two options for handling of requests that match a SNORT rule. Drop Connection or Send Reject. Both options prevent the request from reaching the Real Server(s); this option configures the response returned to the client sending the malicious request.

Drop Connection Intrusion Handling

A rule match will generate no HTTP response. The TCP connection will terminate, no HTML content will be delivered to the client.

Send Reject Intrusion Handling

Once a rule is matched the response to the client will be set to HTTP 400 “Invalid Request” and the corresponding exploit note will be delivered to the client in a HTML document.

Sample Request: `http://<VIP>/modules/articles/index.php?cat_id=SQL`

Sample Response: `<html><head><title>400 Invalid Request</title></head><body>Invalid Request: COMMUNITY WEB-PHP Xoops module Articles SQL Injection Exploit</body>`

5.1.2 Detection level

The aggressiveness of rule matching can be configured globally for the appliance as per SNORT priority level, details available at http://www.snort.org/docs/snort_manual/node220.html

- **Low** = Only logging with no rejection
- **Default** = Priority 1 (high) rules are block all else is logged
- **High** = Priority 1 (high) and 2 (medium) rules are block all else is logged
- **Paranoid** = All priority levels are blocked and logged

5.1.3 Warnings

The IPS system will throw out any malicious connections, but there are some requests that aren't exactly dangerous, but an indication that something may be wrong. These are not blocked and by default, these are not logged, turning on the WARNING option will allow the logging of these requests.

Examples for non-dangerous operations are requests that are specified as misc-activity in the snort rule file:

Uri: `"/OvCgi/OpenView5.exe?Context=Snmp&Action=Snmp&Host=&Oid="`

which is described as "WEB-MISC HP OpenView Manager DOS" and is only suspicious.

5.1.4 Intrusion Alerts

All intrusion alerts are recorded in the system and warning logs. Alert notification can also be obtained by syslog facility, the minimum level is Notice Host, and email alert facility, the minimum level is Notice Recipient. It is recommended that critical system messages like intrusion alerts be recorded by a syslog facility for records retention.

5.1.5 SNORT Configuration

Rules can be downloaded from www.snort.org Once a new rule set has been obtained or created you can load the rule set by using the WUI and navigating to System Configuration -> Miscellaneous Options -> L7 Configuration. Using the “Browse” button locate the downloaded rules file. The rules files should be encoded in a Tar and Gzip file end with the tar.gz extension and containing a directory named “rules”, LoadMaster will uncompress this file and reload the new rule files. (tar.gz is the standard format for rules download from www.snort.org) Installing a new rules file will replace the current rules. LoadMaster ships with the Community Rules under GPL by default.

5.2 Caching

The LoadMaster advanced caching engine saves valuable Real Server processing power and bandwidth, which can be dedicated to performing critical core business application logic. Significant server performance gains can be achieved when implementing caching. Chatty protocols such as HTTP require frequent creating and closing of connections for fetching of static resources, creating unnecessary resource utilization on Real Server(s) and the network. By enabling LoadMaster caching you can re-purpose connection related resources for more relevant business logic. Deploying LoadMaster caching your organization can also greatly reduce web traffic to Real Server(s) saving on bandwidth in-front of your Real Server(s).

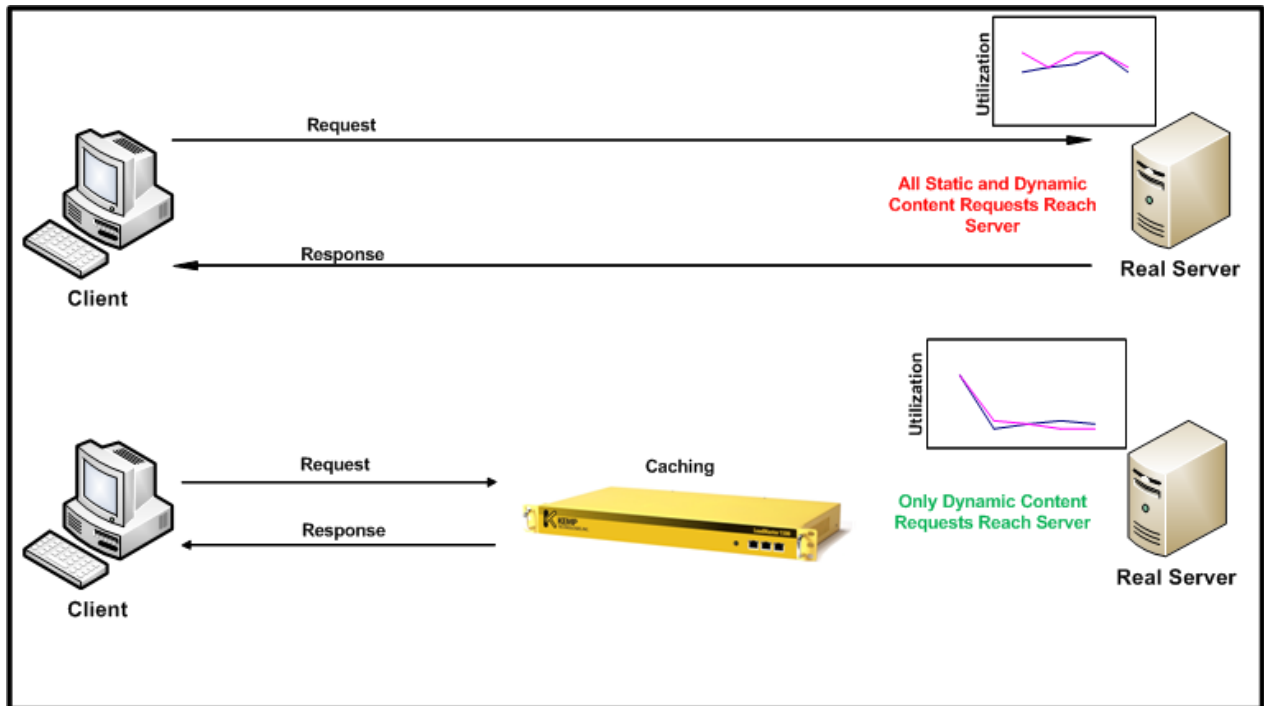


Figure 5-2 : Caching

Caching can be enabled per HTTP and off loaded HTTPS Virtual Services.

Note: HTTP/HTTPS requests with no-cache headers will bypass the cache, following RFC 2616. Cache is filled in a delayed manner please allow up to a few seconds for static content to be cached.

Note: In accordance with RFC 2616, URLs which contain query strings (those containing a “?” in the rel_path part) will not be cached

5.2.1 Flushing Cache

LoadMaster will not monitor file changes on the Real Server and auto-reload the cache maintained within the Virtual Service. You can force reload the cache by deselecting and selecting the “Enable Caching” checkbox. You can also reload a cached object sending a non-cache request, most browser support this by holding the left-shift key and clicking reload (or pressing F5).

5.2.2 Maximum Cache Size

The amount of global memory available for caching can be configured; values have a linear relation to actual memory. Navigate to Virtual Services -> View/Modify -> Modify -> Advanced Properties

5.3 Data Compression

The LoadMaster data compression feature reduces the amount of data to be transferred for HTTP objects by utilizing gzip compression available in all modern web browsers. Leveraging Lempel-Ziv (LZ) compression and HTTP/1.1 GNU zip (gzip) content encoding reduces bandwidth utilization for high compression files such as text files (HTML, CSS, and JavaScript). Data compression allows LoadMaster to compress the application payload per request, reducing network bandwidth consumption without degrading content quality and response time resulting in an improvement for the end-users' overall experience. Data compression is supported on all files. Compression ratios vary by file type.

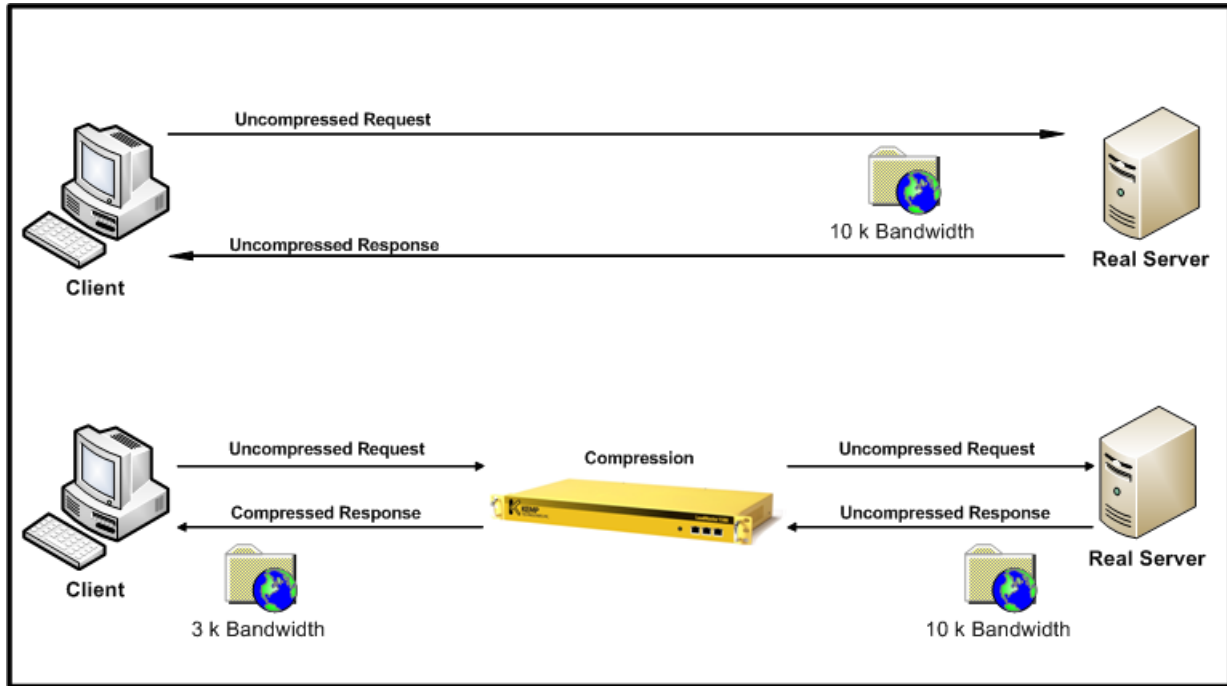


Figure 5-3 : Data Compression

Note: The compression feature should be deployed simultaneously with the caching feature to reduce the real-time inline compression requirements. Using only compression can potential bottleneck Virtual Service throughput depending on hardware platform.

Compression can be enabled per HTTP and off loaded HTTPS Virtual Services.

Compression depends on clients having gzip support. You can verify that a compressed connection to the Virtual Service exists by tracing the client HTTP traffic. If you can locate the following header your client communication to LoadMaster is compressed.

6 SSL Acceleration/Offloading

The LoadMaster series offers SSL termination/acceleration for Virtual Services. With SSL acceleration, the SSL session is terminated at the LoadMaster.

There are two primary benefits to SSL acceleration:

- The LoadMaster offloads the SSL workload off the Real Servers (very useful when hardware acceleration is done)
- The LoadMaster can perform Layer 7 processing: persistence or content switching

Without terminating the SSL session at the LoadMaster, the headers and content cannot be read, so persistence cannot be done. The only consistently reliable persistence method available when the SSL session is not terminated at the LoadMaster is Source IP. SSL session ID is rarely a viable persistence method because of the behavior of many browsers (the SSL session IDs are renegotiated every 2 minutes).

With SSL acceleration, the LoadMaster uses a specialized processor to perform the SSL functions. With this SSL acceleration hardware, the LoadMaster can handle SSL connections as easily as it handles non-SSL connections.

All LoadMasters have the ability to perform SSL termination. There are two types of SSL termination capabilities:

- Hardware SSL
- Software SSL

Functionally, hardware and software SSL are the same. The difference is in what part of the LoadMaster handles the actual cryptographic functions associated with SSL operations.

With software SSL, the LoadMaster's general processor handles encryption/decryption tasks. These tasks are shared with other tasks that the LoadMaster performs, such as load balancing, health checking, and other administrative tasks. Because SSL operations are CPU-intensive, software SSL is sufficient for low levels of SSL traffic but insufficient for higher levels of SSL traffic. Higher connection rates of SSL on a software SSL LoadMaster may degrade overall performance of the LoadMaster.

With hardware SSL, the LoadMaster has a separate specialized processor which handles all SSL functions. No matter the level of SSL connections, the LoadMaster's general processor is not burdened. This specialized hardware is purpose-built for SSL, and can handle extremely high connection rates (TPS) of SSL traffic.

6.1 Self-Signed versus CA Signed Certificates

An SSL certificate is required for all SSL transactions, and as such is required for all SSL-enabled Virtual Services. With the LoadMaster, there are two types of SSL certificates: self-signed certificates generated by the LoadMaster itself and certificates that are signed by a CA (Certificate Authority) such as Verisign or Thawte.

When an SSL-enabled Virtual Service is configured on the LoadMaster, a self-signed certificate is installed automatically.

Generally, self-signed certificates should not be used for public-facing production websites.

They may be acceptable for use in some other scenarios, such as:

- Intranet sites
- QA sites, where web sites are tested but not presented to the general public

6.2 Certificate Basics

Both self-signed and CA signed certificates provide encryption for data in motion. A CA-signed certificate also provides authentication -- a level of assurance that the site is what it reports to be, and not an impostor website.

6.3 Operational Differences

The primary operational difference between a self-signed certificate and a CA certificate is that with a self-signed, a browser will generally give some type of error, warning that the certificate is not issued by a CA. With Internet Explorer 7.0, the self-signed certificate error is shown in Figure 1.

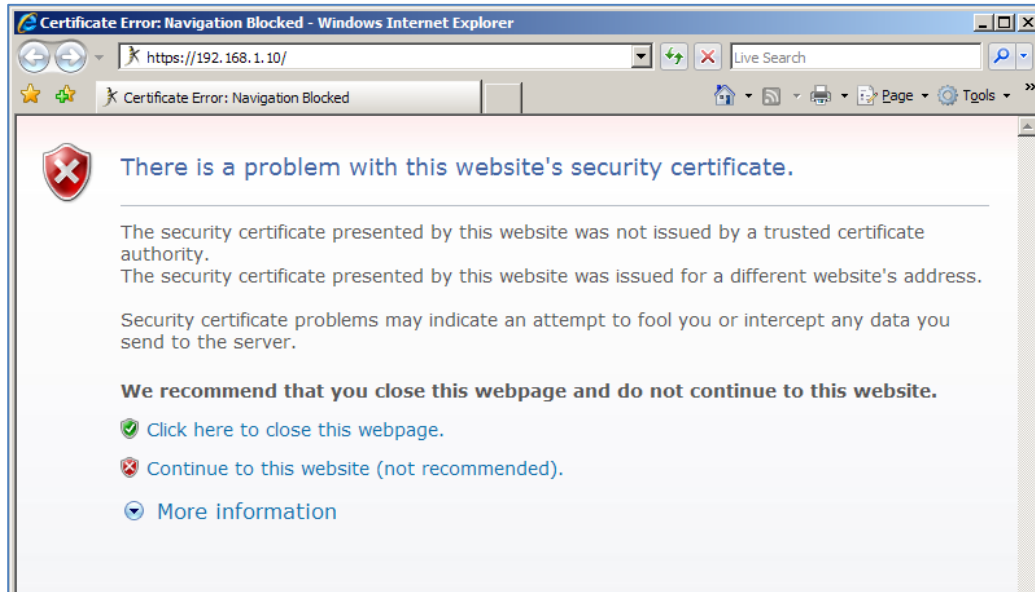


Figure 6-1 : Self-Signed Certificate Error

This is the same warning message you receive when connecting to the WUI, as the WUI uses a self-signed certificate. Generally, this warning should occur only once per browsing session.

7 Rule Based Content Switching

The LoadMaster series of load balancers support content switching, which is sometimes referred to a URL switching. This allows the LoadMaster to direct specific requests to specific Real Servers based on the contents of the requested URL.

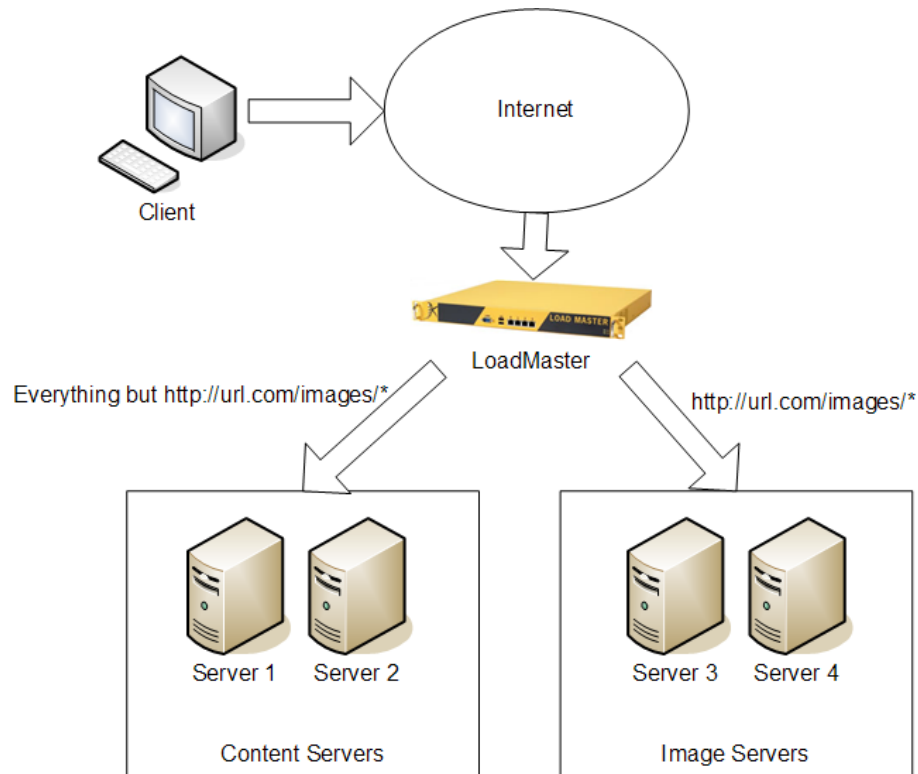


Figure 7-1 Rule-based content switching

For instance, if you have two groups of servers, one group to serve images and the other to serve up all other content, you can create content rules to separate these two classes of request (Fig. 1).

Any URL that includes /images in it, such as “http://url.com/images/party.jpg” or “http://url.com/images/dogs.jpg” would be directed to server 3 and 4, while anything else would be directed to server 1 and 2.

This can be very useful if you have servers that perform different functions (application servers, static content servers, mapping servers, specialized content generation servers, etc.) that must all be served from the same general hostname (e.g., www.websitename.com).

7.1 Terminology

Note: The term content switching does not refer to the process involved with Layer 2 switching. Instead, content switching refers to switching traffic between different servers, depending upon the content requested.

7.2 Limitations to Content Switching

With content switching enabled on a given Virtual Service, you cannot utilize other Layer 7 functionality, such as persistence. You can have one Virtual Service utilizing Layer 7 persistence, and another Virtual Service performing content switching, you just cannot have them running on the same Virtual Service.

7.3 Using Content Switching

There are two parts to configuring content switching: The content rules, and the Virtual Service configuration. The content rules are configured globally on the LoadMaster, and various rules are applied to specific Real Servers operating under a Virtual Service..


8 Health Checking

8.1 Overview


The LoadMaster utilizes health checks to monitor the availability of the Real Servers and the Virtual Services. In case that one of the servers does not respond to a health check within a defined time interval for a defined number of times, the weighting of this server will be reduced to zero. This zero weighting has the effect of removing the Real Server from the Virtual Service configuration until it can be determined that this Real Server is back online.

The LoadMaster uses health checks that can be specified using the Web user interface. As a default the highest possible health check is associated with a Virtual Service. The LoadMaster performs Layer7 health checks for the following ports:

Service	Port	Protocol
FTP	21	TCP
TELNET	23	TCP
SMTP	25	TCP
HTTP	80	TCP
HTTPS	443	TCP
POP3	110	TCP
NNTP	119	TCP
IMAP	143	TCP
DNS	53	UDP

 When creating a Virtual Service and using a service type other than Generic, additional health checking protocols are available. Ex) The service type Remote Terminal will permit checking with Remote Terminal Protocol.

For other ports the LoadMaster uses Layer4 health checks for TCP services and Layer3 health checks for UDP services. The settings for the health checks can be changed from the default settings using the Virtual Service wizard to accommodate non-standard settings. For example, one could run an http service on port 8080 instead of 80, and change the health check to HTTP instead of the default Layer4 check.

 These global settings hold for all servers in the farm, i.e. you cannot assign different timeouts for different servers.

It is mandatory that one of the service checking options be used when defining a Virtual Service on the LoadMaster.

8.2 Service and Non-Service Based Health Checking

Layer3 health checks utilize ICMP based echo requests (pings) to test whether a Real Server can be reached over the network. A Layer3 check is not Virtual Service specific, e.g. when it fails, the corresponding Real Server will be removed from all Virtual Services that use it.

In contrast to the Layer3 health checks, service based health checking for both the Layer 4 and Layer 7 health checks are Virtual Service based. When a Real Server fails such a check, it will be removed only from the corresponding Virtual Service – all other Virtual Services that use this Real Server are unaffected.

Type	Description
ICMP	The LoadMaster sends ICMP echo requests (pings) to the Real Servers. A Real Server fails this check when it doesn't respond with an ICMP echo response in the configured response time for the configured number of retries.
TCP	The LoadMaster attempts to open TCP-connection to the Real Server on the configured service port: It sends a TCP SYN packet to the server on the service port. The server passes the check if it responds with a TCP SYN ACK in the response time interval. In this case the LoadMaster closes the connection by sending a TCP RESET. If the server fails to respond within the configured response time for the configured number of times, it is assumed dead.
FTP	The LoadMaster opens a TCP connection to the Real Server on the Service port (port 21). If the server responds with a greeting message with status code 220, the LoadMaster sends a QUIT command to the server, closes the connection and marks it as active. If the server fails to respond within the configured response time for the configured number of times or if it responds with a different status code, it is assumed dead.
TELNET	The LoadMaster opens a TCP connection to the Real Server on the Service port (port 23). If the server responds with a command string beginning with the char '0xff', the LoadMaster closes the connection and marks the server as active. If the server fails to respond within the configured response time for the configured number of times or if it responds with a different command string, it is assumed dead.
SMTP	The LoadMaster opens a TCP connection to the Real Server on the Service port (port 25). If the server responds with a greeting message with status code 220, the LoadMaster sends a QUIT command to the server, closes the connection and marks it as active. If the server fails to respond within the configured response time for the configured number of times or if it responds with a different status code, it is assumed dead.

Type	Description
HTTP	The LoadMaster opens a TCP connection to the Real Server on the Service port (port 80). The LoadMaster sends a HTTP/1.0 HEAD request the server, requesting the page “/”. If the server sends a HTTP response with a status code of 2 (200-299, 301, 302, 401) the LoadMaster closes the connection and marks the server as active. If the server fails to respond within the configured response time for the configured number of times or if it responds with a different status code, it is assumed dead. HTTP 1.0 and 1.1 support available, using HTTP 1.1 allows you to check host header enabled web servers.
HTTPS	The LoadMaster opens a SSL connection to the Real Server on the Service port (port 443). The LoadMaster sends a HTTP/1.0 HEAD request the server, requesting the page “/”. If the server sends a HTTP response with a status code of 2 (200-299, 301, 302, 401) the LoadMaster closes the connection and marks the server as active. If the server fails to respond within the configured response time for the configured number of times or if it responds with a different status code, it is assumed dead. HTTP 1.0 and 1.1 support available, using HTTP 1.1 allows you to check host header enabled web servers.
POP3	The LoadMaster opens a TCP connection to the Real Server on the Service port (port 110). If the server responds with a greeting message that starts with +OK, the LoadMaster sends a QUIT command to the server, closes the connection and marks it as active. If the server fails to respond within the configured response time for the configured number of times or if it responds with a different status code, it is assumed dead.
NNTP	The LoadMaster opens a TCP connection to the Real Server on the Service port (port 119). If the server responds with a greeting message with status code 200 or 201, the LoadMaster sends a QUIT command to the server, closes the connection and marks it as active. If the server fails to respond within the configured response time for the configured number of times or if it responds with a different status code, it is assumed dead.
IMAP	The LoadMaster opens a TCP connection to the Real Server on the Service port (port 143). If the server respond with a greeting message that start with “+ OK” or “* OK”, the LoadMaster sends a LOGOUT command to the server, closes the connection and marks it as active. If the server fails to respond within the configured response time for the configured number of times or if it responds with a different status code, it is assumed dead.
DNS	The LoadMaster sends Source-of-Authority (SOA) request to the Real Server on the service port (port 53 UDP). If the server successfully responds to the SOA request, the LoadMaster marks it as active. If the server fails to respond within the configured response time for the configured number of times or if it responds unsuccessfully to the SOA request, it is assumed dead.

Type	Description
RDP	The LoadMaster opens a TCP connection to the Real Server on the Service port (port 3389). The LoadMaster sends a 1110 Code (Connection Request) to the server. If the server sends a 1101 Code (Connection Confirm) then LoadMaster closes the connection and marks the server as active. If the server fails to respond within the configured response time for the configured number of times or if it responds with a different status code, it is assumed dead.
None	No health checking is performed

9 SNMP Support

Simple Network Management Protocol (SNMP) is a protocol that allows one to manage many network devices over the network from a remote management station (SNMP manager).

The manager station can request data from the managed stations (SNMP agents) or it can change the value of data on the agents.

The managed stations (SNMP agents) can also be set up to alert the manager when some predefined events occur, e.g. such as a unit failover. The alerting mechanism uses so-called event traps.

The current version is SNMPv3, the two previous revisions in use are SNMPv1 and SNMPv2c (community-based SNMPv2).

The SNMP support of the LoadMaster is based on SNMPv3, and is backward compatible such that all 3 of the above versions can be used. However, since SNMPv1 does not support 64bit-values (as used in the LoadMaster MIB), it is recommended to use SNMPv2c or SNMPv3. MsgSecurity is supported only with SNMP v1 and v2c.

Note: When monitoring LoadMaster in HA please monitor individual appliances by the appropriate Ethernet address.

The information regarding all LoadMaster-specific data objects is stored in three enterprise-specific MIBs (Management Information Base).

ONE4NET-MIB.txt	enterprise id
IPVS-MIB.txt	Virtual Server stats
B-100-MIB.txt	LoadMaster configuration data

These MIBs (which are located on the LoadMaster CD and also available for download from www.kemptechnologies.com) need to be installed on the SNMP manager machine in order to be able to request the performance-/config-data of the LoadMaster via SNMP. A file describing the MIBs (one4net.mib.desc) can be found online.

The SNMP support is disabled by default.

10 LoadMaster Software Upgrades

10.1 Online Upgrades

The LoadMaster provides the ability to perform online software updates and upgrades. Patches will be made available by KEMP Technologies, these patches should be installed on a machine which supports an FTP, a HTTP or an SSH daemon.

Patches are checksummed (with MD5) and encrypted to protect against data corruption or tampering.

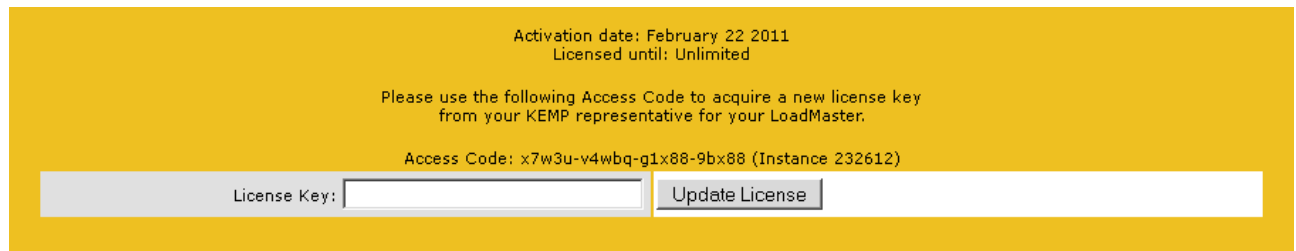
Using the configuration menu (utilities->software upgrade), it is possible to download the patch from the server machine (the protocol used can be FTP, SCP or HTTP). When the patch has been downloaded, the patch will be unpacked and checked.

If the patch is valid, the patch version will be displayed and the user will be asked if the patch should be installed. Upon the successful installation of the patch, the LoadMaster should be rebooted to activate the new version.

If for some reason, the patch does not perform as required, the previous version of the software may be reactivated via the configuration menu.

Converting from a 30 or 60 day evaluation license to a full license or from a L4 only to a L4 and L7 license can be performed using the menu item Utilities->Update License. If the LoadMaster is already running in a L4+L7 mode, this menu option is not available.

License information can be entered in the Web User Interface at System Configuration -> System Administration -> Update License




The screenshot shows a yellow background with the following text and form elements:

- Activation date: February 22 2011
- Licensed until: Unlimited
- Please use the following Access Code to acquire a new license key from your KEMP representative for your LoadMaster.
- Access Code: x7w3u-v4wbq-g1x88-9bx88 (Instance 232612)
- License Key:
- Update License

After updating a license key a reboot should be performed to enable the new functionality.

Patch support can expire; in that case you will be notified during the upgrade procedure.

 If you receive the message 'Update not permitted' please contact KEMP Technologies for re-licensing.

11 User Management

LoadMaster supports multiple user logins with varying levels of access that can be managed by navigating to System Configuration -> System Administration -> User Management. Each username must be a minimum of three characters and a maximum of ten. Passwords must be a minimum of six characters long. Users created here can only access the Web User Interface; (WUI) remote access via SSH is not supported.

11.1 Roles/Permission

The factory default username is “**bal**” and the default password is “**1fourall**”. The factory default user retains the highest level of access. All users created on LoadMaster have a subset of access permitted by the default account. Changing roles for users take effect in real-time. Roles can be combined and are mutually exclusive.

The default access for users is read only access to LoadMaster’s Web User Interface., generating Certificate Signing Requests, read access to log files, and the ability to perform basic debugging.

11.1.1 Real Servers

This role permits enabling and disabling Real Servers.

11.1.2 Virtual Services

This role permits managing Virtual Services. Virtual Service modifications permitted include add, delete and modify for any subnet.

11.1.3 Rules

This role permits managing Rules. Rule modifications permitted include add, delete and modify.

11.1.4 Certificate Creation

This role permits managing SSL Certificates. Certificate management includes add, delete and modify SSL Certificates.

11.1.5 3rd Party Certificates

This role permits managing 3rd Party SSL Certificates. Certificate management includes the ability to add and delete intermediate certificates.

11.1.6 Certificate Backup

This role permits managing 3rd Party SSL Certificates. Certificate management includes the ability to add and delete intermediate certificates. Also included in this role is the ability to export and import certificate.

11.1.7 Allowed Network

This role is based on configured subnets on Loadmaster; it is a dynamic role. Each subnet can be assigned to a user. Only Virtual Services, Interfaces and Real Servers of that subnet are viewable. This role should be used in conjunction with other roles.

11.1.8 All Permissions

This role gives users all permissions **except** the permission to change the **bal** password and the permission to create or delete other users

11.1.9 GEO

This role is used only with the LoadMaster GEO product

12 Bonding and VLAN

12.1 Overview

LoadMaster bonding/VLAN tagging can be easily setup and configured using the Web User Interface (WUI), successful deployment requires that the pre-requisites have been satisfied. This guide is designed to introduce interface bonding and VLAN configuration on LoadMaster. Bonding support is available with all network modules.

12.2 Pre-requisite (Switch Compatibility)

VLAN Tagging

IEEE 802.1Q

Bonding/Teaming (802.3ad/Active-Backup)

IEEE 802.1AX/IEEE 802.3ad/LACP

12.2.1 Switch configuration

Enabling the Active-Backup mode generally does not require switch intervention and can be configured directly on LoadMaster. Using the 802.3ad bonding mode will require configuring a link aggregation group on the switch in conjunction with the LoadMaster. Please read your switch documentation to establish the corresponding team/bond, common terms for link aggregation include "Ethernet trunk", "NIC teaming", "port channel", "port teaming", "port trunking", "link bundling", "EtherChannel", "Multi-Link Trunking (MLT)", "NIC bonding", "Network Fault Tolerance (NFT)" and "LAG".


When enabling VLAN trunking on the switch port make sure to configure the port to support the appropriate mode, General, Access, or Trunking. General descriptions are as follows; check your switch documentation for specifics.


- General: the port belongs to VLANs, and each VLAN is user-defined as tagged or untagged (full 802.1Q mode).
- Access: the port belongs to a single untagged VLAN.
- Trunk: the port belongs to VLANs in which all ports are tagged.

12.3 Bonding/Teaming (802.3ad/Active-Backup)

There are a few key things to keep in mind when creating bonds/teams:

- You can only bond interfaces higher than the parent, so if you choose to start with port 10 then you can only add ports 11 and greater
- Bond links first if you need VLAN tagging then add VLANs after the bond has been configured
- In order to add a link to a bonded interface, any IP addressing must first be removed from the link to be added
- Enabling the Active-Backup mode generally does not require switch intervention

 Ensure that all bonded interfaces are configured for the same link speed, both on the switch and LoadMaster.

 If you wish to bond port 0, KEMP recommends you move the web administrative interface and/or the remote SSH access to a different port temporarily until the bonding has been completely configured and working.

12.4 VLAN Tagging

Things to keep in mind:

- Configure VLAN tagging on the switch first, if required
- Start by deciding if you need bonding, if you do first establish your bonded configuration and then proceed by adding the VLAN tagging information
- VLANs can be added to physical interfaces or bonded interfaces

13 Miscellaneous


13.1 IPv6 Support

This version of LoadMaster software includes IPv6 support. Before you layout your network addresses, consider which will remain as IPv4 and which will convert to IPv6. The LoadMaster is capable of supporting, and is able to translate between, unlike networks. Thus, you may have an internal network that is IPv6, and interconnect to an external IPv4 network.

13.2 Remote Syslog Support

The LoadMaster can produce various warning and error messages using the syslog protocol. These messages are normally stored locally and may be displayed via the diagnostics menu point. It is also possible to configure the LoadMaster to transmit these error messages to a remote syslog server (menu point: extended->syslog). Six different error message levels are defined. Each level of message may be sent to a different host server.

Notice messages are sent for information only; Emergency messages normally require immediate user action.

 To enable a syslog process on a remote Linux server to receive syslog messages from the LoadMaster, the syslog must be started with the “-r” flag.

13.3 How to get a license

After boot, a login prompt appears; login as ‘bal’ (password ‘1fourall’).

To unlock the LoadMaster software you need a license key. The license key will be generated individually for each single LoadMaster instance in conjunction with a hardware dependent Access Code.

There are three different licenses that you can get for your LoadMaster:

1. An evaluation license. This is a fully functional license valid for up to 30 days.
2. A full, non time-limited LoadMaster license.
3. A full, non time-limited license for a LoadMaster High Availability (HA) cluster consisting of two machines.

An evaluation license can be upgraded to either a full single or a full HA license.

License information can be entered in the Web User Interface at System Configuration -> System Administration -> Update License. Repeat process for second LoadMaster if using HA systems.

13.3.1 Get a 30 day evaluation license

If not already provided, contact your KEMP Technologies Representative to obtain evaluation license. Be sure to provide the Access Code (or codes if HA), so the evaluation license can be “mapped” to the

unit(s). Customer contact should have provided KEMP with a valid email address to send license to Customer contact.

13.3.2 Get a full LoadMaster license

1. A service agreement upon purchase must be approved by KEMP in order to obtain a full LoadMaster appliance.
2. If not already provided contact your KEMP Technologies Representative to obtain evaluation license. Be sure to provide the Access Code (or codes if HA), so the evaluation license can be “mapped” to the unit(s). Customer contact should have provided KEMP with a valid email address to send license to Customer contact.

13.3.3 Get full High Availability LoadMaster cluster licenses

1. A service agreement upon purchase must be approved by KEMP in order to obtain a full LoadMaster HA license.
2. If not already provided contact your KEMP Technologies Representative to obtain evaluation license. Be sure to provide the Access Code (or codes if HA), so the evaluation license can be “mapped” to the unit(s).
3. Customer contact should have provided KEMP with a valid email address to send license to Customer contact.

You can request a license by visiting <http://www.kemptechnologies.com/activate.shtml>

Note: TPS Limits for SSL acceleration (100 default, 1000, 2000, 10,000) will be determined upon service agreement. Please contact your KEMP representative for more information and pricing.

Note: The License Keys and Access Codes are NOT interchangeable between machines.

13.3.4 Upgrading the evaluation license to a full single or HA license

1. A service agreement upon purchase must be approved by KEMP in order to obtain a full LoadMaster HA license.
2. If not already provided contact your KEMP Technologies Representative to obtain evaluation license. Be sure to provide the Access Code (or codes if HA), so the evaluation license can be “mapped” to the unit(s).
3. Customer contact should have provided KEMP with a valid email address to send license to Customer contact.

You can request a license by visiting <http://www.kemptechnologies.com/activate.shtml>

Note: TPS Limits for SSL acceleration (100 default, 1000, 2000, 10,000) will be determined upon service agreement. Please contact your KEMP representative for more information and pricing.

Note: The License Keys and Access Codes are NOT interchangeable between machines.

13.4 Backup and Restore

The configuration of a LoadMaster balancer can be saved over a network to a remote server. The complete configuration (the Virtual Service Configuration and the “base” Configuration) of the LoadMaster will be saved to a single file on the server. It is important to note that no SSL certificate information is contained within the backup. The server must be running an FTP daemon or an SSH daemon. By default the remote protocol will be FTP. Using console or SSH access go to ‘7’ Utilities, then ‘2’ Transfer protocol to change setting. Consult the WUI User Manual to perform this function via its Web User Interface.

When a configuration is restored, the user will be asked which parts of the configuration should be restored:

- The Virtual Service Configuration only,
- The LoadMaster “base” Configuration only,

- The Virtual Service + the LoadMaster “base” Configuration.

The “base” configuration contains the information about the basic configuration of the LoadMaster, i.e. the IP addresses of the various interfaces and the keyboard and time zone settings.

The Virtual Service Configuration contains only the information about the Virtual Services and the Real Servers.

Note: When performing a restore on the standby machine of a HA cluster; only the base configuration can be restored. The Virtual Service Configuration will be taken from the active machine.

13.5 Interoperability between L4 / L7 Virtual Services

When one switches a service from one persistency method to another, the absolute values of all VS / RS counters will be reset to zero.

This may cause peaks in the service graphs when displaying relative values (bytes per second, etc.) when e.g. the bytes counter jumps from terabyte values to zero.

13.6 Log Information

Log files are viewable in the WUI at System **Configuration > Logging Options > Log Files**

- Boot.msg File contains Linux standard boot information.
- Warning Message File contains event generated by the core load-balancing engine.
- System Message File contains event generated by the core load balancing and the underlying Linux operation system.

Note: Log files are volatile, to ensure critical log information is available in the event of a recycle on LoadMaster please use the syslog facility.

13.7 Debugging Utilities

Utilities can be executed in the WUI at System Configuration -> Logging Options -> Log Files -> Debug Options These utilities are best utilized with the KEMP Support Team.

13.7.1 Disable All Transparency

Alter transparency for all Virtual Services, this option should only be changed with approval from the KEMP Support Team.

13.7.2 Enable L7 Debug Traces

Enable additional debugging information that is captured in the System Messages log.

13.7.3 Perform a PS

Reports the process status.

13.7.4 Perform a l7adm

Display detail information about the Layer 7 Virtual Services in table format.

13.7.5 Ping Host

Issue an ICMP echo request to any IP4 device. Please make sure the target IP supports ICMP.

14 Various Networking Issues

14.1 S-NAT

When using a two-armed or multi-armed LoadMaster configuration, it is sometimes useful for the Real Servers to have access to the Internet. The default route for the Real Servers is through the LoadMaster. If however the Real Servers do not have routable addresses i.e. private addresses, this is not possible.

Using S-NAT, the LoadMaster will map all connections originating on a Real Server so that they appear to come from the LoadMaster itself, either from the IP address of the eth0 interface or from an IP address associated with a VIP. The Real Servers can thus use the Internet as if directly connected but with the extra security protection that they cannot be addressed directly from the Internet.

The use of S-NAT in single-armed configurations is not recommended.

The S-NAT functionality may be enabled or disabled over the configuration menus and WUI.

The S-NAT IP address is configurable. To configure the S-NAT IP you can use the WUI, system or the SSH access.

14.2 Default Gateway and Routes

In simple configurations, where the LoadMaster is installed in a network where there is only one route to the Internet, only the default gateway needs be specified. All traffic from the LoadMaster to the Internet will then be routed over this gateway. An example configuration is given in figure A.

When the LoadMaster is installed in a more complicated network configuration (for example as depicted in figure B), additional routes may be specified so that traffic for the specified subnets will be routed over alternative gateways. For example in figure B, a route could be set up to route data from a private network or over a secondary link gateway.

The options for routing configuration are static routes, per Virtual Service default gateway and a appliance level default gateway (see the Installation and Configuration Guide in this handbook). The LoadMaster does not currently support dynamic routing protocols.

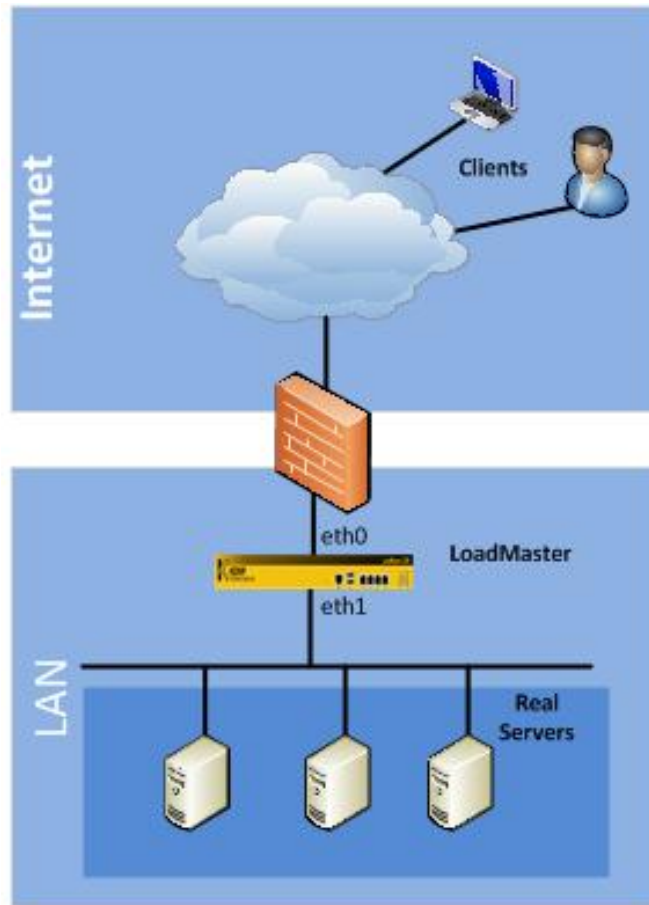


Figure 14-1 : LoadMaster single, 2-arm configuration

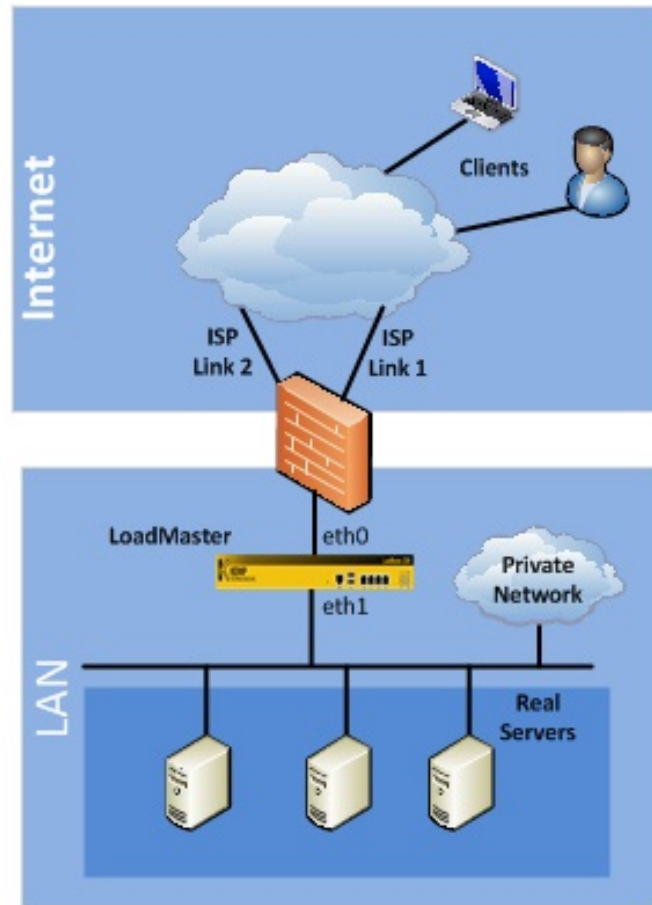



Figure 14-2 : LoadMaster dual ISP, single, 2-arm configuration

14.3 Non-Local Real Server Support

Load balancing a non-local Real Server is permitted when a Virtual Service is non-transparent. To make a Virtual Service non-transparent enable the “Force L7” checkbox. By default you can only load balance Real Servers that reside on the subnets configured on LoadMaster. To enable load balancing of Real Servers that do not reside on the same subnet use the Web User Interface and navigate to System Configuration > System Administrator > Miscellaneous Options > L7 Configuration > Enable Non-Local Real Servers. Then when adding Real Servers that are remote make sure to check the “Allow Remote Addresses” in the Real Server configuration panel.

15 Getting Started

To initially setup your LoadMaster machine(s) you will need a PC with a browser and the ability to connect to an IP address.

 If you do not have the capability to use a PC and a browser to configure the LoadMaster, you may use a console plugged into the Serial port of the LoadMaster, or you may plug in a VGA monitor and a USB keyboard. See Appendices B and C for instructions and console commands.

15.1 The LoadMaster Hardware Appliance


Delivery Content

The delivery of each LoadMaster contains the following components:

- A/C power cable.
- A Console (Serial) Cable
- A QuickStart Guide.
- Rack mounts for standard 19” server racks (where applicable).
- Appliance specific information sheet

15.2 Connecting the LoadMaster Hardware

The location of eth0 varies by LoadMaster model. Check the documentation that came with your LoadMaster for the location of eth0.

 If you are unsure of the correct connections, review LoadMaster Network Topologies, page 12.

15.2.1 Connection of eth0

Connect one end of a Category 5 Ethernet cable into the LoadMaster LAN port marked as ‘0’ and connect the other end to the hub/switch which interfaces with the default gateway. This is the external network side. If running single arm, the same port, eth0, is connected to the server farm side.

If running an HA configuration single arm, the eth0 ports on both LoadMasters will be connected to the network side and the server farm side.

15.2.2 Connection of eth1 and eth2

If running dual arm and in a single configuration, connect one end of a Category 5 Ethernet cable into the LAN port marked as ‘1’ and connect the other end to the hub/switch which interfaces with the server farm. This is the internal server side.

If running dual arm and in an HA configuration, connect one end of a Category 5 Ethernet cable into the LAN port marked as ‘1’ on one unit and connect the other end to the LAN port marked as ‘1’ on other unit. This is the backup linkage between the HA pair.

Then connect one end of a Category 5 Ethernet cable into the LAN port marked as ‘2’ and connect the other end to the hub/switch which interfaces with the server farm. This is the internal server side.

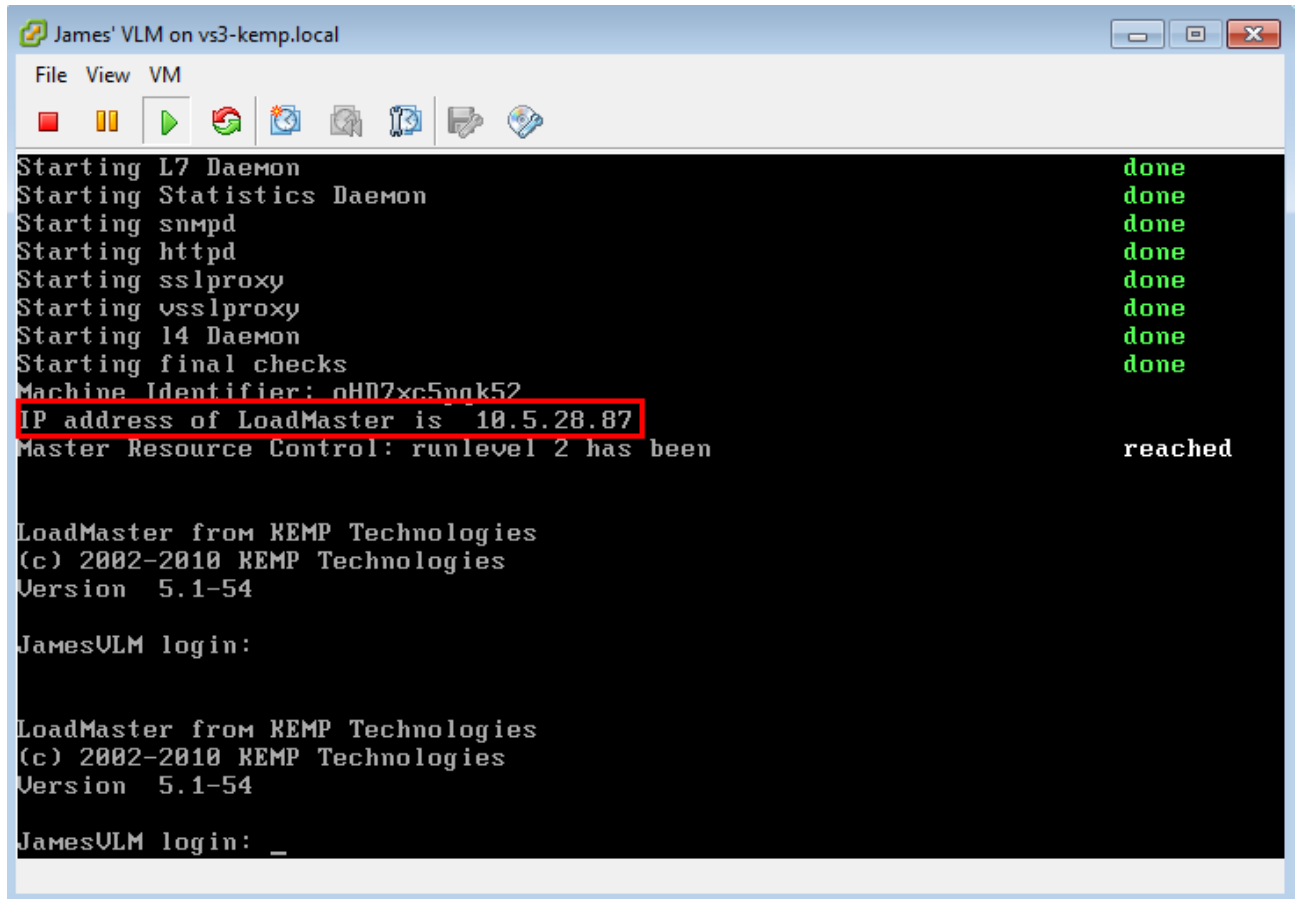
 Eth0 by default will point to the external network side of the LoadMaster. All other interfaces will default to the internal farm (server) side of the LoadMaster.

15.3 Setting up the Software

15.3.1 Console

If you do not have browser ability, got to Appendix B and C for Console Terminal operation and Command Line Interface respectively. The LoadMaster will first attempt to acquire an address via DHCP. The IP address where the LoadMaster may be reached will be displayed on the console (see below).

This is applicable to LoadMaster VLM only.



```
James' VLM on vs3-kemp.local
File View VM
Starting L7 Daemon done
Starting Statistics Daemon done
Starting snmp done
Starting http done
Starting sslproxy done
Starting vsslproxy done
Starting 14 Daemon done
Starting final checks done
Machine Identifier: oH07xc5nqk52
IP address of LoadMaster is 10.5.28.87
Master Resource Control: runlevel 2 has been reached

LoadMaster from KEMP Technologies
(c) 2002-2010 KEMP Technologies
Version 5.1-54


JamesVLM login:

LoadMaster from KEMP Technologies
(c) 2002-2010 KEMP Technologies
Version 5.1-54

JamesVLM login: _
```

15.3.2 Browser

1. Using a computer that is connected to the same network as the LoadMaster (or a PC that can reach that network), open a browser window and input <https://192.168.1.101>
2. Login with the default credentials:
Login: **bal**
Password: **1fourall**
3. You will be prompted to change the password, do this and re-authenticate using your new credentials.
4. The LoadMaster will prompt you to enter a license key.
5. At this point the WUI should reflect your license and be fully configurable. If you do not see any menu options, refresh your browser or restart the LoadMaster.

 You must have a service agreement or an evaluation product of KEMP Technologies to receive the license key for the LoadMaster. License keys are linked to the individual LoadMaster and are not transferable between LoadMaster units.

15.4 Login and License Key

If you are configuring a pair of LoadMasters in high availability mode, you must make sure that the first appliance is fully configured before the second one is connected and powered on. Setting up the HA-2 appliance is similar to setting up the HA-1 appliance.

15.5 HA Setup

HA-2 setup is as follows:

1. Login with the default credentials:

Login: **bal**

Password: **1fourall**

2. You will be asked to enter in a license key. This may have been provided to you in the box. Contact KEMP Technologies if you did not receive a license. Note: The Access Code on screen may not match the one on your license. This is normal.


3. You will be asked to assign the network side IP Address.

4. You will then be asked to enter in the address you gave the network side of the HA-1 appliance.

5. The second LoadMaster will pull data from the HA-1 appliance (the first one you configured).

6. Reboot the HA-2 unit.

If you are using a One-Armed Configuration, then it is beneficial to connect the Eth1 ports of the LoadMasters directly together via a patch cable. No further configuration is necessary.

 Both real IP's as well as the shared IP addresses may be "pinged" to test the LoadMaster cluster. At this point the Loadmaster is ready to be configured to operate with your application.


16 Fast Track

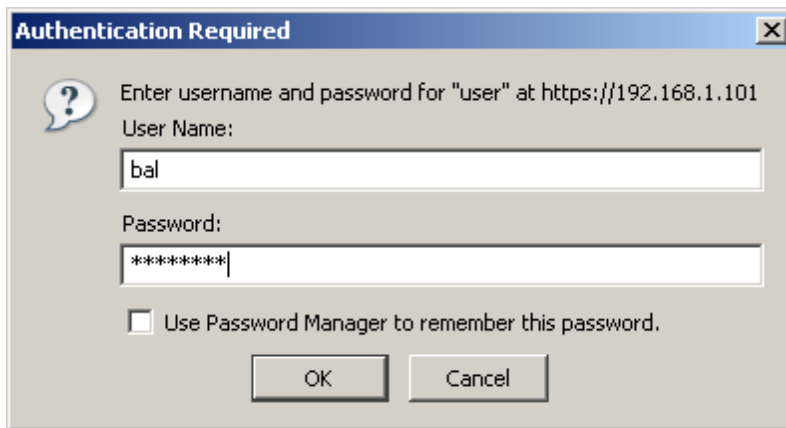
The following sections will take you through the steps required to create Virtual Services of increasing complexity. The full and detailed configuration will be found in section B following.

16.1 How to Login

Start your preferred Internet browser and enter the URL of the LoadMaster: **https://192.168.1.101**.

Then you will be asked to authenticate. The default username is ‘**bal**’ with the pre-defined password ‘**fourall**’.

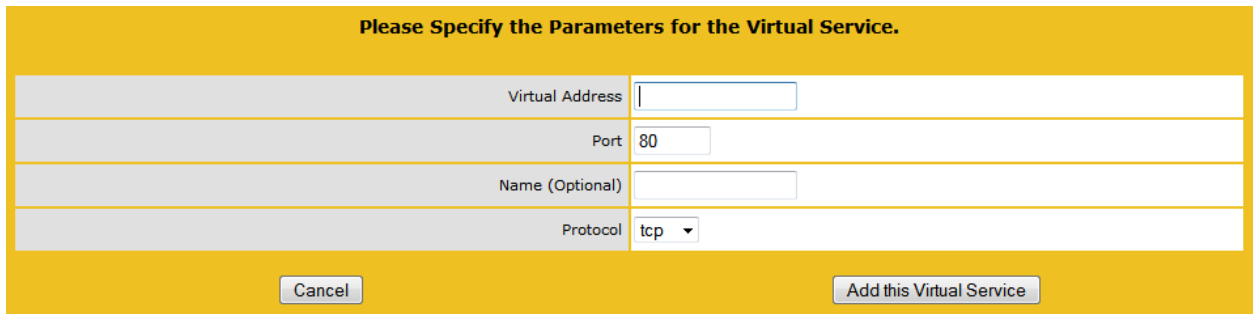
 A password for user ‘bal’ must be set in Initial Set-up of the LoadMaster. That password will be the one that will be used to connect to WUI.



16.2 Create a Simple Virtual Service

This section will take you through the steps required to create a simple Virtual Service that has two Real Servers.

To begin the process of creating a new Virtual Service, first click on the “Virtual Services” submenu link on the left, then click the “Add New” menu item. This brings up the Virtual Service parameters page and it is here that you enter the virtual IP (VIP) address of your Virtual Service, its port, the name you want to give the service and the protocol.



For example, if you gave your customer “www.a-domain.com” the IP address 192.168.1.200 then enter this as the VIP address. The port number is usually 80 for http services. The protocol may be TCP or UDP, but in the vast majority of cases TCP will be the one used.

Once you are satisfied with the choice of VIP, port and protocol click “Add This Virtual Service” to bring up the Virtual Service properties. In this example, we are not concerned with most of these values and will create a Virtual Service with no persistence, no content switching and Round Robin as the scheduling method, which are the default settings.

Properties for 192.168.201.120:80 - Operating at Layer 7

Basic Properties [Duplicate VIP](#) [Change Address](#)

[<-Back](#)

Service Name	Standard Set Nickname
Alternate Address	Set Alternate Address
Service Type	HTTP/HTTPS
Activate or Deactivate Service	<input checked="" type="checkbox"/>

Standard Options

Extra Ports	Set Extra Ports
L7 Transparency	<input checked="" type="checkbox"/>
Persistence Options	Mode: None
Scheduling Method	resource based (adaptive)
Idle Connection Timeout (Default 660)	Set Idle Timeout
Use Address for SNAT	<input type="checkbox"/>

[+ SSL Properties \(Acceleration Enabled\)](#)

[+ Advanced Properties](#)

[+ Real Servers](#)

The final action to be performed is adding Real Servers. To get to the Real Server parameters page, click the “Add New...” button in the Real Server table. Here we specify the IP address of the Real Server we wish to add, the port and forwarding method it is to use and its relative weight.

Real Servers

[Add New ...](#)

Real Server Check Parameters	HTTP Protocol	Checked Port	Set Check Port
	URL:	Set URL	
	Use HTTP/1.1:	<input type="checkbox"/>	
	HTTP Method:	HEAD	
	Custom Headers:	Show Headers	

Operation	IP Address	Port	Forwarding method	Weight	Status
Disable Modify Delete	192.168.201.62	80	nat	1000	Enabled

Enter Real Server IP address and you do not need to be concerned about the port, forwarding method and weight. Click “Add This Real Server” to finish.

The Virtual Service properties page should now display the recently added Real Server in the Real Server table. To add another Real Server, repeat the process but with a different Real Server IP address.

All changes are made in real-time, so we have now created the Virtual Service. To see a summary of Virtual Services created; click the “View/Modify Existing” link in the “Virtual Services” link submenu to the left. The Virtual Service table should now list the service we have just created.

16.3 Virtual Service Templates

Adding VS' can be a repetitive task when being performed over multiple LoadMasters and KEMP have developed a general template mechanism that will allow consistency when creating VS'. Currently we support only VS templates.

Name	Comment	Operation
Import Templates		
Template file:	<input type="text"/>	<input type="button" value="Browse..."/>
<input type="button" value="Add New Template"/>		

If there are templates installed on the machine, when a new VS is to be added, a new combo box can be seen which will show the list of templates that are available. Selecting a template will fill in the port and protocol of the VS, when the VS is created the rest of the VS will be populated with the contents of the template. Once loaded, the VS may be modified as any manually created VS.

The template can contain multiple VSs which are created atomically i.e. all VSs in the template are created or none are.



Currently templates are created only by KEMP technical staff. Contact technical support for more information on how to have your own template created.

16.4 Create a Virtual Service with Content Rules

This section will take you through the steps required to set up a Virtual Service that makes use of content switching. Content Switching means that the LoadMaster can distribute requests to a server depending on the content of the request.

16.4.1 Setting up Content Rules

On the left side of the WUI configuration screen, you'll see an option under “Rules & Checking” called content rules. Click on Content Rules to bring up all the global content rules.

Content Matching Rules

	Operation	Name	Match Type	Options	Header	Pattern
1	<input type="button" value="Modify"/> <input type="button" value="Delete"/>	RL1	RegEx	Ignore Case		rules

Header Modification Rules

	Operation	Name	Rule Type	Header	Pattern	Replacement
2	<input type="button" value="Modify"/> <input type="button" value="Delete"/>	RL5	Add Header	TEST		rules

There is also a default (catch-all) rule, which matches everything, but that is not editable.

To create a content rule, click on “Create New...”, which will bring you to the content rule screen.

Rule Name	<input type="text"/>
Rule Type	Content Matching ▾
Match Type	Regular Expression ▾
Header Field	<input type="text"/>
Match String	<input type="text"/>
Negation	<input type="checkbox"/>
Ignore Case	<input type="checkbox"/>
Include Host in URL	<input type="checkbox"/>
Include Query in URL	<input type="checkbox"/>

To create a rule that will send all URL requests that have /images/ as the root path to a group of servers, the “Match String” will be “/images/*”. The match string is a regular expression, which is a type of statement that matches or excludes based on the strings. In regular expressions “*” means “match all”.

A Regular expression is a sequence of characters. Any character, which is not a special character, will match itself. The following special characters are defined.

^	This can only be placed at the start of the string and means that the string must match at the start of the URL
\$	This can only be placed at the end of the string and means that the string must match at the end of the URL
?	This matches any single character
*	This matches zero or more characters
[This starts the set notation. This matches a SINGLE character, which is contained within a set. If the set starts with a “^”, then this will match a SINGLE character which is NOT within the set

Examples:

“[0-9]” will match any single digit.

“[^abf]” will match any character, which is not an “a”, “b” or an “f”.

“^[^a-z]” will match any first character in the URL which is not a small letter.

“/home/*.gif” match any URL which points to a “.gif” file in the “/home” directory.

“[gG][iI][fF]” match any URL which contains the string “gif” or “GIF” or “gIF” or “giF” or “GiF” etc.

Note: Given an input URL such as “/home/cgi-bin/XXX.cmd?value=hello”, the end of the string used in matching is terminated by the “?” character i.e. a postfix string of “cmd” will match this URL, while a postfix of “hello” will not.

You have the option to Include Host in URL (such as whether to match support.kemptechnologies.com).

Another option is Negation. Without negation, all requests that include “/images/” would match this rule. With negation, all requests except “/images/” would match this rule.

Include query would include everything after the “?” in a URL, which is the URL query. An example would be http://support.kemptechnologies.com/images/imagid.jsp?item=1, where the query could be “item=1”.

Click on “Commit” and the rule will be added, but will not affect any Virtual Service. Once the rules have been added, they need to be applied to Real Servers within individual Virtual Services.

Note: This syntax is different to PCRE syntax

16.4.2 Configuring Virtual Services for Content Switching

The first step in configuring a Virtual Service for content switching is to make sure that the only persistence option chosen is either “None” or “SRC” (the Layer 4 persistence option).

With that set, there should be an option to enable Content Switching under “Advanced Properties”.

Advanced Properties

Content Switching	Disabled <input type="button" value="Enable"/>
HTTP Header Modifications	<input type="button" value="Show Header Rules"/>
Enable Caching	<input type="checkbox"/>
Enable Compression	<input type="checkbox"/>
Detect Malicious Requests	<input type="checkbox"/>
Not Available Server	<input type="text"/> <input type="button" value="Set Server Address"/>
Not Available Redirection Handling	Error Code: <input type="text"/>
	Redirect URL: <input type="text"/> <input type="button" value="Set Redirect URL"/>
Default Gateway	<input type="text"/> <input type="button" value="Set Default Address"/>

Once you click enable, you'll see that any Real Servers have a new column on the right side.

Real Servers for this Virtual Service

Operation			IP Address	Port	Forwarding method	Weight	Status	Rules
<input type="button" value="Disable"/>	<input type="button" value="Modify"/>	<input type="button" value="Delete"/>	10.0.0.1	80	nat	1000	Enabled	None

Since you've just enabled Content Switching, no rules are active. As an example, take four web servers configured on a Virtual Service. These servers would be on 192.168.1.100, 101, 102, and 103. The 100 and 101 servers would be general content servers, and 102 and 103 would be the images servers.

Click on the “None” button for each server. You'll have the opportunity to add multiple rules to each server, but in this example, you'll only add one rule per server. The rule just created in the previous section will be added to 102 and 103, and the default rule will be added to 100 and 101.

Real Servers for this Virtual Service

Operation			IP Address	Port	Forwarding method	Weight	Status	Rules
<input type="button" value="Disable"/>	<input type="button" value="Modify"/>	<input type="button" value="Delete"/>	10.0.0.1	80	nat	1000	Enabled	1

You'll then have four servers, each with one rule in place. You should be then able to test your Virtual Service configuration.



Note: In order to use content switching you will need to disable HTTP Keepalives on your Real Servers. Please review RFC 2616 to understand the impact of alerting this parameter.

16.5 Create an SSL accelerated Virtual Service

This section will explain how to create a Virtual Service with SSL Acceleration activated.

SSL Acceleration transfers the processing of SSL from the Real Servers to the LoadMaster, meaning that only one certificate is required per Virtual Service.



When SSL Acceleration is enabled, communication from the LoadMaster to the Real Servers is *unencrypted*.

16.5.1 Adding an SSL Virtual Service

The process for adding an SSL-enabled Virtual Service is the same for a regular Virtual Service. First, add the Virtual Service. Under the Virtual Services menu on the left, select “Add New”. You'll be prompted to put the Virtual Address, port, service name and protocol.

Please Specify the Parameters for the Virtual Service.

Virtual Address	<input type="text"/>
Port	<input type="text" value="80"/>
Name (Optional)	<input type="text"/>
Protocol	<input type="text" value="tcp"/>

Cancel
Add this Virtual Service

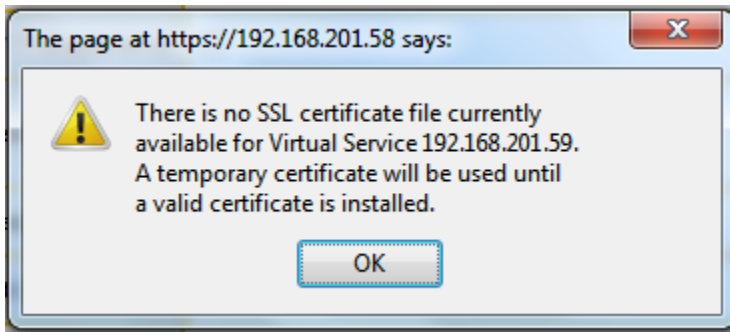
The port defaults to port 80, which is the standard HTTP port. Since you're setting up an SSL-enabled Virtual Service, change the port to 443, which is the default HTTPS port. Leave the protocol as TCP, and click “Add this Virtual Service”.

You'll then be presented with the Virtual Service properties screen. Among the various sections in this screen is the “SSL Options” (Figure 3).

SSL Properties

SSL Acceleration	Enabled: <input checked="" type="checkbox"/> Reencrypt: <input type="checkbox"/>
Certificates	Self Signed Certificate in use: <input type="button" value="Add New"/> <input type="button" value="Add Intermediate Cert"/>
Rewrite Rules	<input type="text" value="None"/>
Client Certificates	<input type="text" value="No Client Certificates required"/>

To enable SSL for this Virtual Service, simply select the “Enabled” box for SSL Acceleration. This will immediately pop up a dialog screen that a temporary certificate will be used for the service.



As soon as SSL is enabled, the LoadMaster will install a self-signed certificate for the Virtual Service. You can add Real Servers to this SSL Virtual Service just as you would do for any other Virtual Service. When adding Real Servers, make sure to add them on port 80 (or whatever port that the non-SSL service is running on), and not port 443.

Real Server Address	<input type="text"/>
Port	80
Forwarding method	nat
Weight	1000

16.5.2 Adding an SSL Certificate

If you have a CA certificate you would like to use with a SSL-enabled Virtual Service, or have a custom self-signed certificate that you'd like to use, you can add it to the Virtual Service through the WUI.

There is a button to add an SSL certificate in the properties screen under the SSL properties section.

SSL Properties

SSL Acceleration	Enabled: <input checked="" type="checkbox"/> Reencrypt: <input type="checkbox"/>
Certificates	Self Signed Certificate in use: <input type="button" value="Add New"/> <input type="button" value="Add Intermediate Cert"/>
Rewrite Rules	None
Client Certificates	No Client Certificates required

Also, in the View/Modify Services listing of the Virtual Services there is an Add New button in the Certificates column.

	Virtual IP Address	Prot	Name	Layer	Certificate Installed	Scheduler	Status	Real Servers	
1	[3ffe:1900:4545::3:200:f8f1]:80	tcp	Test03	L7		round robin	Down		<input type="button" value="Modify"/> <input type="button" value="Delete"/>
2	192.168.201.59:80	tcp	Test01	L7		round robin	Up	192.168.201.60 192.168.201.65	<input type="button" value="Modify"/> <input type="button" value="Delete"/>
3	192.168.201.61:443	tcp	Test02-SSL	L7	<input type="button" value="Add New"/>	round robin	Up	192.168.201.60	<input type="button" value="Modify"/> <input type="button" value="Delete"/>
4	192.168.201.62:3389	tcp	Terminal Svcs	L7		round robin	Down		<input type="button" value="Modify"/> <input type="button" value="Delete"/>

Either route brings you to the same screen, the screen to input the certificate information.

At this point there are two options.

Add Intermediate

Clicking the button will allow you to add an intermediate certificate as a temporary measure. Paste in the certificate data, name the certificate and click Add Certificate button.

Import Certificate

Name the certificate that you want to create and click the Import Certificate button. It will bring up the screen below. Here you have the option to locate the certificate on your PC and paste the data into the screen, or, Browse for the certificate on your PC and click Open. You will need to input the Passphrase (password) that the certificate was created with.

A certificate file with both components, or the certificate file by itself, is typically a .pem or .crt file. If the key is separate, it typically has the .key extension.

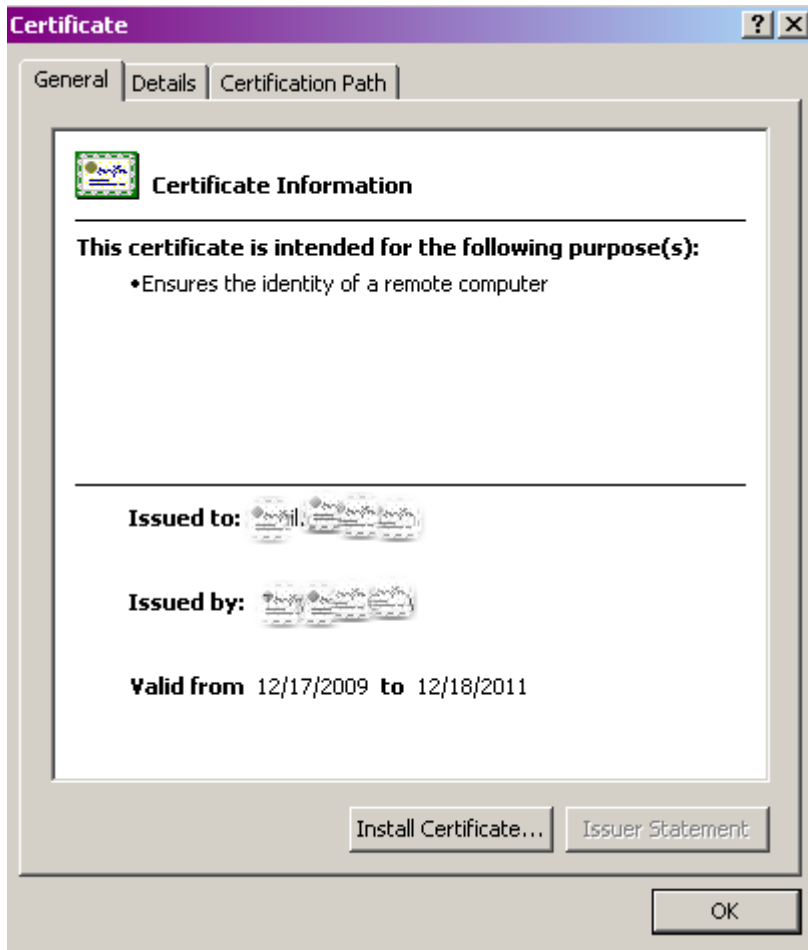
To add this certificate to the Virtual Service, copy the portion of the certificate that begins and ends with a “-----BEGIN CERTIFICATE-----” and “-----END CERTIFICATE-----” statement.

In the private key section, enter the portion of the certificate file that begins and ends with “-----BEGIN RSA PRIVATE KEY-----” and “-----END RSA PRIVATE KEY-----”.

Some private keys are protected by a passphrase. If that is the case with your certificate file, input the password in the third and final field (Figure 12). Otherwise, leave the field blank and click “Submit”.

The certificate will then be installed for the Virtual Service, and you'll see the confirmation.

It helps to see what a host certificate looks like in order to determine which parts are pasted into which field. A host certificate may consist of one or two files. If it's one file, then the certificate contains two



16.5.4 Intermediate Certificates

Some certificates issued by Certificate Authorities require a third certificate, often referred to as an intermediate certificate, or third-party certificate. This additional certificate provides a chain path from the CA to the certificate issued to your site.

While some CAs use intermediate certificates, others do not. Check with your CA to determine if one is needed.

If you've installed a CA certificate, and you still get an SSL error when browsing the Virtual Service, it's likely that you need to install an intermediate certificate.

16.5.5 Installing Intermediate Certificates

Installing an intermediate certificate is simple to do through the WUI. First, obtain the intermediate certificate from the CA. This can usually be found on their web site, and is usually in a text window for cut and paste.

In the left side of the WUI, select “3rd Party Certs”. This will bring up a list of installed 3rd party certificates, if any. To add, click “add new”. Past the contents of the intermediate certificate, which should begin and end with “-----BEGIN CERTIFICATE-----” and “-----END CERTIFICATE-----”.

You must also give it a file name for the LoadMaster to save the certificate (Figure 16). It's helpful to name the certificate file after the CA that assigned the certificate.

Copy and Paste the entire body of the Intermediate Certificate below:

Intermediate Certificate:

Desired File Name
(i.e. - VeriSignCert.pem or Thwarte.cer):

Cancel
Add Certificate

You do not need to associate these third party/intermediate certificates with any Virtual Service certificates. The LoadMaster will automatically build the required certificate chain.

Also, you only need one intermediate certificate per CA. If you have several certificates installed from VeriSign, for instance, you only need to install the VeriSign intermediate certificate once.

16.5.6 IIS Certificates

Migrating SSL from Microsoft Internet Information Server to LoadMaster

When putting a LoadMaster in a situation where a Microsoft IIS server was previously performing SSL, you have the option to import your IIS certificate into the LoadMaster. You can migrate this SSL certificate from Microsoft Internet Information Server (IIS) to the LoadMaster by completing two simple tasks. The first task is to export the SSL certificate from the IIS using Microsoft export tools; you want to make sure to export the certificate and private key as Personal Information Exchange File (PFX). The second step is to import the PFX file into LoadMaster using the LoadMaster WUI. To start the import process on LoadMaster simply click the “Add New” button in the SSL enabled Virtual Service. Set the “An IIS Certificate:” file to the corresponding PFX file and click “Submit”.

16.5.7 Re-encrypt SSL

With SSL acceleration, the SSL session is terminated at the LoadMaster, and sent to the Real Servers unencrypted. In some security situations, it may be necessary to encrypt the connection between the LoadMaster and Real Servers. This can be done with reverse SSL.

With reverse SSL, the SSL session is first terminated at the LoadMaster. persistence and other Layer 7 functionality can then be performed. After that, the traffic is re-encrypted in a new SSL session between the LoadMaster and the Real Server.

This is turned on by a single option in the properties screen of a Virtual Service in the SSL section.

SSL Properties

SSL Acceleration Enabled: Reencrypt:

16.5.8 Certificate Signing Request

You can create a CSR for submission directly to your signing authority of choice. Using the WUI navigate to Certificates -> Generate CSR fill in the information and create the CSR and private key.



Store the private key in a vault. The private key will be required once your authority creates your certificate.

16.5.9 Backup/Restore Certificates

LoadMaster supports exporting of ALL certificate information. This includes private key, host and intermediate certificates. The export file is designed to be used for import into another LoadMaster and is encrypted. Export and import can be completed using the WUI at Certificates -> Backup/Restore Certs. Please make sure to note the pass phrase used to create the export, it will be required to complete the import.

You can selectively resort only Virtual Service certificates including private keys, intermediate certificates or both.

16.5.10 SSL Ciphers

Following is a list of the ciphers supported by the LoadMaster:

- ADH-AES256-SHA:(TLSv1 256 bits)
- DHE-RSA-AES256-SHA: (TLSv1 256 bits)
- DHE-DSS-AES256-SHA: (TLSv1 256 bits)
- AES256-SHA: (TLSv1 256 bits)
- ADH-DES-CBC3-SHA:(TLSv1 168 bits)
- EDH-RSA-DES-CBC3-SHA: (SSLv3 168 bits)
- EDH-DSS-DES-CBC3-SHA: (TLSv1 168 bits)
- DES-CBC3-SHA: (SSLv3 168 bits)
- ADH-RC4-MD5: (SSLv3 128 bits)
- IDEA-CBC-SHA: (SSLv3 128 bits)
- RC4-SHA: (SSLv3 128 bits)
- RC4-MD5: (SSLv3 128 bits)
- ADH-AES128-SHA: (TLSv1 128 bits)
- DHE-RSA-AES128-SHA: (SSLv3 128 bits)
- DHE-DSS-AES128-SHA: (SSLv3 128 bits)
- AES128-SHA: (SSLv3 128 bits)

16.5.11 Web User Interface Root Certificate Installation

By default LoadMaster uses a self-signed certificate to ensure secure administrative access to the Web User Interface. However most modern browsers will throw a warning when such a certificate is used. In order to eliminate this warning you can install the LoadMaster certificate by clicking the “Download LM Root Cert” button. This will download the certificate file that can be installed on your browser so that the security warning can be avoided

16.6 Load Balancing Microsoft Terminal Services

Setting up a Virtual Service to balance Microsoft Terminal Servers is very similar to setting up any other Virtual Service. The system tries to automatically detect the type of the Virtual Service based on the port of the Virtual Service.

Once a port number of 3389 is entered, the system automatically chooses Remote Terminal as a service type.

If the Virtual Service uses port 80, 8080 or 443, then it will be configured as a HTTP/HTTPS service. If it uses port 3389 then it will be configured for Terminal services. If the port is set to anything else, the service will be configured as “Generic”.



The type of the service can always be changed manually by using the Mode selection option.

This configuration is intended to allow the LoadMaster to balance Microsoft Terminal Services across multiple servers. Upon first connection, a server is allocated using the standard scheduling methods, i.e. Round Robin, Least Connection, Adaptive, etc.

If a user disconnects from his/her session without logging out, it is preferable to maintain persistence with the server that he/she originally connected to. This allows that user to come back to the screen they were working on, with all the same windows open and applications running where they had left off.

This is where the Persistence Mode of Terminal Service comes in. If this persistence mode is enabled, when a user reconnects, the LoadMaster will try to connect the session to the same server. It does this in one of three ways:

Properties for 192.168.201.62:3389 - Operating at Layer 7

<-Back
Basic Properties
Duplicate VIP
Change Address

Service Name	Terminal Svcs Set Nickname
Alternate Address	<input type="text"/> Set Alternate Address
Service Type	Remote Terminal ▾
Activate or Deactivate Service	<input checked="" type="checkbox"/>

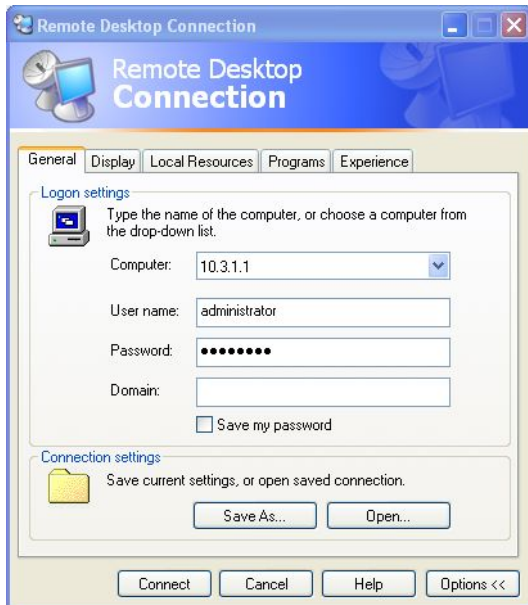
Standard Options

Extra Ports	<input type="text"/> Set Extra Ports
L7 Transparency	<input checked="" type="checkbox"/>
Persistence Options	Mode: Terminal Service or Source IP ▾ Timeout: 1 Hour ▾
Scheduling Method	round robin ▾
Idle Connection Timeout (Default 660)	<input type="text"/> Set Idle Timeout
Use Address for SNAT	<input type="checkbox"/>
Service Specific Access Control	Access Control

If the terminal servers support a Session Directory, the LoadMaster will use the "routing token" supplied by the Session Directory to determine the correct host to connect to. The LoadMaster persistency timeout value is irrelevant here - it is a feature of the Session Directory.

Note: The switch "IP address redirection" in the Session Directory configuration MUST be UNCHECKED for this to work.

Using Session Directory with LoadMaster is optional, in terms of persistence. If the Client pre-populates the username and password fields (see figure x) in the initial request, then this value is stored on the LoadMaster. As long as these fields are still populated upon reconnect, the LoadMaster will look up the name and reconnect to the same server as the original connection. The persistence timeout is used to limit the time the information is kept on the LoadMaster.



Username and password have been pre-populated

If using "Terminal-Service or source IP" mode, then if neither of these two modes succeeds, then the source IP address will be used for persistency.

16.7 Configuring Port Following

When using “shopping cart” like services where a user selects items and adds them to a list, any of the previous types of persistency can be used. When the user then decides to pay for the items, this is normally performed using a secure SSL (https) service. When port following is turned on, the Real Server where the “shopping cart” connection is active will be selected for the SSL session. This selection will only occur when a connection is still open from the same client (as determined by the source IP address), and if the SSL service has the same IP address as the “shopping cart” service.

For example, if a connection is made to the HTTP service of `www.somewebsite.com`, and then a new SSL connection is made to the same address, then the SSL session will be directed to the same Real Server as the original HTTP service.



This only works correctly if both services have the same set of Real Servers. Both Virtual Services should have the same Layer 7 persistence.

16.7.1 Create the Virtual Service for HTTP

1. From Main Menu pane, select Virtual Services.
2. Under Virtual Services, click the “ADD New” button to start the Add Virtual Service.
3. For the Virtual Address, enter the IP and port 80.
4. Click the “Add this Virtual Service” button to get to the “Properties for 192.168.1.50:80 - Operating at Layer 4” screen.
5. Enter service nickname ‘http’ in the textbox for “Service Nickname”, then click the “Set Nickname” button.
6. In order to create the 1st Real Server, click the “Add New” button under REAL Server for this Virtual Service, option is lower on the same screen.

7. Enter the IP for “Real Server Address” and then click the “Add This Real Server” button. Leave “Port” number as 80.
8. In order to create the 2nd Real Server, click the “Add New” button under REAL Server for this Virtual Service, option is lower on the same screen.
9. Enter the IP for “Real Server Address” and then click “Add This Real Server” button. Leave “Port” number as 80.
10. Select "Super HTTP as the persistence mode
11. Click “View/Modify Existing” option under Virtual Services tab in the Main Menu.
12. Check that the Virtual Service appears with the correct Virtual IP Address, Port number and Real Servers and Status is Up in the “Status” column.

16.7.2 Create the Virtual Service for HTTPS/SSL Offloading

1. From Main Menu pane, select Virtual Services.
2. Under Virtual Services, click the “ADD New” button to start the Add Virtual Service.
3. For the Virtual Address, enter IP And change the “Port” to 443 from 80.
4. Click the “Add this Virtual Service” button to get to the “Properties for 192.168.1.50:443 - Operating at Layer 4” screen.
5. Enter service nickname ‘https’ in the textbox for “Service Nickname”, then click the “Set Nickname” button.
6. Put a check mark on checkbox labeled “Enable” for SSL Acceleration in the SSL Properties section.
7. Click “OK” if warning message appears as “There is no SSL certificate file currently available for Virtual Service 192.168.1.50. A temporary certificate will be used until a valid certificate is installed”. This message is simply a warning.
8. In order to create the 1st Real Server, click the “Add New” button under REAL Server for this Virtual Service, option is lower on the same screen.
9. Enter the IP for “Real Server Address” and then click the “Add This Real Server” button. Leave “Port” number as 80.
10. In order to create the 2nd Real Server, click the “Add New” button under REAL Server for this Virtual Service, option is lower on the same screen.
11. Enter the IP for “Real Server Address” and then click “Add This Real Server” button. Leave “Port” number as 80.
12. Select "Super HTTP as the persistence mode
13. Click “View/Modify Existing” option under Virtual Services tab in the Main Menu.
14. Check that the Virtual Service appears with the correct Virtual IP Address, Port number and Real Servers and Status is Up in “Status” column.

16.7.3 Configure Port Following for HTTPS VS

1. On the Main Menu pane, select the Virtual Services menu.
2. Go to View/Modify Existing option.
3. Click the “Modify” button for the Virtual Server with port 443.
4. Select the “Port Following” dropdown in the Advanced Properties pane. Select the port 80 VS
5. Wait 10 seconds, or uncheck and check the “Activate or Deactivate Service” checkbox in the basic properties pane for immediate activation.

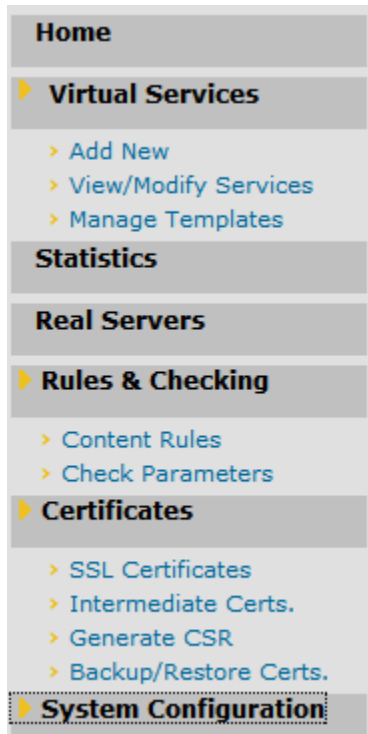
16.7.4 Configure Port Following for HTTP VS

1. On the Main Menu pane, select the Virtual Services menu.
2. Go to View/Modify Existing option.
3. Click the “Modify” button for the Virtual Server with port 80.
4. Select the “Port Following” dropdown in the Advanced Properties pane. Select the port 443 VS
5. Wait 10 seconds, or uncheck and check the “Activate or Deactivate Service” checkbox in the basic properties pane for immediate activation.

17 Full Web User Interface (WUI) Menu Tree



This section is Quick Reference that will help you find your way through the menu structure of the LoadMaster WUI. Some of the diagrams shown in the previous section, Fast Track, will be the same and have not been duplicated here.

The LoadMaster menu consists of a series of collapsible submenus on the left of the screen.



17.1 Home


An introduction page showing the vital information of the LoadMaster.

IP address	192.168.201.58
Machine Identifier	Uf7hqm21CS4a (Instance 472654)
Boot Time	Thu Jul 21 15:02:14 UTC 2011
LoadMaster Version	6.0-5.20110705-1029
License	Activation date: July 21 2011 Licensed until: Unlimited
CPU Load	0% 
TPS	Total 0 (SSL 0)
NetLoad	Mbits/sec
eth0	0.0 

While most of the information on this is self-explanatory, following are some comments and notes:

CPU Load: Applicable to the CPU of the LoadMaster appliances and to the CPU running a VLM.

Net Load: shown for each configured interface.

 The CPU Load and Net Load data are updated every 5 seconds.

17.2 Virtual Services

A list of Virtual Services on the LoadMaster, summarizing the properties of each and giving the options to modify or delete services, or create a new service.

	Virtual IP Address	Prot	Name	Layer	Certificate Installed	Scheduler	Status	Real Servers	
1	[3ffe:1900:4545::3:200:f8f1]:80	tcp	Test03	L7		adaptive	Up	192.168.201.65:80	<input type="button" value="Modify"/> <input type="button" value="Delete"/>
2	192.168.201.59:80	tcp	Test01	L7		round robin	Up	192.168.201.60 192.168.201.65	<input type="button" value="Modify"/> <input type="button" value="Delete"/>
3	192.168.201.61:443	tcp	Test02-SSL	L7	<input type="button" value="Add New"/>	round robin	Up	192.168.201.60	<input type="button" value="Modify"/> <input type="button" value="Delete"/>
4	192.168.201.62:3389	tcp	Terminal Svcs	L7		round robin	Up	192.168.201.60	<input type="button" value="Modify"/> <input type="button" value="Delete"/>



CAUTION –Delete is permanent, there is no UNDO feature. Use with care.

17.2.1 Add New VS

Here the Virtual IP (VIP) address, port and protocol and name are defined. The VIP address, name and port are manually entered into the text fields and the protocol is selected from the drop-down list.



For the LoadMaster *Exchange* appliance there is a maximum limit of thirteen (13) Virtual Services that may be configured.

17.2.2 View/Modify Existing VS (HTTP Service)

Each configured Virtual Service may be changed by clicking the MODIFY button or deleted by clicking the DELETE button. Here the properties of the Virtual Services are shown, and may be modified.

The Virtual Service status may be one of the following:



Up

Up – At least one Real Server is available.



Down

Down – No Real Servers are available.



Sorry

Sorry – All Real Servers are down and traffic is routed to a separately configured server, not part of the Real Server set, with no checking.



Disabled

Disabled – The service has been administratively disabled.



Redirect

Redirect – A fixed redirect response has been configured.



Fail Message

Fail Message – A fixed error message has been configured.



Unchecked

Unchecked – The User has disabled checking of the Real Servers. All RS are accessed and presumed UP.

The screen below shows a screen for a Virtual Service. It is composed of five component sections:

Properties for 192.168.201.121:443 - Operating at Layer 7

Basic Properties

[<Back](#) [Duplicate VIP](#) [Change Address](#)

Service Name	HTTPS	Set Nickname
Alternate Address		Set Alternate Address
Service Type	HTTP/HTTPS	
Activate or Deactivate Service	<input checked="" type="checkbox"/>	


+ **Standard Options**

+ **SSL Properties (Acceleration Enabled)**

+ **Advanced Properties**

+ **Real Servers**

- + **Basic properties** - where the usual and most common attributes are set.
- + **Standard Options** – the most widely used features of a Virtual Service.
- + **SSL properties** – if SSL acceleration is being used, it will show Acceleration Enabled and this section of the screen will be used to configure the functions.
- + **Advanced properties** – the additional features for a Virtual Service.
- + **Real Servers** – where Real Servers are assigned to a VS.

 Depending upon the service type, and enabled or disabled features, only specific fields and options may show in the WUI. The screen shots in this document may not represent every possible configuration.

17.3 Basic Properties Screen

The fields in this screen are:

17.3.1 Service Name

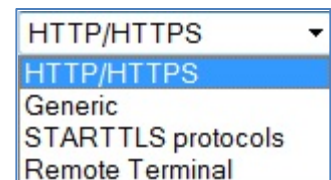
This text field allows you to assign a nickname to the Virtual Service being created, or change an existing one.

17.3.2 Alternate Address

This is where, if so desired, you would specify a secondary address in either IPv6 or IPv4 format.

17.3.3 Service Type

Setting this controls the options displayed for the Virtual Service. It's important to make sure the Service Type is set according to the type of application you are load balancing.



17.3.4 Activate or Deactivate Service

This checkbox gives you the option to activate or deactivate a Virtual Service. The default is checked - active.

17.4 Standard Options Screen

Standard Options	
Extra Ports	<input type="text"/> <input type="button" value="Set Extra Ports"/>
L7 Transparency	<input type="checkbox"/>
Persistence Options	Mode: <input type="text" value="Super HTTP and Source IP"/> Timeout: <input type="text" value="6 Minutes"/>
Scheduling Method	<input type="text" value="weighted least connection"/>
Idle Connection Timeout (Default 660)	<input type="text"/> <input type="button" value="Set Idle Timeout"/>
Use Address for SNAT	<input type="checkbox"/>

17.4.1 Extra Ports

You may specify a range of ports, sequential or otherwise, starting with the base port already configured for the Virtual Service. The port numbers are inputted to the field and separated with a space, and the maximum range is 1,024 ports. Therefore, if the base port is 80, then the maximum value in this field is 1,104.

17.4.2 Force L7

If visible, the Force L7 should be checked (default). If it is unchecked it will force the Virtual Service to Layer 4.

17.4.3 L7 Transparency

Enabling this option makes the Virtual Service transparent (NO NAT). However, If the client resides on the same subnet as the Virtual IP and Real Servers the Virtual Services will automatically NAT (enable non-transparency) the source IP.

17.4.4 Persistence Options

Persistence is setup on a per Virtual Service basis. This section allows you to select whether persistence is enabled for this service, to set the type of persistence and the persistence timeout value.

If persistence is enabled it means that a client connection to a particular Real Server via the LoadMaster is persistent, in other words the same client will subsequently connect to the same Real Server. The timeout value determines for how long this particular connection is remembered.

- ⚠ If you have content switching enabled, you will still see all Layer 7 options available in the persistence menu. If you do select a Layer 7 option (any option other than NONE or SRC), then content switching will automatically be disabled, and the rule list applied to Real Servers will be lost.

The pull-down list gives you the option to select the type of persistence. These are:

Source IP Address

The source IP address (of the requesting client) is used as the key for persistency in this case.

Super HTTP

Super HTTP is the recommended method for achieving persistence for HTTP and HTTPS services with the LoadMaster. It functions by creating a unique fingerprint of the client browser and uses that fingerprint to preserve connectivity to the correct Real Server. The fingerprint is based on the combined values of the User-Agent field and, if present, the Authorization header. Connections with the same header combination will be sent back to the same Real Server.

Server Cookie

The LoadMaster checks the value of a specially set cookie in the HTTP header. Connections with the same cookie will go to the same Real Server.

Server Cookie or Source IP

If cookie persistence fails, it reverts to source-based persistence.

Active Cookie

The LoadMaster automatically sets the special cookie.

Active Cookie or Source IP

If active cookie persistence fails, it reverts to source-based persistence.

Hash All Cookies

The Hash All Cookies method creates a hash of the values of all cookies in the HTTP stream. Cookies with the same value will be sent to the same server for each request. If the values change, then the connection will be treated as a new connection, and the client will be allocated to a server according to the load balancing algorithm.

Hash All Cookies or Source IP

Hash All Cookies or Source IP is identical to Hash All Cookies, with the additional feature that it will fall back to Source IP persistence in the event no cookies are in the HTTP string.

Super HTTP and Source IP Address

This is the same as super HTTP BUT it also appends the source IP address to the string, thus improving the distribution of the resulting HASH.

URL Hash

With URL Hash persistence, the LoadMaster will send requests with the same URL to the same server.

HTTP Host Header

With HTTP Host Header persistence, the LoadMaster will send all requests that contain the same value in the HTTP Host: header to the same server.

Hash of HTTP Query Item

This method operates in exactly the same manner as Server Persistence, except that the named item being inspected is a Query Item in the Query String of the URL. All queries with the same Query Item value will be sent to the same server.

Selected Header

With Selected Header persistence, the LoadMaster will send all requests that contain the same value in the specified header to the same server.

SSL Session

Each session over SSL has its own session id. You can persist on it. BUT in older versions of MS, the session id was changed every 2 minutes, which made it pretty useless. Now they don't change it so often, but it is still difficult to work with.

17.4.5 Scheduling Methods

This section allows you to select the method by which the LoadMaster will select a Real Server, for this particular service. The scheduling methods are as follows:

Round Robin

Round Robin causes the LoadMaster to assign Real Servers to a session in order, i.e. the first session connects to Real Server 1, the second to Real Server 2 etc. There is no bias in the way the Real Servers are assigned.

Weighted Round Robin

This method uses the weight property of the Real Servers to determine which Real Servers get preference. The higher the weight a Real Server has, the higher the proportion of connections it will receive.

Least Connection

With this method, the current Real Server with the fewest open connections is assigned to the session.

Weighted Least Connection

As with Least Connection, but with a bias relative to the weight.

Resource Based (Adaptive)

Adaptive scheduling means that the load on the Real Servers is periodically monitored and that packets are distributed such that load will be approximately equal for all machines. More details can be found in the section covering scheduling methods.

Fixed Weighting

All traffic goes to highest weight RS that is available. Real Servers should be weighted at the time they are create and no two RS' should have same weight otherwise led unpredictable results may occur.

Weighted Response Time

Every 15 seconds the LoadMaster measures the time it takes for a response to arrive for a healthcheck probe and uses this time to adjust the weights of the RS's accordingly. I.E. a faster response time relative to the other RS's = a higher weight = more traffic sent to that server.

Source IP Hash

Instead of using the weights or doing round robin, a hash of the source IP is generated and used to find the correct real server. This means that the real server is always the same from the same host.

You don't need any source IP persistence.



This MAY cause real server imbalance.

17.4.6 SSL Properties Screen

SSL Properties	
SSL Acceleration	Enabled: <input checked="" type="checkbox"/> Reencrypt: <input type="checkbox"/>
Certificates	Self Signed Certificate in use: <input type="button" value="Add New"/> <input type="button" value="Add Intermediate Cert"/>
Rewrite Rules	<input type="text" value="None"/>
Client Certificates	<input type="text" value="No Client Certificates required"/>

This checkbox appears when the criteria for SSL Acceleration have been met, and serves to activate SSL Acceleration. If there is no certificate for the Virtual Service, you will be prompted to install a certificate. To download a certificate, enter the remote host where the certificate is located and your username and password for this host. Then enter the filename of the certificate and the private key, and click "Get File" to install them.

Certificates

You may add a new certificate or add an intermediate certificate chain to the LoadMaster.

Rewrite Rules

When the Real Server rejects a request with an HTTP redirect, the resulting Location URL may need to be converted to specify HTTPS instead of HTTP (and vice-versa).

Client Certificates

No Client Certificates required: enables the LoadMaster to accept https requests from any client. This is the recommended option.

Client Certificates required: requires that all clients forwarding a https request must present a valid client certificate.

Client Certificates and add Headers: requires that all clients forwarding a https request must present a valid client certificate. The LoadMaster also passes information about the certificate to the application by adding headers. For more information regarding the headers that are added please refer to **Appendix G: Headers Added by LoadMaster When ‘Client Certificates and Add Headers’ Option is Selected.**

- ⚠ This option should not be changed from the default of **No Client Certificates required**. You would only change from the default option if you are sure that all clients that access this service have valid client certificates.

17.4.7 Advanced Properties Screen

Advanced Properties	
Content Switching	Disabled
HTTP Header Modifications	Show Header Rules
Enable Caching	<input checked="" type="checkbox"/> Maximum Cache usage No Limit
Enable Compression	<input type="checkbox"/>
Detect Malicious Requests	<input type="checkbox"/>
Add Header to Request	<input type="text"/> : <input type="text"/> Set Header
"Sorry" Server	<input type="text"/> Set Server Address
Not Available Redirection Handling	Error Code: <input type="text"/> Redirect URL: <input type="text"/> Set Redirect URL
Add a Port 80 Redirector VS	Redirection URL: <input type="text"/> https://%h%s Add HTTP Redirector
Default Gateway	<input type="text"/> Set Default Gateway
Alternate Source Addresses	<input type="text"/> Set Alternate Source Addresses
Service Specific Access Control	Access Control

Content Switching

Enable Rule based Content Switching on this Virtual Service. Once enabled, rules must be assigned to the various Real Servers. Rules can be attached to Real Server by selecting the “None” button located next the Real Server. Once rules are attached to a Real Server the “None” button will display the count of rules attached.

HTTP Header Mods - Rule Precedence

The order in which Content Switching rules are matched are specified here. This option only appears when Content Switching is enabled. This contains a summary list of rules assigned to the Virtual Service in question.

Real Servers for this Virtual Service								
Operation			IP Address	Port	Forwarding method	Weight	Status	Rules
Disable	Modify	Delete	10.0.0.3	80	nat	1000	Enabled	4
Disable	Modify	Delete	10.0.0.4	80	nat	1000	Enabled	None


This shows the Real Servers configured and whether any rules have been assigned to them. In this example the first RS has two rules and by clicking the button marked ‘2’ brings up the screen below.

Operation	Name	Match Type	Options	Header	Pattern
	RL1	RegEx	Ignore Case		rules
Promote	RL4	postfix	Ignore Case		kemp
Promote	RL6	RegEx	Ignore Case		tech
	default				

This screen shows the rules that are assigned to this Real Server and the order in which they apply. To re-order the rules they have to be deleted from the RS and then added back in the required processing order. A rule may be promoted in the order of precedence by clicking its corresponding “Promote” button.

Enable Caching

This option enables caching of static content saving valuable Real Server processing power and bandwidth. Caching can be enabled per HTTP and off loaded HTTPS Virtual Services.

-  Types of files that can be cached may be defined in AFE configuration under the Systems Configuration, Miscellaneous options menu.

Maximum Cache Usage

This option limits the size of the cache memory per Virtual Service. For example, two Virtual Service each running with a limit of 50% will use 100% of the cache store. The default is “No Limit”. It is recommended to limit the cache size to prevent unequal use of the cache store. Ensure that the cache maximum usage is adjusted so that each Virtual Service has a percentage of cache to use. If there is not remaining space to be allocated for a cache enabled Virtual Service, that service will not cache content.

Enable Compression

Files sent from LoadMaster are compressed with Gzip.



If compression is enabled without caching, LoadMaster performance may suffer.



Types of files that can be compressed may be defined in AFE configuration under the Systems Configuration, Miscellaneous options menu.

Detect Malicious Requests

The Intrusion Prevention System (IPS) service will provide in-line protection of Real Server(s) by providing real-time mitigation of attacks and isolation of Real Server(s). Intrusion prevention is based on the industry standard SNORT database and provides real-time intrusion alerting.

Checking the “Detect Malicious Requests” checkbox enables the IPS per HTTP and off loaded HTTPS Virtual Services. There are two options for handling of requests that match a SNORT rule. Drop Connection, where a rule match will generate no HTTP response, or Send Reject, where a rule match

will generate a response to the client of HTTP 400 “Invalid Request”. Both options prevent the request from reaching the Real Server(s).

Port Following

Port following enables a switch from an HTTP connection to an HTTPS (SSL) connection to be persistent on the same Real Server. Port following can only be switched on if the current service is an HTTPS service, and if there exists a HTTP service with the same IP address as this HTTPS service. Both Virtual Services must have the same set of Real Servers and both Virtual Services should have a Layer 7 persistence enabled.

Sorry (Not Available) Server

If no Real Servers are available, the LoadMaster will redirect to a specified location, with no checking. This is colloquially referred to as the ftp server.

Not Available Redirection Handling

When no Real Servers are available to handle the request you can define the error code and URL that the client should receive.


Error Code:

If no Real Servers are available, the LoadMaster can terminate the connection with a HTTP error code. Select the appropriate error code.

Set Redirect URL:

When no Real Servers are available and an error response is to be sent back to the client, a Redirect URL can also be specified. The URL value can be parameterized. %h is used to substitute hostname and %s will substitute URI.


17.4.8 View/Modify Existing (Remote Terminal Service)

 This section is not relevant to the LoadMaster *Exchange* product.

Properties of the Virtual Service include the Generic Type and also provide Remote Terminal specific options.

Persistence

If the terminal servers support a Session Directory, the LoadMaster will use the "routing token" supplied by the Session Directory to determine the correct host to connect to. The LoadMaster persistency timeout value is irrelevant here - it is a feature of the Session Directory.

 The switch "IP address redirection" in the Session Directory configuration MUST be UNCHECKED for this to work.

Using Session Directory with LoadMaster is optional, in terms of persistence. If the Client pre-populates the username and password fields (see figure x) in the initial request, then this value is stored on the LoadMaster. As long as these fields are still populated upon reconnect, the LoadMaster will look up the name and reconnect to the same server as the original connection. The persistence timeout is used to limit the time the information is kept on the LoadMaster.

If using "Terminal-Service or Source IP" mode, then if neither of these two modes succeeds, then the source IP address will be used for persistency.

Service Check for the Virtual Service

Only three options are available; ICMP, TCP and RDP. Remote Terminal Protocol opens a TCP connection to the Real Server on the Service port (port 3389). The LoadMaster sends a 1110 Code (Connection Request) to the server. If the server sends a 1101 Code (Connection Confirm) then LoadMaster closes the connection and marks the server as active. If the server fails to respond within the

configured response time for the configured number of times or if it responds with a different status code, it is assumed dead.

17.4.9 Real Servers

This section allows you to create a Real Server (RS) and lists the Real Servers that are assigned to the Virtual Service. The properties of the Real Servers are summarized and there is also the opportunity to add or delete a Real Server, or modify the properties of a Real Server. When Content Switching is enabled, there is also the opportunity to add rules to, or remove rules from, the Real Server (see Add Rule).

17.4.10 Add Real Server

Clicking the Add New Button brings you to the following screen where the properties of the Real Server are set. These are:

Please Specify the Parameters for the Real Server

Real Server Address	<input type="text"/>
Port	<input type="text" value="80"/>
Forwarding method	<input type="text" value="nat"/>
Weight	<input type="text" value="1000"/>

The following Real Servers are already configured

192.168.201.60:80
192.168.201.65:80

The Real Server can be on one of the following networks


192.168.201.0/24

Real Server Address: The Real Server IP address (this is not editable when modifying a Real Server).

Port: The forwarding port of the Real Server. This field is editable, so the port may be altered if necessary.

Forwarding Method: Either NAT (Network Address Translation) or Route (Direct) forwarding. Whether it is available is dependent on the other modes selected for the service.

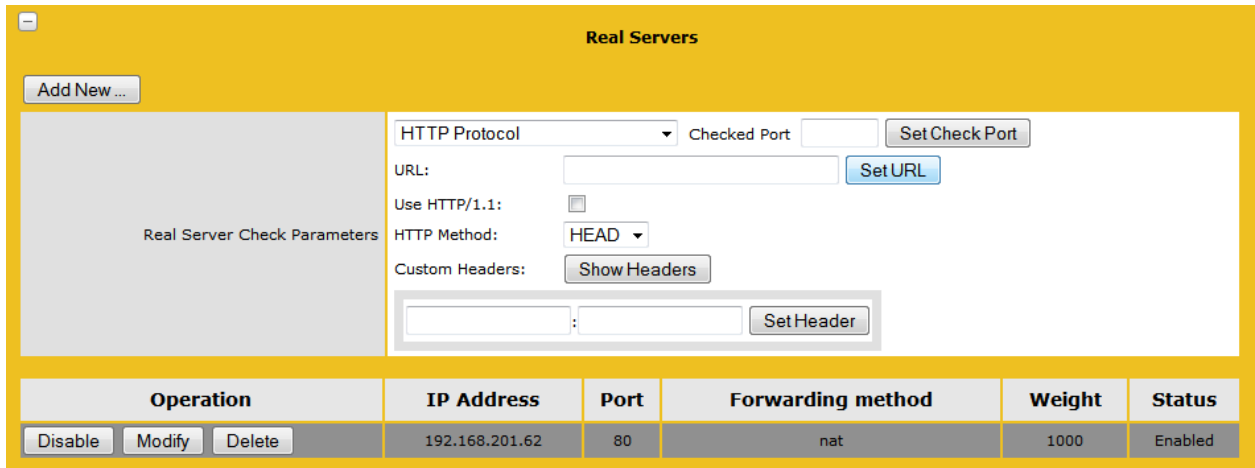
Weight: The Real Server's weight. This is weight of the Real Server, as used by the Weighted Round Robin, Weighted Least Connection and Adaptive scheduling method. The default initial value for the weight is 1000, the maximum is 65535, and the minimum is 1. It is a good benchmark to give a Real Server a weight relative to its processor speed, i.e. if server1 seems to bring four times the power of server2, assign a weight of 4000 to server1 and weight of 1000 to server2.

 For the LoadMaster *Exchange*, there is a limit of six (6) Real Servers that may be configured.

Click Add This Real Server and it will be added to the pool.

17.4.11 Real Server Check Parameters

This provides a list of checks for well-known services, as well as lower level checks for TCP/UDP or ICMP. With the service checks, the Real Servers are checked for the availability of the selected service. With TCP/UDP the check is simply a connect attempt.



Real Server Check Protocol

The list to the right shows the options that may be used to verify RS health. You may also specify a specific healthcheck port on the RS. If none are specified here, it will default to the RS port.

Healthcheck URL

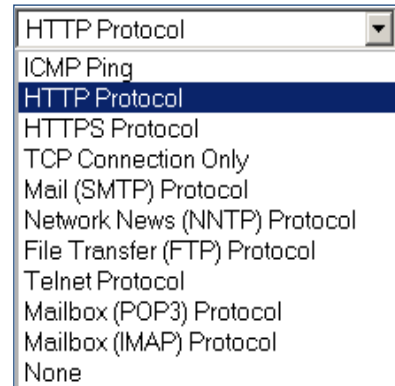
By default, the health checker tries to access the URI / to determine if the machine is available. A different URL can be specified here.

Use HTTP/1.1:

By default the LoadMaster uses HTTP/1.0. However you may opt to use HTTP/1.1 which will operate more efficiently.


HTTP Healthcheck Method

When accessing the healthcheck URL, the system can use either the HEAD or the GET method.



HTTP Reply 200 Pattern

When using the GET method, the contents of the returned response message can be checked. If the response contains the string specified by this Regular Expression, then the machine is determined to be up. (The response will have all HTML formatting information removed before the match is performed. Only the first 4K of response data can be matched.

 If the pattern starts with a caret ‘^’ symbol, it inverts the pattern response.

The following health-check methods may be specified.

Method	Action
ICMP Ping	An ICMP ping is sent to the Real Server
HTTP	HTTP checking is enabled
HTTPS	HTTPS (SSL) checking is enabled
TCP	A basic TCP connection is checked.
Mail	The SMTP (Simple Mail Transfer Protocol) is used.
NNTP	The (Network News Transfer Protocol) is used.
FTP	The (File Transfer Protocol) is used.
Telnet	The (Telnet protocol) is used.

POP3	The (Post Office Protocol – mail client protocol) is used.
IMAP	The (Internet Message Access Protocol – mail client protocol) is used.
None	No checking performed.

Custom Headers

Here you can specify up to 4 additional headers/fields which will be sent with each healthcheck request. Clicking the button Show Headers will show the entry fields. The first field is where you define the key for the custom header that is to be part of the healthcheck request. The second field is the value of the custom header that is to be sent as part of the healthcheck request. Once the information is input, click the Set Header button.

If a user has specified HTTP/1.1, the Host field is sent as before to the RS. This can be overridden by specifying a Host entry in the addition headers section. The User-Agent can also be overridden in the same manner. If an RS is using adaptive scheduling, the additional headers which are specified in the healthcheck are also sent when getting the adaptive information.

17.5 Statistics

Shows the activity for the Loadmasters within the system (Global), the Real Servers and the Virtual Services

17.5.1 Global Statistics

CPU


This table displays the following CPU utilization information for a given LoadMaster:

Use the percentage of the CPU, which is spent in processing in user mode

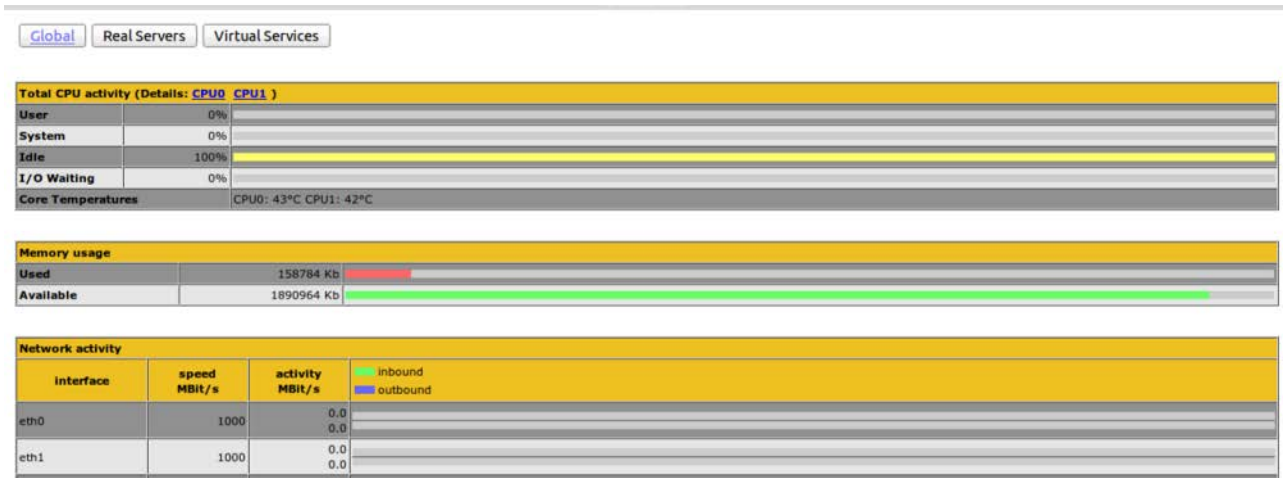
System the percentage of the CPU spent processing in system mode

I/O Waiting the percentage of the CPU spent waiting for I/O to complete

Idle the percentage of CPU, which is idle

 The sum of these 4 percentages will = 100%

Core Temp: temperature for each CPU core is displayed for LoadMaster hardware appliances by clicking the link for each CPU. Temperature will not show on a Virtual LoadMaster statistics screen.



Memory

This bar graph shows the amount of memory in use and the amount of memory free on the LoadMaster.

Network Activity

These bar graphs show the current network throughput on each interface.

17.5.2 Real Server Metrics

These graphs display the connections, bytes, bits or packets, depending on choice -the buttons in the top right of the page toggle which value is to be displayed- handled by each Real Server. The value is a sum over all Virtual Services that this Real Server is a part of, and is represented as a percentage of, the overall value for the whole LoadMaster.

Global													Real Servers	Virtual Services	Connections				Bytes	Bits	Packets
	Name	RS-IP	Status	Adaptive	Total Conns	Last 60 Sec	5 Mins	30 Mins	1 Hour	Active Conns	Current Rate Conns/sec	[%]	Conns/sec								
1		192.168.201.60	Up		0	0	0	0	0	0	0	0									
2		192.168.201.61	Up	0	0	0	0	0	0	0	0	0									
3		192.168.201.62	Up		0	0	0	0	0	0	0	0									
4		192.168.201.65	Up		0	0	0	0	0	0	0	0									
4	System Total Conns				0	0	0	0	0	0	0/sec										

17.5.3 Virtual Service Metrics


These graphs display the connections, bytes, bits or packets, depending on choice -the buttons in the top right of the page toggle which value is to be displayed- for each Virtual Service, and displays how these are distributed across the Virtual Service's Real Servers by means of the percentage of the total for the Virtual Service that each Real Server handles.

Global													Real Servers	Virtual Services	Connections				Bytes	Bits
	Name	Virtual IP Address	Protocol	Status	Total Conns	Last 60 Sec	5 Mins	30 Mins	1 Hour	Active Conns	Current Rate Conns/s	Real Servers								
												RS-IP	[%] Conns/s							
1	Standard	192.168.201.120:80	tcp	Up	0	0	0	0	0	0	0	192.168.201.60	0							
												192.168.201.61	0							
2	HTTPS	192.168.201.121:443	tcp	Up	0	0	0	0	0	0	0	192.168.201.62	0							
3	Second SSL	192.168.201.122:443	tcp	Up	0	0	0	0	0	0	0	192.168.201.62	0							
4	Terminal	192.168.201.140:3389	tcp	Up	0	0	0	0	0	0	0	192.168.201.65	0							
4	System Total Conns				0	0	0	0	0	0	0/sec									

17.6 Enable/Disable Real Servers

	Real Server	Status	Operation	
1	192.168.201.60	Enabled	Enable	Disable
2	192.168.201.61	Enabled	Enable	Disable
3	192.168.201.62	Enabled	Enable	Disable
4	192.168.201.65	Enabled	Enable	Disable

This screen shows the current status of the Real Servers and gives the user the option to Disable or Enable each RS. Each Real Server has a corresponding buttons, and pressing one button will take an online server offline, and vice-versa. The status can be Enabled (Green), Disabled (Red) or Partial (Yellow) –meaning the Real Server is enabled in one Virtual Service.

 **CAUTION:** disabling a Real Server will disable it for all Virtual Services configured to use it. If it is the only RS available, i.e. the last one, the VS will effectively be down and not pass any traffic.

17.7 Rules & Checking


17.7.1 Content Rule Management

This screen shows rules that have been configured and gives the option to Modify or Delete.

Content Matching Rules						
	Operation	Name	Match Type	Options	Header	Pattern
1	<input type="button" value="Modify"/> <input type="button" value="Delete"/>	RL1	RegEx	Ignore Case		rules
2	<input type="button" value="Modify"/> <input type="button" value="Delete"/>	RL2	prefix	Negate Add Host		1234

Header Modification Rules						
	Operation	Name	Rule Type	Header	Pattern	Replacement
3	<input type="button" value="Modify"/> <input type="button" value="Delete"/>	RL5	Add Header	TEST		rules

To define a new rule, click on "Create New". You must give the rule a name.

 Rule names must be alphanumeric, unique and start with an alpha character. They are case sensitive, thus two different rules can exist in the form "Rule1" and "rule1". Giving a rule an existing name will overwrite the rule of that exact name.

Rule Name	<input type="text"/>
Rule Type	Content Matching ▾
Match Type	Regular Expression ▾
Header Field	<input type="text"/>
Match String	<input type="text"/>
Negation	<input type="checkbox"/>
Ignore Case	<input type="checkbox"/>
Include Host in URL	<input type="checkbox"/>
Include Query in URL	<input type="checkbox"/>
<input type="button" value="Cancel"/> <input type="button" value="Create Rule"/>	

Rule Types:

- Content Matching – matches the content of the header
- Add Header – adds a header according to the rule
- Del Header – deletes the header according to the rule
- Replace Header – replaces the header according to the rule
- Modify URL – changes the URL according to the rule

Match Types:

- Regular Expression – compares the header to the rule
- Prefix – compares the prefix of the header according to the rule
- Postfix – compares the postfix of the header according to the rule

For further information on configuring rules, please refer to the **Setting up Content Rules** section.

17.7.2 Header Modification

For separate detailed documentation see:

<http://www.kemptechnologies.com/fileadmin/content/downloads/documentation/5.1/Header-Modification-Guide.pdf>

17.7.3 Adaptive Parameters

Adaptive Parameters	
Adaptive Interval (sec)	10
Adaptive URL	/load <input type="button" value="Set URL"/>
Port	80 <input type="button" value="Set Port"/>
Min. Control Variable Value (%)	5
<input type="button" value="Reset values to Default"/>	

Adaptive Interval

This is the interval, in seconds, at which the LoadMaster checks the load on the servers. A low value means the LoadMaster is very sensitive to load, but this comes at a cost of extra load on the LoadMaster itself. 7 seconds is a good starting value. This value must not be less than the HTTP checking interval.

Adaptive URL

The Adaptive method retrieves load information from the servers via an HTTP inquiry. This URL specifies the file where the load information of the servers is stored. The standard location is "/load". It is the servers' job to provide the current load data in this file in ASCII format. In doing so, the following must be considered:

An ASCII file containing a value in the range of 0 to 100 in the first line where:

0=idle and 100=overloaded. As the number increases, i.e. the server becomes more heavily loaded, the LoadMaster will pass less traffic to that server. Hence, it 'adapts' to the server loading.

The file is set to "/load" by default.

The file must be accessible via HTTP

The URL must be the same for all servers that are to be supported by the adaptive method

Note: This feature is not only of interest for HTTP based Virtual Services, but for all Services. HTTP is merely used as the transport method for extracting the application specific load information from the Real Server.

Port

This value specifies the port number of the HTTP daemon on the servers. The default value is 80.

Min Control Variable Value

This value specifies a threshold below which the balancer will switch to static weight-based scheduling, i.e. normal Weighted Round Robin. The value is a percentage of the maximum load (0-50). The default is 5.

17.7.4 Service (Health) Check Parameters

The LoadMaster utilizes Layer 3, Layer4 and Layer7 health checks to monitor the availability of the Real Servers and the Virtual Services.

Service Check Parameters	
Check Interval(sec)	9
Connect Timeout (sec)	4
Retry Count	2
<input type="button" value="Reset values to Default"/>	

Check Interval

With this field you can specify the number of seconds that will pass between consecutive checks. The recommended value is 7 seconds.

Connect & Response timeouts

The HTTP request has two steps: contact the server, and then retrieve the file. A timeout can be specified for each step, i.e. how long to wait for a connection, how long to wait for a response. A good value for both is 3 seconds.

Retry Count

This specifies the number of retry attempts the check will make before it determines that the server is not functioning. A value of 1 or less disables retries.

17.8 Certificates

17.8.1 SSL Certificates

Filename:

Filename	Common Name(s)	Virtual Services	Operations
1kkeycert	www.kemptest020207.com	192.168.201.121:443	VS to Add <input type="button" value="Add VS"/> VS to Delete <input type="button" value="Del VS"/> <input type="button" value="Replace Certificate"/> <input type="button" value="New CSR"/> <input type="button" value="Delete Certificate"/>
myhines	*.myhines.com	192.168.201.122:443	VS to Add <input type="button" value="Add VS"/> VS to Delete <input type="button" value="Del VS"/> <input type="button" value="Replace Certificate"/> <input type="button" value="New CSR"/> <input type="button" value="Delete Certificate"/>

Administrative Certificates

Administrative Certificate

Self Signed Virtual Services

192.168.201.120:80

Shown above is the Manage Certificates screen where:

Import Certificate – imports the certificate with your chosen filename.

Add Intermediate – see 6.2 below.

Filename – is the name given to the certificate at the time it was created.

Common Name(s) – is the FQDN (Fully Qualified Domain Name) for your site.

Virtual Services – the Vs' with which the certificate is associated.

Operations –

- **VS to Add** – the dropdown lists all the SSL Virtual Services configured on the LoadMaster. Click **Add VS** when you have located the one you want. It will appear in the Virtual Services box.
- **VS to Delete** – removes the association of the certificate and VS. It will neither delete the certificate nor the VS, only the link between them.
- **Replace Certificate** – updates or replaces the certificate stored in this file.
- **New CSR** – generates a new CSR based upon the current certificate.

Administrative Certificates – the certificate you want to use, if any, for the administrative interface..

17.8.2 Intermediate Certificates

This shows a listing of the installed intermediate certificates and the name assigned to them.

Intermediate Certificates currently installed on your LoadMaster

File Name	Options
james.pem	<input type="button" value="Delete"/>
james1.pem	<input type="button" value="Delete"/>

If you already have a certificate, or you have received one from a CSR, paste the complete certificate in the window shown and then assign the certificate the desired name. The name may contain only alpha characters with a maximum of 32 characters.

Copy and Paste the entire body of the Intermediate Certificate below:

Intermediate Certificate:


Desired File Name
(i.e. - VeriSignCert.pem or Thwarte.cer):

.pem or .cer

Cancel
Add Certificate

17.8.3 Certificate Signing Request

If you do not have a certificate, you may complete the Certificate Signing Request (CSR) and click Create CSR button.

 All CSR's are generated with a 2048-bit key by default. If the box marked Use 2048 bit key is unchecked, a 1024-bit key CSR is generated. The exception is the LoadMaster model LM-1500 that can generate a 1024-bit key only. However, it will accept and can use a 2048-bit key certificate.

All Fields are optional except "Common Name"

2 Letter Country Code (ex. US):	<input style="width: 95%;" type="text"/>
State/Province (Entire Name - New York, not NY):	<input style="width: 95%;" type="text"/>
City:	<input style="width: 95%;" type="text"/>
Company:	<input style="width: 95%;" type="text"/>
Organization (e.g., Marketing, Finance, Sales):	<input style="width: 95%;" type="text"/>
Common Name: (The fully qualified domain name for your web server)	<input style="width: 95%;" type="text"/>
Email Address:	<input style="width: 95%;" type="text"/>
SAN/UCC Names	<input style="width: 95%;" type="text"/>
Use 2048 bit key	<input checked="" type="checkbox"/>

Cancel
Reset
Create CSR

After clicking the 'Create CSR' button, the following screen appears:

The following is your 2048 bit *unsigned* certificate request. Copy the following, in its entirety, and send it to your trusted certificate authority

```
-----BEGIN CERTIFICATE REQUEST-----
MIICVzCCAT8CAQAwEjEQA4GA1UEA4MHdGVzdGNqbTCCASiwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBAAORcVNLzvYeuMmcFmetWUqu8KxLqdPLYffTcWQaj2kv2
IgYUgWjMxOyF5FCZ6fboKzLbPsin079rqq0wV9EFQn5PbemUXmGK67R8pqtQkh7
/zFtteCosrOahtdVcqrJnZHas8r0hvoEaAtAYUPgDdNIazHKtt4VCyhe3Uaj6RKHK
dkBk8LtzCrGwG86XAxM7H/Xbsyh/DrZ084gA1UCEDBuen8qk+Fkkt2mZz1SG9RH
6Zv6TvdjUHVog0MsBTCo7KRxKb2yIK4HAz9oWG/3IqQkY7pJCPovsRbrNZ1UzGak
TfnMG4AOY1qZCRGFTWvUTJOF04Y16rkJTj+J4VimkUUCAwEAAaAMA0GCSqGSIb3
DQEBBQAA4IBAQCpZLcgmGBSEKwckfApsN3YXmha+f12uosBo/JDyNjazz2HF
JSmFOLf7xNhn9ZmaJUBGJrV23YmVJ2cjhMjRN2usOkOj75FCjwdRwzm11PaINz
vTTk/Z1qdl7EE9TdGQPAHead16RSYMs5WzW83mVoheg7uAcKg2HV00KmPWP6U66
6eTuNBvFxy/lxOGjIU2uh7wKr0SbydCmKdU7di6UvYQBMaO/qltcSnHOHcft+rm
ZmNeHgflErwZDRLYI6VQ2M3eWGb7L16/8avbDC3Hq1CjdWBBHANSSp8zavZ1QHfa
hEDRTKBIAG/Sg+E1ELjJXXTBenbHurK01FrP
-----END CERTIFICATE REQUEST-----
```

The following is your private key. Copy the following, in its entirety, and save as a .key file. Do this using a text editor such as Notepad or VI (Do not use Microsoft Word - extra characters will be added making key unusable). Key will later be used during the certificate upload process. DO NOT lose or distribute this file!


```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEASfXU0v09h64wx8x61ZSq7wrEup08th99NxZBqPaS/Y1AZhS
DCMzE7J9IVnp9ugg4sGmyKfTv2uqrTBXOQVA3k9t6ZReYyrrtHymq1CSHv/MW21
4K1ys4CG11VypEmdkcCzyvSG84Rq0BhQ+AN00hrMccq23hULKF7dRqPpEocp2QGTw
u3MKsbAbzpcDEzsF9dusKH8OtK7ziADVQIQMG56fyqT4WSRtPaZnPv1b1EfpM/pO
9204dWiDQyWFMKjSpHEpvbIgrgcDP2hYb/cipCRjukkKk5WxFus1nVTMYCRN+cwb
gDRjWpkJEYVNa9RMk4XThjXquQ1OP4nhWYrRQIDAQABAoIBAQC6MrosQfKHudwl
jqbKbKzEqyHhS4iVNLVGP58KzFBApTgu6z4DDXQo3EAvkvYYI/fSg4VoWgtggXC3
2NdN0Jn9kg4jPiVYg1ZknOPc/+VgakeBSr2fpozFIMacrhviHe+ulltB4KxjwxTA
BQOHpHHMmXKEdLvgax7N8oKJ7xr2LjVMg3oRzqhHLyVJ0j+/KsGldYEap2gcjJ8
fm77ISoF2rKj4dTmtM86IATMTuMwou2efoJB3FO9H4p6GtTJmQQ3VHdEo+XhMh8
Ngx5VVPQ0a5QqgkUyTgqOUA9LKMfF2KF5TaFNox059W2D/JHBWkzZoF3vy4InDQL
C4K/Gt1hAoGBAPOoYp0PoZaex6vRK6x+NasXO1Z2H2mknhyQ663RL7yHF1VGOC/gN
1MeCOfrN9NEDjRit3dGSmm7gx4cVCbeZu/m72nk3Dwa900dALtfgqg/HNFgiKvWv
YyvRCDsxhk0Q9nncew/a4upLAXNBjMpBvbsUbGwFtpOVROCUtwaFJAxAZaGBAPAG
y2ngD9rbAajy/fstA4ELN5n9FV9rLONHzYRwcuNyA51CSDvCubGNL41sSRA0xwC8
dUeRr1n3zaISCy2W3ATR58gdnL94tSX2w4dRKYegx/qHCUn9mrl/CYwZixG4MUGC
Aewdcu52uKngw6wZbRtXsZCwPnQrKJGangG5117NAoGBAN+9EMvVjBV9jxd7c491
8pHuCp0wLKiSUsMjRqsluSdHE8DGMo08QrFytVnVbqcdIVzUw5R/s011a0MNUe
2Pw1aCfQPVlGjgOhpmaR795I9QDxgmNgdM3PnkWj9qfdKUR8B8ua3D824AIs+VTZ
aAoP3PoGWHYi5z8KfvESZechAoGAAb866c1ctC4V5AHowVRBi0XmoLML3YbtK7Zr
FqX04E8IY3QtdGpNabJqXyivm3OW4zV78QppaVE5a02SsUFA1rQkaLtc2zPstVt
L0WNuL8d1K/4HFbBMopvKlRhPT7G9QAaPKq1ZHDuxSWSNqV2WsmqzGfL/JJ32B90
+QARoh0CgYAgty53Php1Ou1Tps+ex6I7agUiZYGjAO5jVJ1YLHMWk5RF9SsKk
FuY12rSzauub9zK6C54PrNmybHxgRmcYSPFudSfYvS+042Lqkix+v3q3KybRvo
UiFaERnASdclugN3p88XISjXHLXm09dyxk1Vyznpftuv56a4b0a7uA==
-----END RSA PRIVATE KEY-----
```

The top part of the screen should be copied and pasted into a plain text file and sent to the Certificate Authority of your choice. They will validate the information and return to you a validated certificate.

The lower part of the screen is your private key and should be kept in a safe place. This key should not be disseminated as you will need it to use the certificate. Copy and paste the private key into a plain text file (do not use any application such as MS Word) and keep the file safe.

17.8.4 Backing Up and Restoring Certificates

When backing up certificates, you will be prompted to input a mandatory passphrase (password). The parameters of the passphrase are that it must be alpha numeric, it case sensitive with a maximum of 64 characters.

 **CAUTION** This passphrase is a mandatory requirement to restore a certificate. A certificate cannot be restored without the passphrase. If it is forgotten, there is no way to restore the certificate.

Certificate Backup

Backup all VIP and Intermediate Certificates Passphrase

Restore Certificates

Backup File

Which Certificates What to restore

Passphrase

17.9 System Configuration

This section provides access to the parameters of the LoadMaster and the systems as an entire entity and is shown on the lower left side of the screen.


17.9.1 Interfaces

Describes the external network and Internal network interfaces. The screen has the same information for the eth0 and eth1 Ethernet ports. The example below is for eth0 on a non HA unit. Also see VLAN bonding in this document.

Network Interface 0


Interface Address (address[/prefix])	192.168.201.58/24	Set Address
Link Status	Speed: 1000Mb/s, Full Duplex Automatic	Force Link
Additional addresses (address[/prefix])	3fe:1900:4545::3:02	Add Address Modify Address Delete

VLAN Configuration
Interface Bonding

 If you have an older infrastructure that does not support VLAN tagging, you may associate additional subnets to any interface by designating a base network address and a subnet mask. The LoadMaster will not create any routes to these additional subnets. If needed, an external device supporting router-on-a-stick configuration can be deployed alongside the LoadMaster.

Subnets on this Interface

Subnet	Local Address	Action
11.0.0.0/8	11.0.0.1	Add Delete

 If the unit is part of an HA configuration, the following screen will be displayed when clicking one of the interfaces.

Network Interface 0

Interface Address (address[/prefix])	192.168.201.128/24	Set Address
HA Shared IP address	192.168.201.140	Set Shared address
HA Partner IP address	192.168.201.141	Set Partner address
Use for HA checks	<input checked="" type="checkbox"/>	
Link Status	Speed: 1000Mb/s, Full Duplex Automatic	Force Link
Additional addresses (address[/prefix])		Add Address

VLAN Configuration
Interface Bonding

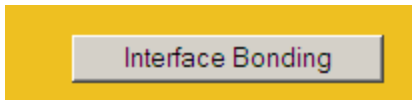
This screen tells the user:

- This is the Master machine of the pair (top left of the screen).
- This LoadMaster is up and the paired machine is down (green and red icons).
- The IP address of this LoadMaster.
- The HA shared IP address. This is the IP address used to configure the pair.

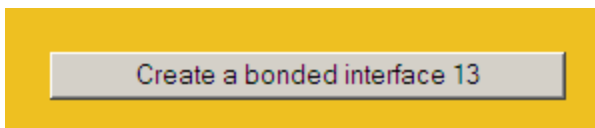
- The IP address of the paired machine.
- This interface is enabled for HA healthchecking
- The speed of the link is automatically detected.
- Any alternate addresses on this interface.

Creating a Bond/Team

Click the starting interface for the bond.

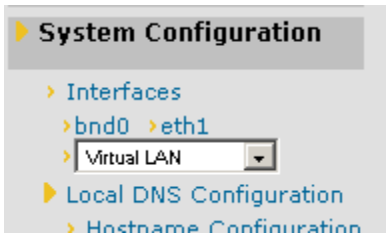


Confirm the bond creation by clicking

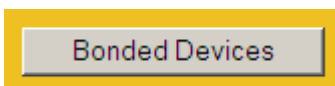


Acknowledge the warning dialogs

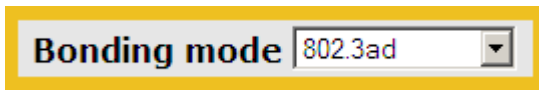
Using the Web User Interface (WUI) navigate to **System Configuration** ▶ **Interfaces** ▶ **bndX**



If you do not see the “bndX” interface refresh your browser, then select the bonded interface, then click



Select the desired bonding mode



Add the additional interfaces to this bond



Configure the IP and Subnet Mask on the bonded interface

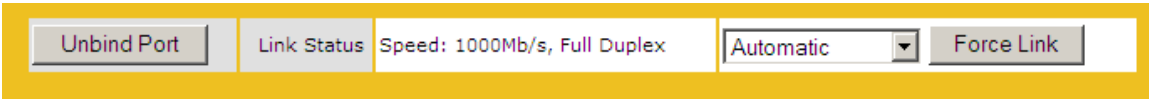
Removing a Bond/Team

Remove all VLANs on the bonded interface first; if you do not remove them they will automatically be assigned to the physical port at which the bond started.

Using the Web User Interface (WUI) navigate to **System Configuration** ▶ **Interfaces** ▶ **bndX** If you do not see the “bndX” interface refresh your browser, then select the bonded interface, then click

Bonded Devices

Unbind each port by clicking the “Unbind Port” button, repeat until all ports have been removed from bond.

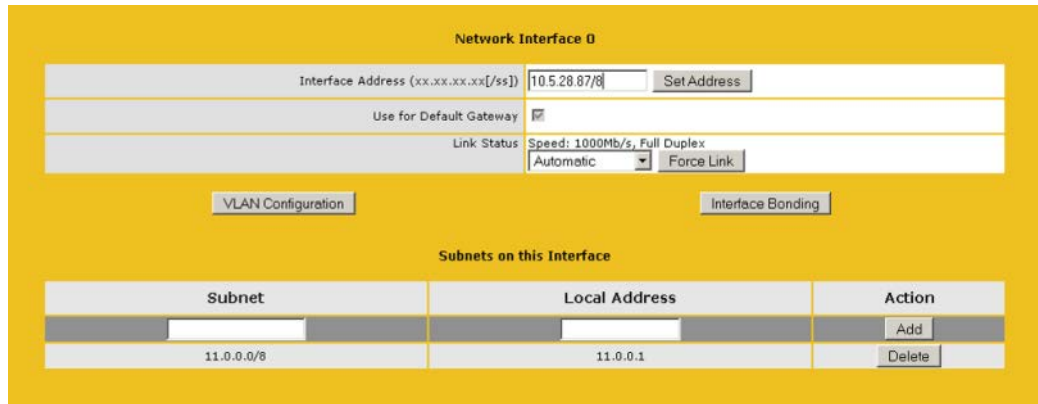


Once all child ports have been unbonded you can unbind the parent port by clicking “Unbond this interface”



▶
Adding a VLAN

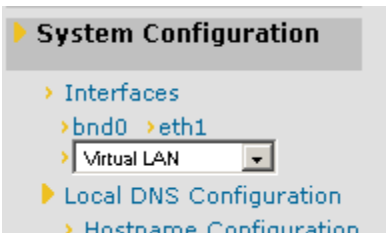
Select the interface and then click **VLAN Configuration**



Add the “VLAN Id” value and click **Add New VLAN**



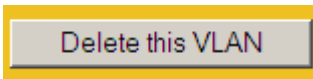
Repeat as needed, to view the VLANs you can navigate to ▶ **System Configuration** ▶ **Interfaces** ▶



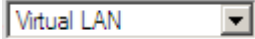
Removing a VLAN

To remove a VLAN select the appropriate VLAN ID by navigating to ▶ **System Configuration** ▶ **Interfaces** ▶ **Virtual LAN** ▶

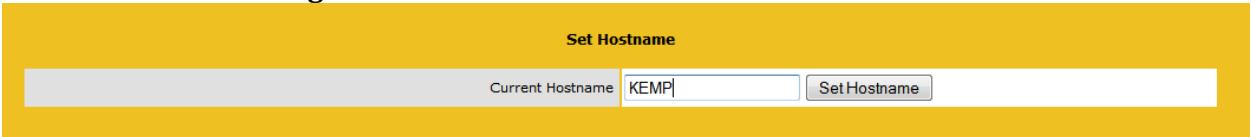
Once selected remove the IP and then click Set Address, once the IP has been removed you will have the option to delete the VLAN



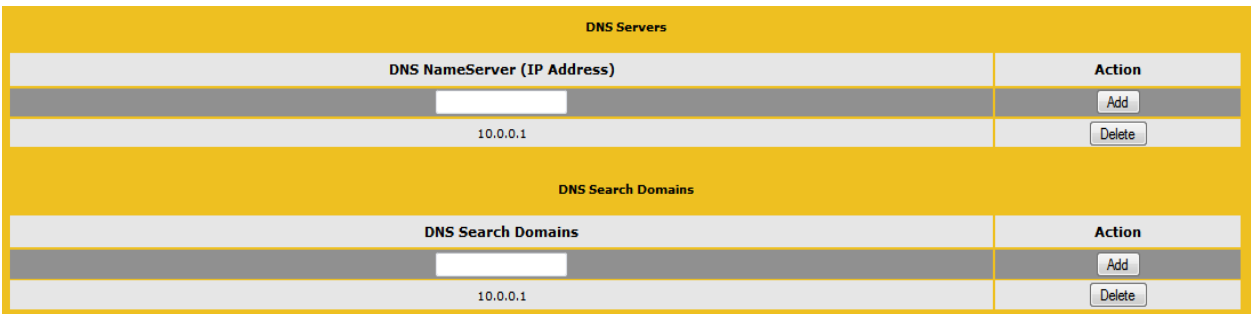
Repeat as needed, to view the VLANs you can navigate to **System Configuration** **Interfaces**



17.9.2 Local DNS Configuration



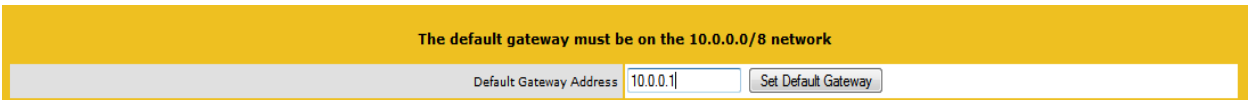
Hostname Used for Diagnostic logging



Max 3 dns servers and 6 search domains.

17.9.3 Route Management

This option permits the configuration of default and static routes. The Load Master requires a **default gateway** through which it can communicate with the Internet.



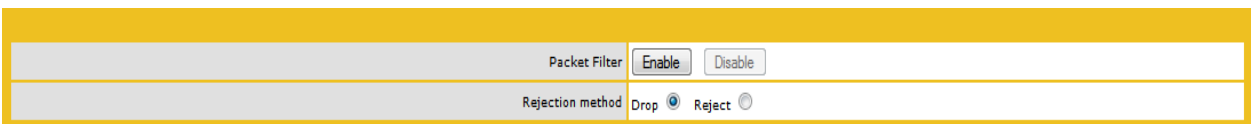
Further routes can be added. These routes are static and the gateways must be on the same network as the Load Master. To segment traffic you can also leverage the Virtual Service level default gateway.



17.9.4 Access Control

Packet Filter Enabled

Using this toggle option the Packet filter can be activated or deactivated. If the filter is not activated, the Load Master acts as a simple IP-forwarder. When the filter is activated, only the Virtual Service addresses can be addressed.



Reject/Drop blocked packets

When a connection request is received from a host, which is blocked using the ACL, the request is normally ignored (dropped). The Load Master may however be configured to send back an ICMP reject packet. For security reasons it is usually best to drop any blocked requests.

Access Control Lists

The Load Master supports a “blacklist” Access Control List system. Any host or network entered into the Access Control List will be blocked from accessing any service provided by the Load Master.

Blacklist	
Blocked addresses	Operation
<input type="text"/>	<input type="button" value="Block Address(es)"/>

Whitelist	
Allowed addresses	Operation
<input type="text"/>	<input type="button" value="Allow Address(es)"/>

The Access Control List is only enabled when the Packet Filter is enabled. The whitelist allows a specific IP address or address range access. If the address or range is part of a larger range in the blacklist, the whitelist will take precedence for the specified addresses.

This option allows a user to add or delete a host or network IP address to the Access Control List. Only “dotted-quad” IP addresses are allowed. Using a network specifier specifies a network.

For example, specifying 192.168.200.0/24 will block all hosts on the 192.168.200 network.

17.9.5 System Administration

These options control the base level operation of LoadMaster. It is important to know that applying changes to these parameters in a HA pair must be done using the floating management IP. Many of these options will require a system reboot. When configuring these parameters only the active system in a pair is affected.

17.10 User Management

Change the appliance password. This is a local change only and does not affect the password of the partner appliance in a HA deployment.

Change Password		
Current Password	<input type="password"/>	
New Password	<input type="password"/>	
Re-enter New Password	<input type="password"/>	
<input type="button" value="Reset"/>		<input type="button" value="Set Password"/>

Other Users		
User	<input type="text"/>	
Password	<input type="password"/>	
Use RADIUS Server	<input type="checkbox"/>	
<input type="button" value="Add User"/>		

User	Permissions	Action
CJMtest	Real Servers, Virtual Services, Rules, System Backup, 10.0.0.0/8	<input type="button" value="Modify"/> <input type="button" value="Delete"/> <input type="button" value="Password"/>

The User Management screen allows you to change a current Users password, add a new User and associated password or change the permissions for an existing User (see below).

Permissions for User CJMtest	
Real Servers	<input type="checkbox"/>
Virtual Services	<input type="checkbox"/>
Rules	<input type="checkbox"/>
System Backup	<input type="checkbox"/>
Certificate Creation	<input type="checkbox"/>
Intermediate Certificates	<input type="checkbox"/>
Certificate Backup	<input type="checkbox"/>
All Permissions	<input type="checkbox"/>
Allowed Network 1	None Assigned ▼
Allowed Network 2	None Assigned ▼

In this screen you may set the level of User permissions insofar as what configuration changes they are allowed to perform. The primary User, bal, always has full permissions. Secondary Users may be restricted to certain functions and to certain networks.

17.11 Update License

Access Code information will be displayed on screen. This includes the activation date and the expiration date of the current license. To apply a new license, enter the license code. A reboot may be required depending on which license you are applying.

Activation date: February 22 2011
 Licensed until: Unlimited

Please use the following Access Code to acquire a new license key
 from your KEMP representative for your LoadMaster.

Access Code: x7w3u-v4wbq-g1x88-9bx88 (Instance 232612)

License Key:

17.11.1 System Reboot

Reboot

Reboot the appliance.

Shutdown

Clicking the button attempts to power down the LoadMaster and if for some reason that fails, it will at a minimum halt the CPU.

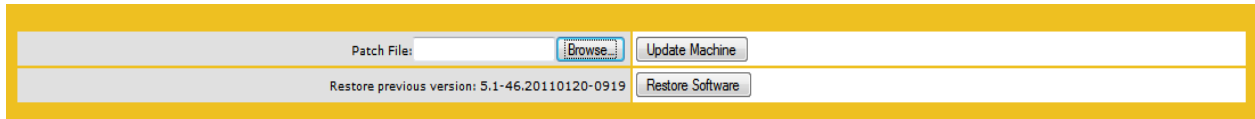
Reset To Factory Defaults

Reset the configuration of the appliance with exception to the license information and usernames and passwords. This only applies to the active appliance in a HA pair.

Reboot	<input type="button" value="Reboot"/>
Shutdown	<input type="button" value="Shutdown"/>
Reset To Factory Defaults	<input type="button" value="Reset Machine"/>

Update Software

Contact support to obtain the location of firmware patches and upgrades. Firmware download requires Internet access. Detailed patch information is available at <http://forums.kemptechnologies.com/viewforum.php?f=9>.



Update Machine

Once you have downloaded the firmware you can browse to the file and upload the firmware directly into LoadMaster. The firmware will be unpacked and validated on LoadMaster. If the patch is validated successfully you will be asked to confirm the release information. To complete the update you will need to reboot the appliance, which can be deferred.

Restore Software

If you have completed an update of LoadMaster's firmware you can revert to the previous build.

17.11.2 Backup/Restore

Create a Backup

Generate a backup that contains the Virtual Service configuration and the local appliance information. License information and SSL Certificate information is not contained in the backup.

Restore Configuration

When performing a restore (from a remote machine), the user may select what information should be restored: the Virtual Service configuration only, Base Configuration only, or both.

Automated Backup

If the Enable Automated Backups box is checked, the system may be configured to perform automated backups on a daily or weekly basis.

When to Perform Backup – specify the time (24 hour clock) and may be set daily, or specific day of the week. When set, click the Set Backup Time button.

Remote User –username required to access remote host.

Remote Password – password required to access remote host.

Remote Host – remote host name.

Remote Pathname –the location on the remote host to store the file.

Create a Backup

Backup the LoadMaster

Restore Configuration

Backup File:

 LoadMaster Base Configuration
 VS Configuration

Automated Backups

Enable Automated Backups	<input checked="" type="checkbox"/>
When to perform backup	0 : 0 Day of week: Daily <input type="button" value="Set Backup Time"/>
Remote user	<input type="text"/> <input type="button" value="Set Remote User"/>
Remote password	<input type="text"/> <input type="button" value="Set Remote Password"/>
Remote host	<input type="text"/> <input type="button" value="Set Remote Host"/>
Remote Pathname	<input type="text"/> <input type="button" value="Set Remote Pathname"/>



The Automated Backup transfer protocol is currently only FTP.

17.11.3 Date/Time

You can manually configure the date and time of LoadMaster or leverage an NTP server.

NTP host(s)	<input type="text"/> <input type="button" value="Set NTP host"/>
Set Date	4 Mar 2011 <input type="button" value="Set Date"/>
Set Time	15 : 57 : 11 <input type="button" value="Set Time"/>
Set TimeZone	UTC <input type="button" value="Set TimeZone"/>

NTP host(s)

Specify the host which is to be used as the NTP server. NTP is a strongly preferred option for an HA cluster. For a single unit it is at the user discretion.



The time zone must always be set manually.

17.12 Logging Options

Logging of LoadMaster events can be both pushed and also pulled from the appliance. It is important to note that log files on LoadMaster are not historical, if the appliance reboots the logs are reset. It is important to keep a record of events generated on LoadMaster on a remote facility.

17.12.1 Log Files

Boot.msg File - contains information during the initial starting of LoadMaster.

Warning Message File - contains warnings during the operation of LoadMaster.

System Message File - contains system events during the operation of LoadMaster, this included both operating system level and LoadMaster internal events.

Reset Logs - will reset ALL log files.

Save all Log Files - is used if you need to send logs to KEMP support as part of a support effort. Click this button, save the files to your PC and forward them to KEMP support.

Boot.msg File	<input type="button" value="View"/>
Warning Message File	<input type="button" value="View"/>
System Message File	<input type="button" value="View"/>
Reset Logs	<input type="button" value="Reset"/>
Save all Log Files	<input type="button" value="Download Log Files"/>

17.12.2 Debug Options

The LoadMaster has a range of features that will aid the User and KEMP Support staff with diagnosing connectivity issues. Clicking the Debug Options button will bring up the screen shown below.

Disable All Transparency – disables transparency on every VS and forces them to use Layer 7. Use with caution.

Enable L7 Debug Traces – generates log traffic in the message files. Due to the large amount of files being logged it slows down L7 processing.

Perform an I7adm – displays raw statistics about the L7 subsystem.


Enable IRQ Balance – enable this option only after consulting with KEMP support staff.

Disable All Transparency	<input type="button" value="Disable Transparency"/>
Enable L7 Debug Traces	<input type="button" value="Enable Traces"/>
Perform an I7adm	<input type="button" value="I7adm"/>
Enable IRQ Balance	<input type="button" value="Enable IRQ Balance"/>
Enable FIPS 140-2 level 1 Mode	<input type="button" value="Enable FIPS mode"/>
Perform a PS	<input type="button" value="ps"/>
Display Meminfo	<input type="button" value="Meminfo"/>
Display Slabinfo	<input type="button" value="Slabinfo"/>
Perform an Ifconfig	<input type="button" value="Ifconfig"/>
Ping Host	Host: <input type="text"/> <input type="button" value="Ping"/>
Kill VM Instance: 210600	<input type="text"/> <input type="button" value="Kill VM"/>

TCP dump

Interface: eth0	Address: <input type="text"/>	Port: <input type="text"/>	Start: <input type="button" value="Start"/>	Stop: <input type="button" value="Stop"/>	Download: <input type="button" value="Download"/>
-----------------	-------------------------------	----------------------------	---	---	---

Enable FIPS 140-2 Level 1 Mode – switch to the FIPS level for this machine. Requires a reboot.

 This forces the LoadMaster to use FIPS 140-2 Level 1 software for all SSL traffic. Once the LoadMaster has been switched to FIPS *it cannot be reversed*. See FIPS 140-2 Addendum document.

Perform a PS – performs a ps on the system.

Display Meminfo – displays raw memory statistics.

Display Slabinfo – displays raw slab statistics.

Perform an Ifconfig – displays raw Ifconfig output.

Ping Host – performs a ping on the specified host.

Kill VM Instance nnnnnn – kills the VM instance.



As this disables the virtual machine you should have previously consulted with KEMP support.

TCP dump -

A TCP dump can be captured either by one or all Ethernet ports. Optionally an address and port may be specified. The User has control over stopping and starting the dump and then downloading to a particular location.

17.12.3 Syslog Options

The LoadMaster can produce various warning and error messages using the syslog protocol. These messages are normally stored locally and may be displayed via the diagnostics menu point. It is also possible to configure the LoadMaster to transmit these error messages to a remote syslog server (menu point: extended->syslog).

Six different error message levels are defined and each message level may be sent to a different server. Notice messages are sent for information only; Emergency messages normally require immediate user action.



One point to note about syslog messages is they are cascading in an upwards direction. Thus, if a host is set to receive WARN messages, the message file will include message from all levels above WARN but none for levels below.



We recommend you do not set all six levels for the same host because multiple messages for the same error will be sent to the same host.

Emergency Host	<input type="text"/>
Critical Host	<input type="text"/>
Error Host	<input type="text"/>
Warn Host	<input type="text"/>
Notice Host	<input type="text"/>
Info Host	<input type="text"/>



To enable a syslog process on a remote Linux server to receive syslog messages from the LoadMaster, the syslog must be started with the “-r” flag.

17.12.4 SNMP Options

With this menu, the SNMP configuration can be modified.

Enable/Disable SNMP metrics

This toggle option enables or disables SNMP metrics. For example this option allows the LoadMaster to respond to SNMP requests.

- By default SNMP is disabled.
- When the feature is enabled, the following traps are generated:
 - ColdStart** generic (start/stop of SNMP sub-system)

- ⚠ **VsStateChange** (Virtual Service state change)
- ⚠ **RsStateChange** (Real Server state change)
- ⚠ **HaStateChange** (HA configuration only: LoadMaster failover)

The information regarding all LoadMaster-specific data objects is stored in three enterprise-specific MIBs (Management Information Base).

ONE4NET-MIB.txt	enterprise id
IPVS-MIB.txt	Virtual Server stats
B-100-MIB.txt	LoadMaster configuration data

These MIBs (located on the LoadMaster CD) need to be installed on the SNMP manager machine in order to be able to request the performance-/config-data of the LoadMaster via SNMP.

The description of the counters can be taken from the LoadMaster MIBs (the description clause). Apart from just reading the MIB this can be done for Linux (nad ucidsnmp) with the command:

```
snmptranslate -Td -OS <oid>
where <oid> is the object identifier in question.
```

Example: <oid> = .1.3.6.1.4.1.one4net.ipvs.ipvsRSTable.rsEntry.RSConns
 snmptranslate -Td -Ov .1.3.6.1.4.1.one4net.ipvs.ipvsRSTable.rsEntry.RSConns
 .1.3.6.1.4.1.12196.12.2.1.12

```
RSConns          OBJECT-TYPE
-- FROM          IPVS-MIB
SYNTAX           Counter32
MAX-ACCESS       ead-only
STATUS           current
DESCRIPTION      "the total number of connections for this RS"
 ::= { iso(1) org(3) dod(6) internet(1) private(4) enterprises(1) one4net(12196) ipvs(12)
       ipvsRSTable(2) rsEntry(1) 12 }
```

The data object defined in the LoadMaster MIBS is a superset to the counters displayed by the WUI.

Note: The data objects on the LoadMaster are not writable, so that only GET requests (GET, GET-NEXT, GET-BULK,..) should be used.

Enable SNMP	<input checked="" type="checkbox"/>
SNMP Clients	<input type="text"/>
Community String	public
Contact	<input type="text"/>
Location	<input type="text"/>
Enable SNMP Traps	<input type="checkbox"/>

Configure SNMP Clients

With this option, the user can specify from which SNMP management hosts the LoadMaster will respond to.



If no client has been specified, the LoadMaster will respond to SNMP management requests from *any* host.

Configure SNMP Community String

This option allows the SNMP community string to be changed. The default value is “public”.

Configure SNMP Contact

This option allows the SNMP Contact string to be changed. For example, this could be e-mail address of the administrator of the LoadMaster.

Configure SNMP Location

This option allows the SNMP location string to be changed.

SNMP traps

When an important event happens to a LoadMaster a Virtual Service or to a Real Server, a trap is generated. These are sent to the SNMP trap sinks.

Enable/Disable SNMP Traps

This toggle option enables and disables the sending of SNMP traps.



SNMP traps are disabled by default.

Configure SNMP Trap Sink1

This option allows the user to specify a list of hosts to which a SNMPv1 trap will be sent when a trap is generated.

Configure SNMP Trap Sink2

This option allows the user to specify a list of hosts to which a SNMPv2 trap will be sent when a trap is generated.

17.12.5 Email Options

This option permits the configuration of email alerting for LoadMaster events. Email notification can be delivered for six predefined informational levels. Each level can have a distinct email address and each level supports multiple email recipients. Email alerting depends on a mail server, support for both an open relay mail server and a secure mail server is provided. Testing email configuration can be done using the Web User Interface and navigating to System Configuration -> System Administration -> Logging Options -> Email Options

Enable Email Logging	<input checked="" type="checkbox"/>
SMTP Server	<input type="text"/> <input type="button" value="Set Server"/> Port <input type="text"/> <input type="button" value="Set Port"/>
Server Authorization (Username)	<input type="text"/> <input type="button" value="Set"/>
Authorization Password	<input type="text"/> <input type="button" value="Set Password"/>
Local Domain	<input type="text"/> <input type="button" value="Set Domain"/>
Connection Security	None <input type="button" value="v"/>

Emergency Recipients	<input type="text"/>
Critical Recipients	<input type="text"/>
Error Recipients	<input type="text"/>
Warn Recipients	<input type="text"/>
Notice Recipients	<input type="text"/>
Info Recipients	<input type="text"/>

Sample Email Alert:

Subject: KEMP2 INFO Log Message

From: INFO-Logger.KEMP2@kemptechnologies.com

Date: 3:42 PM

To: info@kemptechnologies.com

```
Oct 22 19:42:16 KEMP2 logger: This is a test from the Load Master
```

Set SMTP Server

Enter the FQND or IP address of the mail server. If you are using FQDN please make sure to set the DNS Server.

Set Authorized User

Enter the username if your mail server requires authorization for mail delivery. This is not required if you mail server does not require authorization.

Set Authorized Users Password

Enter the password if your mail server requires authorization for mail delivery. This is not a required if you mail server does not require authorization.

Set Local Domain

Enter the top-level domain if your mail server is part of a domain. This is not a required parameter.

Connection Security

Select the type of security for the connection;

- None

- STARTTLS, if available
- STARTTLS
- SSL/TLS
-

Set Email Recipient

Enter the email address that correspond with the level or notification desired. Multiple email addresses are supported by a comma-separated list, such as:

INFO: info@kemptechnologies.com , sales@kemptechnologies.com

ERROR: support@kemptechnologies.com

17.13 Miscellaneous Options

17.13.1 Remote Access

Allow Remote SSH Access	<input checked="" type="checkbox"/>	Using: All Networks	Port: 22	<input type="button" value="Set Port"/>
		Disable SSH-V1 Prot <input checked="" type="checkbox"/>		
Allow Web Administrative Access	<input checked="" type="checkbox"/>	Using: eth0: 10.10.10.1	Port: 443	<input type="button" value="Set Port"/>
Administrative Default Gateway		<input type="button" value="Admin Default Gateway"/>		
Radius Server		<input type="button" value="Radius Server"/>	Shared Secret: <input type="text"/>	<input type="button" value="Set Secret"/>
Enable Hover Help	<input checked="" type="checkbox"/>			
Enforce Strict IP Routing	<input type="checkbox"/>			
Remote GEO LoadMaster Access		<input type="button" value="Set GEO LoadMaster access"/>		
GEO LoadMaster Port		22	<input type="button" value="Set GEO LoadMaster Port"/>	

Allow Remote SSH Access

You can limit the network from which clients can connect to the SSH administrative interface on LoadMaster.

Allow Web Administrative Access

This option allows you to assign the Interface address that will be hosting the Web User Interface access.

Administrative Default Gateway

When administering the LoadMaster from a non-default interface, this option allows the User to specify a different default gateway for administrative traffic only.

RADIUS Server

The address of the RADIUS server that is to be used to validate User access to the LoadMaster. To use RADIUS server you have to specify the shared secret.

Enable hover help

Enables blue hover notes shown when the pointer is held over a field.

Remote GEO LoadMaster Access

Set the addresses of the GEO LoadMasters that can retrieve service status information from this LoadMaster.

GEO LoadMaster Port

The port over which GEO LoadMasters will use to communicate with this LoadMaster unit.

17.14 L7 Configuration

Allow Connection Scaling over 64K Connections

Under very high load situations, Port Exhaustion can occur. Enabling this option will allow the setting of Alternate Source Addresses which can be used to expand the number of local ports available.

Allow connection scaling over 64K Connections	<input type="checkbox"/>
Always Check Persist	<input type="checkbox"/>
Add Port to Active Cookie	<input type="checkbox"/>
Conform to RFC	<input checked="" type="checkbox"/>
Close on Error	<input type="checkbox"/>
Add Via Header In Cache Responses	<input type="checkbox"/>
Real Servers are Local	<input type="checkbox"/>
Drop Connections on RS failure.	<input type="checkbox"/>
L7 Connection Drain Time (secs)	300 <input type="button" value="Set Time"/> (Valid values:60 - 86400)
Additional L7 Header	X-ClientSide <input type="button" value="v"/>
L7 Connection Timeout (secs)	660 <input type="button" value="Set Time"/> (Valid values:0, 60-86400)
100-Continue Handling	RFC Conformant <input type="button" value="v"/>

Always Check Persist

Override the default optimized behavior to only check persistence on initial TCP/IP connection.

Add Port to active Cookie

When using active cookies, the LM creates the cookie from (among other things) the IP address of the client. However if many clients are behind a proxy server, all clients all of those clients come from the same IP address. Turning this on adds the clients source port to the string as well. making it more random

Conform to RFC

This option addresses parsing the header of an HTTP request in conformance with RFC 1738

The request consists of 3 parts: GET /pathname HTTP/1.1 and when "conform" is on, the LoadMaster scans through the pathname until it finds a space. It then presumes that the next thing is HTTP/1.x. If the pathname contains spaces and the browser is conformant to the RFC, the pathname will have the spaces escaped to "%20" so the scan for a space will functions correctly.

However, on some broken browsers, spaces are not escaped and the wrong pathname is processed. And since the system can't find the HTTP/1.x, the LM will reject the request.

Turning off this feature, forces the LM to assume that the pathname extends to the last space on the line. It is then assumed that what follows is HTTP/1.x. So making pathnames with spaces in them useable – however, it is non-conformant to the RFC 1738.

Close on Error

If the LM has to send back a failure report to the client, for example a file is newer in the cache, this forces the LM to close the connection after sending the response. You can continue using the connection after sending a failure report, but some systems could become confused. This option forces the close instead of continuing

Add Via Header in Cache Responses

The relevant HTTP RFC, states that proxies should add a Via header to indicate that something came from the cache. Unfortunately older LM versions didn't do this. This switch is used to enable backward compatibility with older versions (if needed).

Real Servers are Local

The LM has an automatic detection of local / non-local clients for the purpose of transparency (selective transparency). This works well in most cases, BUT it doesn't work well if the client is actually a real server. Turning this on, helps the LM determine that an RS is actually local so making selective transparency work. You need an inverted kind of topology to even need to even think about it.



Do not enable this feature unless you have spoken with a KEMP engineer.

Drop Connections on RS Failure

This is useful for MS Outlook users whereby it closes the connection immediately if it detects that a Real Server has failed. Exchange users need this set by default when this version is installed (L7_TIMEOUT is also set to 86400 at the same time).

L7 Connection Drain Time (secs)

The number of seconds a persistence entry is permitted to override the disablement of a Real Server. Once a Real Server has been disabled, the drain timer starts. Existing clients with a valid persistence to this server will be permitted to return. Once the timer expires they will be scheduled to a new Real Server via the scheduling method. Connection drain does not pertain to deleted servers.

Additional L7 Header

This enables Layer 7 header injection for HTTP/HTTPS Virtual Services. Header injection can be set to X-ClientSide (KEMP LoadMaster specific) or X-Forwarded-For, or None. Refer to the Transparency Guide for an explanation of transparency and the value of header injection.

L7 Connection Timeout

The number of seconds that all Layer 7 Virtual Services can have no activity, the connection is closed after the timeout is reached.

100-Continue Handling

100-Continue processing is complicated. Depending on which MS http server version, different things need to be done with 100-Continue messages. If you look in the RFC, these messages are rather ambiguous, and Microsoft's implementation is even more mysterious (Only MS servers send out 100-Continue messages, everyone else doesn't need them). So depending on MS server version, you need to do different things when encountering a 100-Continue message from the RS.



Speak with a KEMP engineer. To understand how this may be configured.

17.14.1 Network Options

Enable SNAT	<input checked="" type="checkbox"/>
Enable Non-Local Real Servers	<input type="checkbox"/>
Enable Alternate GW support	<input type="checkbox"/>
Enable TCP Timestamps	<input type="checkbox"/>
Enable TCP Keepalives	<input type="checkbox"/>
Enable Reset on Close	<input type="checkbox"/>
Subnet Originating Requests	<input type="checkbox"/>

Enable SNAT

Enables translation..

Enable Non-Local Real Servers

Allow non-local Real Servers to be assigned to Virtual Services.

Enable Alternate GW support

Provides the ability to move the default gateway to a different interface.

Enable TCP Timestamps

The LoadMaster can include a timestamp in the SYN when connecting to Real Servers.



Enable this only upon request from KEMP support.

Enable TCP Keepalives

By default the TCP keepalives are enabled which improves the reliability of TCP connections that are long lived (SSH sessions). Keepalives are not usually required for normal HTTP/HTTPS services.



The keepalive messages are sent from the LoadMaster to the Real Server and to the Client. Therefore, if the Client is on a mobile network, there may be an issue with additional data traffic.

Enable Reset on Close

When enabled the LoadMaster will close its connection with the Real Servers by using RESET instead of the normal close handshake. This only makes a difference under highloads of many connections.

Subnet Origination Requests

When transparency is turned off for a Virtual Service, the source IP address of connections to the Real Servers is the Virtual Service. When enabled, and subnets are being used, the source IP address will be the subnet local address of the LoadMaster. If the Real Server is on a subnet, then the subnet address of the LoadMaster will be used.

17.15 AFE Configuration

Cache Configuration	
Maximum Cache Size	100 <input type="button" value="Set Size"/> (Valid values:1 - 101)
Cache Virtual Hosts	<input checked="" type="checkbox"/>
File extensions that should not be cached: .aspx .jsp .php .html	<input type="text"/> <input type="button" value="Add"/> No Entry <input type="button" value="Delete"/>
Compression Options	
File extensions that should not be compressed: .asf .gif .gz .jpeg .jpg .mov .mp3 .mp4 .mpe .mpeg .mpg .pdf .png .swf .tgz .wav .wma .wmv .z .zip	<input type="text"/> <input type="button" value="Add"/> No Entry <input type="button" value="Delete"/>
Intrusion Detection Options	
Detection Rules	<input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Install new Rules"/>
Detection level	Default - Only Critical problems are rejected <input type="button" value="v"/>
Client Limiting	
Client Connection Limiter	0 <input type="button" value="Set Limit"/> (Valid values:0 - 100000)

Maximum Cache Size

How much memory can be utilized by the cache in Mbytes.

Cache Virtual Hosts

When not enabled the cache presumes there is only one virtual host supported on the Real Server. Enabling this option allows the cache to support multiple virtual hosts which have different content.

File Extensions Not to Cache

A list of files types that should not be cached.

File Extensions Not to Compress

A list of file types that should not be compressed.

Intrusion Detection

Supports four levels of what to do when problems are encountered.

- **Low** – only logging with no rejection
- **Default** – only critical problems rejected
- **High** – Serious and critical problems rejected
- **Paranoid** – All detected problems rejected

Client limiting:

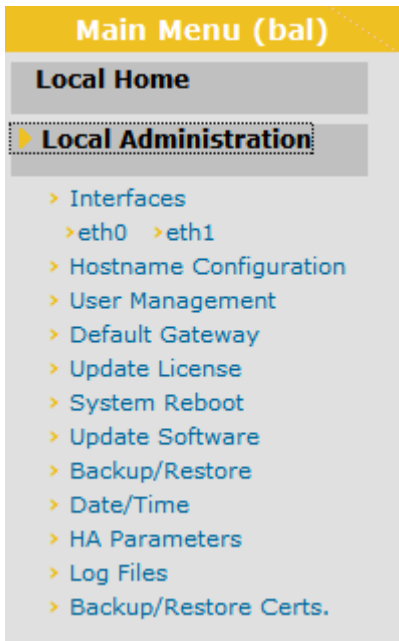
It is possible to set a limit of the number of connections per second from a given host. (limits up to 100K are allowed). After setting the "default limit" to a value the system allows you to set different limits for specific hosts / networks so you can limit a network and / or host.

If you set a network and a host on that network, the host should be placed first since the list is processed in the order that it is displayed.

17.16 HA Parameters

The role of the appliance can be changed by setting the HA Mode. Changing the HA Mode will require a reboot, once LoadMaster has rebooted, HA Parameter will appear provided the role is not “Non HA Mode”. HA will NOT work if both machines are specified the same.

When logged into the HA cluster, use the shared IP address to view and set full functionality to the pair. If you log into the direct IP address of either one of the devices the menu options are quite different (see menus below). Logging into one of the LoadMaster directly is usually reserved for maintenance.



Direct IP Menu



Shared IP Menu





HA Parameters	
HA Mode	HA (First) Mode ▾
HA version	Upgraded (carp) ▾
HA Timeout	9 Seconds ▾
HA Initial Wait Time	0 <input type="text"/> <input type="button" value="Set Delay"/> (Valid Values: 0, 10-180)
HA Virtual ID	1 <input type="text"/> <input type="button" value="Set Virtual ID"/> (Valid Values: 1-255)
Switch to Preferred Server	No Preferred Host ▾
HA Update Interface	eth0: ▾
Force Partner Update	<input type="button" value="Force Update"/>
Inter HA L4 TCP Connection Updates	<input type="checkbox"/>
Inter HA L7 Persistency Updates	<input type="checkbox"/>

HA Status

At the top of the screen, next to the date and time, icons are shown to denote the real-time status of the LoadMaster units in the cluster. There will be an icon for each unit in the cluster.



The four possible icons are:

Green		The unit is online and operational and the HA units are correctly paired.
Red/Yellow		The unit is not ready to take over. It may be offline or incorrectly paired.
Blue		The unit is pacified, i.e. it has rebooted more than 3 times in 5 minutes. In this state you can only access the machine via the direct machine WUI (not the shared WUI), and, it is not participating in any HA activity, i.e. no changes from the master will be received and it will not take over if the master fails.
Grey		Both machines are active, i.e. both are set to master, and something has gone seriously wrong. <i>CALL KEMP support.</i>

In HA mode each LoadMaster will have its own IP address used only for diagnostic purposes directly on the unit. The HA pair have a shared IP address over which the WUI is used to configure and manage the pair as a single entity.

HA Mode

If using a single LoadMaster, select Non-HA Mode. When setting up HA mode, one LoadMaster must be set to HA (First) and the other HA (Second). If they are both set to the same option, HA will not operate.



KEMP supplies a license that is HA enabled for each HA unit and specifies first or second unit. Therefore it is not recommended that you change this option until you have discussed the issue with KEMP Support.

HA Version

By default the system uses a version of VRRP (CARP - Common Address Redundancy Protocol) to check the status of the partner. The systems can also support the legacy heartbeat program. Changes to this option require both machines to be rebooted for the change to take effect.

HA Timeout

The time that the Master machine must be unavailable before a switchover occurs. With this option, the time it takes an HA cluster to detect a failure can be adjusted from 3 seconds to 15 seconds in 3 second increments. The default value is 9 seconds. A lower value will detect failures sooner, whereas a higher value gives better protection against a DOS attack.

HA Initial Wait Time

How long after the initial boot of a LoadMaster, before the machine decides that it should become active. If the partner machine is running, then this value is ignored. This value can be changed to mitigate the time taken for some intelligent switches to detect that the LoadMaster has started and to bring up the link

HA Virtual ID

When using multiple HA LoadMaster clusters on the same network, this value uniquely identifies each cluster so that there are no potential unwanted interactions.

Switch to Preferred Server

By default, neither partner in a HA cluster has priority. So that when a machine restarts after a switchover, the machine becomes the slave and stays in that state until forced to Master. Specifying a preferred host means that when this machine restarts, it will always try to become master and the partner will revert to slave mode.

HA Update Interface

The interface used to synchronize the HA information within the HA cluster.

Force Partner Update


Immediately forces the configuration from the active to standby unit without waiting for normal update.

Inter HA L4 TCP Connection Updates

When using L4 services, enabling updates will allow L4 connections to be maintained across a HA switchover. This option is ignored for L7 services.

Inter HA L7 Persistence Updates

When using L7 services, enabling this option will allow persistence information to be shared between the HA partners. If an HA failover occurs, the persistence information will not be lost. Enabling this option can have a significant performance impact.

 Both HA1 and HA2 must be on the same subnet with the same default gateway and be located within the same physical site. They must not be separated by an intra-site link and must use the same gateway to return traffic.

Appendix A. The LoadMaster Setup Questionnaire

Single LoadMaster Balancer Solution

Machine 1

Network side: eth0

IP Address

Netmask

Farm side: eth1

IP Address

Netmask

Hostname

Name Servers

(Space separated list)

Search Domains

(Space separated list)

Default Gateway

(IP Address)

Highly Available dual LoadMaster Balancer Solution

Machine 1

Machine 2

Network side: eth0

IP Address

Netmask

Shared IP address

Farm side: eth1

IP Address

Netmask

Shared IP address

Hostname

Name Servers

(Space separated list)

Search Domains

(Space separated list)

Default Gateway

(IP Address)

Appendix B: Loadmaster Console Operation

Quick Setup

You will need a PC to connect via COM+ (Console) port with a terminal emulation application, or a standard VGA and keyboard. Using a null modem cable (reversal) to connect the COM+ port to the LoadMaster COM port on the rear of the unit. The COM+ settings should 115200,8,N,1.

When you log into the LoadMaster for the first time and the license key has been validated the Quick Setup will start immediately.

Quick setup can also be accessed from the main configuration menu.

Quick setup allows a LoadMaster to be quickly configured; only the most important parameters needed by the LoadMaster are setup. Once the LoadMaster is configured and running, all the parameters can be changed using the Web User Interface.

Quick Setup welcomes you with the following message:

"This menu will allow you to quickly set up the LoadMaster. The first step is to set up the network interfaces, then the hostname(s) of your LoadMaster(s) and finally the default gateway and DNS parameters."

The Quick Setup procedure allows the configuration of the following parameters:

Ethernet IP address(s) – for eth0

Ethernet IP address(s) – for eth1

Hostname(s) – for local (and partner machine if running in a HA cluster)

DNS parameters

Domain parameters

Default Gateway

After these parameters have been set, the configuration should be activated. The

LoadMaster is then ready for work.

Note: If a parameter has been incorrectly set. Use the [CANCEL] button until the main menu appears. Quick Setup can then be performed again to correct the error.

Ethernet IP address(s) – eth0

The user is asked to input the IP address of the eth0 (NETWORK side) Ethernet interface. This should be input as a “dotted quad” followed by a network specifier.

I.e. 192.168.200.12/24

If no network specifier is given, the user will then be asked to specify the netmask, this may be input as either a network specifier (I.e. for the above example /24.) or as a “dotted quad” (I.e. If the IP address is 192.168.200.12 then the network mask should be 255.255.255.0).

When configuring a HA cluster, the shared IP address will then be requested. This must be on the same network as the primary IP address of eth0 (as previously configured).

Ethernet IP address(s) – eth1

The user will now be asked to input the IP address of the eth1 (FARM side) Ethernet interface. When running in a Single-Armed configuration, this entry should be left empty.

The format of the input is the same as used for eth0. If an address is given, then this must be on a different network to the address(s) on eth0.

Hostname

The hostname of the LoadMaster must now be set. A standard (or previously set) name is suggested.

When configuring a LoadMaster HA cluster, the name of the partner machine is requested, a standard name is also suggested here. This name also does not need to be changed unless the configuration requires it.

DNS configuration

The DNS resolver may now be configured. Up to three DNS servers may be specified (Addresses must be in “dotted quad” syntax).

A list of search domains can now also be given. Up to 6 domains can be specified.

Console Main Menu

Many features of the LoadMaster can be configured using the menu system. The menu system can be used by logging onto the console as “bal”, or by remotely logging into the system using the SSH protocol.

Important: Remote access is only permitted if the SSH service is enabled and the password for “bal” has been changed from its default value. If the password has not been changed from its default value, the user “bal” will only be allowed to login from a directly connected console.


Note: If the password for “bal” has been forgotten, a user can login on the console as *pwreset*. The password is *Ipwreset*, this will reset the password for “bal” to *lfourall* until the LoadMaster is rebooted. If unit is rebooted the password will be reset to its old (unknown) value. It is thus strongly advised that the password should be changed using the configuration menu before the next reboot.

Configuration Menu basics

The configuration menu system is made up of a number of hierarchical menus split into functional groups. Navigation around the menus can be performed by using the *Up* and *Down* cursor keys, or by using the “+” and “-“ keys. On menus with numeric entries, the number can also be given.

Example: To change the keyboard mapping, the user can type 3<CR> - which selects the “Local Administration” menu, followed by 3<CR> for “set keyboard map”.

Using “q”<CR> or “ESCAPE” or using the [CANCEL] button will return the user to the previous menu.

 To access the [OK], and [CANCEL] buttons, use the TAB key to toggle between the menu and the buttons.

Using the [CANCEL] button from the main menu, all changes made to the configuration will be ignored.

Using the [OK] button from the main menu performs the menu point, which is currently highlighted.

Important: When the LoadMaster is configured in a HA cluster, and the user is logged onto the standby machine, only the configuration of the local IP interfaces, changing the local password and performing a backup/restore should be performed, all other configuration parameters should only be changed on the active machine. From the main menu, the following options are available.

Quick Setup

This allows the user to quickly configure the basic parameters of the LoadMaster; these include the Ethernet IP addresses and local gateways and name servers.

See the section on “quick setup” in the initial configuration section.

Service Management (CLI)

This menu point starts a Command Line Interface (CLI), which lets the user administer the Virtual Services that are available on the LoadMaster. See Appendix C – ‘Command Line Interface’ for information on the syntax of the commands.

To leave the CLI, the user can type “exit”, or use the ESCAPE or CTRL-D keys.

In this version of the LoadMaster, the syntax of CLI commands has been changed. The original syntax may be selected using the menu option “Use MML format CLI” under Utilities -> Diagnostics.

Local Administration

This menu performs administration tasks for the current LoadMaster balancer. The following options are available:

Set Password

Using this option, the user may change the local password for the user “bal”. The password should be changed for security reasons. Remote access over SSH is not allowed until the password has been changed.

Important: The password is not saved when performing a backup and is not replaced when performing a restore.

If the LoadMaster is running in a HA (high availability) mode cluster. Each LoadMaster can have a separate password. The password information is not transferred between the members of a cluster.

Set Date/Time

This option allows the local date, time and time zone to be set.

A list of time zones is given; the current time zone is always at the start of the list. The user may select a different time zone it required.

The date should be entered in the following format:

02-12-03 (Year-Month-Day)

Followed by the time in the following format:

10:57:15 (Hours:Minutes:Seconds)

Note: When first delivered the LoadMaster is set to use UTC.

Set Keyboard Map

This option allows the keyboard mappings to be changed to support different languages.

A list of different keyboard mappings is supplied; the current mapping is always at the start of the list.

Note: The default keyboard mapping is US/ASCII.

Changes to keyboard mappings do not have any affect during an SSL session. Only after reconnection will the keyboard mappings be activated.

After a keyboard mapping has been selected, the user will be asked to check that the keyboard mapping is correct. If the keyboard mapping is not correct the [CANCEL] button should be pressed and a different mapping selected.

Backup/Restore

This option allows the configuration of the LoadMaster to be saved to either to a remote machine.

When using remote backup, the backup server machine must run an FTP daemon or an SSH daemon.

When performing a restore (from a remote machine), the user may select what information should be restored:

Only the Virtual Service configuration

Only the information about the Virtual Services will be restored.

Only the LoadMaster Base Configuration

Only the LoadMaster configuration not including the Virtual Service configuration.

Both the Virtual Service and Base Configuration information

All the configuration information on the LoadMaster.

Important: Restoring the Virtual Service Configuration on the standby LoadMaster of a HA cluster is not permitted since the Virtual Service configuration is always taken from the Active LoadMaster, and this would overwrite any restored configuration.

Remote Access Control

This option allows the user to enable or disable remote access to the LoadMaster.

Enable/Disable Remote SSH access

This option allows enables or disables access to the LoadMaster via the SSH protocol. If this option is disabled, the menus can only be accessed via the local console. If no password has been specified for “bal”, it is not possible to log in via SSH.

Enable/Disable Remote Web access

This option enables or disables access to the Web user interface.

Change Web Address

The LoadMaster is delivered with the Web user interface configured to be only accessible via the “network” side address. With this option, the Web user interface can be configured to be accessible from only a “farm” side address.

Administrative Default Gateway

You can route traffic for Web User Interface access to a specific gateway device, this overrides the global appliance gateway for only WUI traffic.

Enable Hover Help

Disable or enable inline over help in the Web User Interface.

Basic Setup

This menu allows the user to perform each of the steps in the “quick setup” separately.

Network configuration

The configuration of the various IP addresses of the Ethernet interfaces can be configured.

When using the LoadMaster in a one-armed configuration, the second interface does not have to be configured. When asked to configure the second interface (eth1) just press the [OK] button with no IP address supplied.

If the LoadMaster is supplied with extra optional Ethernet interfaces, these interfaces can only be configured using this menu. In this case, the on-board interfaces are no longer eth0 and eth1 but the highest numbered Ethernet interfaces. I.e. the optional interfaces will be designated as eth0 and eth1. For more information on this topic please contact customer support.

Hostname Configuration

The hostname of the LoadMaster can be changed. When the system is configured as a HA cluster, the hostname of the partner LoadMaster can also be changed.

 It is not required to change the name of the LoadMaster unless there are multiple HA clusters on the same broadcast network (Ethernet segment).

DNS configuration

This option allows the configuration of the LoadMaster name resolution facility. If no DNS parameters are specified, the administration of the LoadMaster must be performed using “dotted quad” addressing only.

This option allows the configuration of up to three DNS server addresses. These must be in “dotted quad” format.

Up to 6 search domains may also be specified.

Routing Configuration

This option permits the configuration of default and static routes.

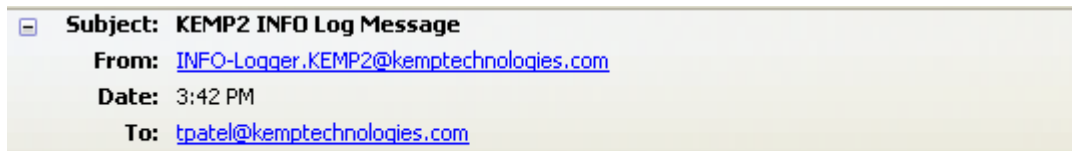
The LoadMaster requires a default gateway through which it can communicate with the Internet. See the “Application Guide” section for more information on this subject.

Other routes can also be specified using this menu. These routes are static and the gateways must be on the same network as the LoadMaster.

Email Configuration

This option permits the configuration of email alerting for LoadMaster events. Email notification can be delivered for six predefined informational levels. Each level can have a distinct email address and each level supports multiple email recipients. Email alerting depends on a mail server, support for both an open relay mail server and a secure mail server is provided. Testing email configuration can be done using the Web User Interface and navigating to System Configuration -> System Administration -> Logging Options -> Email Options

Sample Email Alert:



Oct 22 19:42:16 KEMP2 logger: This is a test from the Load Master

Set SMTP Server

Enter the FQND or IP address of the mail server. If you are using FQDN please make sure to set the DNS Server.

Set Authorized User

Enter the username if your mail server requires authorization for mail delivery. This is not required if you mail server does not require authorization.

Set Authorized Users Password

Enter the password if your mail server requires authorization for mail delivery. This is not required if you mail server does not require authorization.

Set Local Domain

Enter the top-level domain if your mail server is part of a domain. This is not a required parameter.

Set Email Recipient

Enter the email address that correspond with the level or notification desired. Multiple emails are support by a comma-separated list. Ex) support@kemptechnologies.com, info@kemptechnologies.com

Enable L7 Transparency

This is a global configuration that makes **ALL** Layer 7 Virtual Services transparent.

Use X-ClientSide or X-Forwarded-For Header

This enables Layer 7 header injection for HTTP/HTTPS Virtual Services. Header injection can be set to X-ClientSide or X-Forwarded-For Refer to the Transparency Guide for an explanation of transparency and the value of header injection. Header injection requires a Layer 7 persistence or content switching enabled. A custom header parameter and value can be injected on a per Virtual Service level to identify which Virtual Service sent the request to the web server.

Support VS Originating Requests

This option is used when deploying LoadMaster using the “Additional Subnets on this Interface” feature. When creating a non-transparent Virtual Service you can translate the source IP address to either the Virtual Service IP address or the “Local Address” configured on the additional subnet.

Note: Enabling this feature requires a reboot to take effect..

Extended Configuration

This menu allows the user to configure several features, which do not directly affect the main function of the LoadMaster but makes the LoadMaster easier to use.

Interface Control

This option allows the configuration of the protocol used at the physical level on the Ethernet. Normally, the LoadMaster will auto detect (auto-negotiation) which Ethernet protocol it should use. Sometimes this process does not always work. With this option, the user may force the LoadMaster to use a specific protocol (either 100Mb Full or Half Duplex).

Note: If the LoadMaster is connected to a 10Mbit switch, then auto detect **MUST** be used.

Enable/Disable S-NAT

This toggle option will either enable or disable the S-NAT functionality of the LoadMaster.

When S-NAT is enabled, the Real Servers can access the Internet using the LoadMaster as a gateway. The LoadMaster will use “masquerading” so that connection requests from the Real Servers seem to originate on the LoadMaster. This means that the Real Servers can be on a private network and still have access to the Internet.

When S-NAT is disabled, the LoadMaster will not perform “masquerading” and so the Real Servers cannot access the Internet through the LoadMaster.

In Single-Armed configurations, S-NAT does not provide any extra functionality.

Syslog Configuration

With this option, log messages may be sent to different hosts using the syslog protocol.

A different host may be specified for each of six different levels:

INFO	This host will receive all messages from the LoadMaster.
NOTICE	This host will receive all messages from the LoadMaster except INFO.
WARN	This host will receive all messages except NOTICE level messages.

ERROR This host will receive all messages except WARN and NOTICE level messages. I.e. It will receive ERROR, CRITICAL and EMERGENCY messages.

CRITICAL This host will receive only CRITICAL and EMERGENCY messages.

EMERGENCY This host will receive only EMERGENCY messages.

SNMP metrics

With this menu, the SNMP configuration can be modified. For more information on SNMP please see the Application Guide.

Enable/Disable SNMP metrics

This toggle option, enables or disables SNMP metrics. I.e. This option allows the LoadMaster to respond to SNMP requests.

Note: By default SNMP is disabled.

Configure SNMP Clients

With this option, the user can specify from which SNMP management hosts the LoadMaster will respond to.

Important: If no client has been specified, the LoadMaster will respond to SNMP management requests from **any** host.

Configure SNMP Community String

This option allows the SNMP community string to be changed. The default value is “public”.

Configure SNMP Contact

This option allows the SNMP Contact string to be changed. For example, this could be e-mail address of the administrator of the LoadMaster.

Configure SNMP Location

This option allows the SNMP location string to be changed.

SNMP traps

When an important event happens to a LoadMaster a Virtual Service or to a Real Server, a trap is generated. These are sent to the SNMP trap sinks.

Enable/Disable SNMP Traps

This toggle option enables and disables the sending of SNMP traps.

Note: SNMP traps are disabled by default.

Configure SNMP Trap Sink1

This option allows the user to specify a list of hosts to which a SNMPv1 trap will be sent when a trap is generated.

Configure SNMP Trap Sink2

This option allows the user to specify a list of hosts to which a SNMPv2 trap will be sent when a trap is generated.

Enable/Disable L7 persistency state failover

Note: This feature is only available on a HA cluster configuration

When an L7 persistency option has been enabled, the active LoadMaster will automatically send connection information to the standby machine so that if the active machine fails, the standby machine

can take over the processing of requests as if nothing had happened. The connection information is sent using a Multicast protocol. The parameters for this may be changed under “Multicast Configuration”.

This toggle option will either enable or disable the transfer of L7 connection information. If this feature takes too much bandwidth or is not required, then it may be safely disabled.

Enable/Disable L4 connection state failover

Note: This feature is only available on a HA cluster configuration

When a Virtual Service is not using persistency or only IP source address persistency, the active LoadMaster will automatically send connection information to the standby machine so that if the active machine fails, the standby machine can take over the processing of requests as if nothing had happened. The connection information is sent using a Multicast protocol. Only the Ethernet interface parameter under “Multicast Configuration” has any affect on this option.

This toggle option will either enable or disable the transfer of L4 connection information. If this feature takes too much bandwidth or is not required, then it may be safely disabled.

HA Parameters

These configuration options enable you to control the behavior of the Highly Available pair of LoadMasters. Its is important that these changes be made using the shared IP so that changes are synchronized to the standby unit. The individual roles (HA-1 or HA-2) of the appliances can be changed using only the Web User Interface.

Note: These options are only available on a HA cluster configuration which can be enabled in the Web User Interface by navigating to System Configuration -> System Administration -> Miscellaneous Options -> HA Parameters

HA Timeout

With this option, the time it takes a HA cluster to detect a failure can be adjusted. A value between and 1 and 5 can be set. The default value is 1. A lower value will detect failures sooner, while a higher value gives better protection against a DOS attack.

HA Wait Timeout

The time it takes the LoadMaster at Boot time to determine if the partner is NOT available. If the partner is available, then this value is ignored. The value can between 31 and 180. A smaller value gives quicker boot times when the partner is not available. A higher value helps protect against both machines becoming active. A value of zero uses the system default.

HA Update Interface

This option permits you to decide which interface will be used for LoadMaster intercommunication. This interface uses multicast for HA communication.

HA Initial Network Checks

This option informs LoadMaster to perform extra boot time network validations. In general this is not required and should be disabled.

HA Preferred Host

This option allows you to decide in advance which appliance in a HA pair should take the active role when both appliances are healthy. When a failover occurs and the failing appliance returns to a healthy state, active status can be transferred back by setting a preferred host. If no preferred host is set then the active role will transfer during failover to the standby unit. The standby unit will remain active even when the failed partner is brought back online.

HA Virtual ID

The value can be between 1 and 5. Only change this value if you have multiple HA clusters on the same subnet. Each HA pair on the same subnet must have a different ID.

Packet Filter & Access Control Lists

Access control Lists

The LoadMaster supports a “blacklist” Access Control List system. Any host or network entered into the Access Control List will be blocked from accessing any service provided by the LoadMaster.

The LoadMaster also has a packet filter. When enabled the packet filter blocks all IP packets which are not directed at a configured port.

The Access Control list is only enabled when the packet filter is enabled. By default the Access Control List is disabled. This means that all source IP addresses are accepted by the LoadMaster.

Enable Access Control Lists

Using this toggle option the Packet Filter/Access Control List can be activated / deactivated.

Show ACL

This option lists the content of the current Access Control List.

Add address to ACL

This option allows a user to add a host or network IP address to the Access Control List. Only “dotted-quad” IP addresses are allowed. A network is specified by using a network specifier.

I.e. Specifying 192.168.200.0/24 will block all hosts on the 192.168.200 network.

Delete address from ACL

This option allows an IP address or network to be deleted from the Access Control List.

Reject/Drop blocked packets

When a connection request is received from a host, which is blocked using the ACL, the request is normally ignored (dropped). The LoadMaster may however be configured to send back an ICMP reject packet. For security reasons it is usually best to drop any blocked requests.

Utilities

Software Upgrade

Using this option, patches for the operating software of the LoadMaster may be installed or removed.

Install Update

With this option, a patch can be downloaded onto the LoadMaster from a remote server. The server must be running a SSH daemon.

Once the patch has been downloaded, the patch is unpacked and verified. If the patch is valid, then the name of the patch will be displayed and the user will be asked to confirm if the patch should be installed. A copy of the current operating software is saved before the patch is installed, this may be recovered at a later date using the “rollback update” option.

Rollback Update

If a patch needs to be removed, this option allows the previous version of the operating software to be recovered. Only one previous version is available. When the software has been recovered, it is not possible to recover any earlier versions.

Factory Reset

Reset the configuration of the appliance with exception to the license information and usernames and passwords.

Transfer mode

This option allows the user to specify which transfer method should be used to transfer data between the LoadMaster and a remote server. The selected method is used to store a backup on a remote server or to download software patches. The default method is “ftp”.

Use ftp protocol

Using this option, the Internet standard “ftp” protocol is used. Most servers support this protocol.

Use scp protocol

The “scp” - secure copy – transfer method may be selected. This is more secure than “ftp” but is normally only supported on UNIX servers. If this mode is selected, the transfer of SSL certificates can only be performed via the menu system and not via the Web interface.

Use http protocol

Using this transfer method, backups to a remote server cannot be performed.

Software patches can however be downloaded from any Web server where the patch has been made available.

Network Time Protocol Host

The time on the LoadMaster can be synchronized to an NTP server. The time will be synchronized at boot time and every then on an hourly basis. Using this option, the address of the NTP server can be specified.

SSL certificate administration

This option permits the administration of currently installed SSL certificates. A list of Virtual Services, which have SSL acceleration enabled, is given. Selecting a Virtual Service allows the certificates for the service to be managed. Selecting the local option allows the certificate used for the Web interface to be regenerated.

Get a certificate file

This option allows the user to download a certificate file for the Virtual Service.

Note: the SCP protocol may be used to transfer certificate files.

Get a key file

This option allows the user to download a private key file for the Virtual Service. If a private key is included in the certificate file, no additional private key file is required.

Delete the key and certificate files

Allows the user to delete a certificate and key file for a specific Virtual Service.

Update License

This option permits the input of a new license key. I.e. when updating from an evaluation to a full license.

Diagnostics

This menu allows the user to perform diagnostic functions on the LoadMaster.

Ping Remote Host

A remote host may be “pinged.”

Enable Diagnostic login

Important: The option “Enable diagnostic login” should only ever be enabled when requested to by LoadMaster support staff.

If this option is enabled in normal operation, this may result in unauthorized access to the LoadMaster. The diagnostic login will be disabled upon reboot of the LoadMaster or it can be disabled from this menu.

Show Partner IP Address

If the LoadMaster is being used in a HA configuration and the real addresses of either partner is changed, it can cause both LoadMasters to no longer communicate with each other. This option allows the changing of the partners IP address so that communication can be restored.

Reboot

This option will reboot the LoadMaster. All modifications to the configuration will be saved before the reboot.

Note: When running on the active machine of a HA cluster, the configuration on the standby machine will also be updated before the standby machine becomes the active machine (Since the active machine is being rebooted).

Exit LoadMaster Config

This option allows the user to leave the configuration menu system.

If any parameters have been changed, the user will be asked if they want to activate the changes. If this is confirmed, then the changes are activated. If the user does not want to activate the changes, the user will be asked if they want to save the changes for a later activation. If this is NOT confirmed, all changes will be lost. **Appendix C. Command Line Interface (CLI) Reference Guide**

The command interface syntax is loosely based on the industry standard syntax as used by other Load Balancer manufacturers.

The command interface has a line based, hierarchical command set. Changes made to the configuration are only performed when returning to the top level.



A port can either be specified as a numeric value or as a symbolic name. The following names are recognized:

DNS	53
FTP	21
HTTP	80
IMAP4	143
LDAP	389
POP2	109
POP3	110
SMTP	25
SNMP	161
SSL	

TELNET	23
TFTP	69

Top level commands

At the top level the following commands may be specified.

Adaptive

This command switches the input to the adaptive parameters command set.

Delete <name|VIP>

This command will delete the specified VIP.

Disable_rs <IPspec>

This command will disable the specified Real Server. I.e. No more traffic will be directed to the Real Server. This command will disable the Real Server on all Virtual Services where this Real Server is configured.

Enable_rs <IPspec>

This command will re-enable the specified Real Server. The Real Server will be re-enabled for all Virtual Services.

Health check

This command switches the input to the health check parameter command set.

Rules

This command switches the input to the rule configuration command set. Rules are only available if the L7 option has been activated.

Show <name|VIP>

This command will display all information about the given Virtual Service. If no Virtual Service is specified, information about all Virtual Services will be displayed.

Vip <name|VIP>

This command switches the input to the Virtual Service command set. A <VIP> is the IP address of the Virtual Service. A <name> is the name of the Virtual Service.

If no Virtual Service with the specified IP address (or IP name respectively), then a new Virtual Service will be created. No changes will occur to the configuration until the user returns to the top level command level..9 Help

Prints a summary of commands at the current level.

End

Terminate the CLI session.

Exit

Since the input level is at the top level, this command has no affect.

Adaptive scheduling command level

The following commands are available at the adaptive command level. No changes to the configuration will occur until the command level returns to the top level i.e. when the user types “exit”.

Interval <Integer>

With this command, the interval of sampling the server loads will be set to <Integer> seconds.

Min <Integer>

The minimum load (as a percentage) where adaptive balancing takes effect can be set.

If the mean load of the server falls below this threshold, the Virtual Service will be considered "idle" and the weights will return gradually to their "static" values.

Port <PortSpec>

The specified port will be used to access the Real Servers where adaptive checking is enabled.

Show

Displays the current adaptive checking parameters.

Url <String>

<String> specifies a URL, which will be fetched by the adaptive checking system. The contents of this URL should specify the load on the current Real Server, with 0 representing no load and 100 representing a fully loaded server.

For further information regarding Adaptive Balancing, please refer to **Appendix G: Headers Added by LoadMaster When 'Client Certificates and Add Headers' Option is Selected**

When the Client Certificates and add Headers option is selected in the Client Certificates drop-down while enabling SSL Acceleration, a number of headers are added. The following list describes the headers that are added to the https request by LoadMaster.

```
SSL_CLIENT_A_KEY="rsaEncryption"
SSL_CLIENT_A_SIG="md5WithRSAEncryption"
SSL_CLIENT_I_DN="/C=US/ST=Administrator/L=Limerick, Ireland/O=Kemp
Technologies/OU=Mary Rosse House/CN=MMC CA"
SSL_CLIENT_I_DN_C="US"
SSL_CLIENT_I_DN_CN="MMC CA"
SSL_CLIENT_I_DN_L=" Limerick, Ireland "
SSL_CLIENT_I_DN_O=" Kemp Technologies "
SSL_CLIENT_I_DN_OU=" Mary Rosse House "
SSL_CLIENT_I_DN_ST="Administrator"
SSL_CLIENT_M_SERIAL="05"
SSL_CLIENT_M_VERSION="3"
SSL_CLIENT_S_DN="/C=US/O= Kemp Technologies /OU= Mary Rosse House
/ST=Administrator/L= Limerick, Ireland /0.9.2342.19200300.100.1.1=jar/CN=Kemp
Sales/Email=sales@kemptechnologies.com"
SSL_CLIENT_S_DN_C="US"
SSL_CLIENT_S_DN_CN="Kemp Sales"
SSL_CLIENT_S_DN_Email="sales@kemptechnologies.com"
SSL_CLIENT_S_DN_L="Limerick, Ireland "
SSL_CLIENT_S_DN_O="Kemp Technologies "
SSL_CLIENT_S_DN_OU="Mary Rosse House "
SSL_CLIENT_S_DN_ST="Administrator"
SSL_CLIENT_VERIFY="SUCCESS"
SSL_CLIENT_V_END="Jan 16 14:30:35 2005 GMT"
SSL_CLIENT_V_START="Jan 18 14:30:35 2000 GMT"
```

```
SSL_SERVER_A_KEY="rsaEncryption"
SSL_SERVER_A_SIG="md5WithRSAEncryption"
```

```
SSL_SERVER_I_DN="/C=US/ST=Administrator/L=Limerick, Ireland/O=Kemp
Technologies/OU=Mary Rosse House/CN=MMC CA"
SSL_SERVER_I_DN_C="US"
SSL_SERVER_I_DN_CN="MMC CA"
SSL_SERVER_I_DN_L=" Limerick, Ireland "
SSL_SERVER_I_DN_O=" Kemp Technologies "
SSL_SERVER_I_DN_OU=" Mary Rosse House "
SSL_SERVER_I_DN_ST="Administrator"
SSL_SERVER_M_SERIAL="05"
SSL_SERVER_M_VERSION="3"
SSL_SERVER_S_DN="/C=US/O= Kemp Technologies /OU= Mary Rosse House
/ST=Administrator/L= Limerick, Ireland /0.9.2342.19200300.100.1.1=jar/CN=Kemp
Sales/Email=sales@kemptechnologies.com"
SSL_SERVER_S_DN_C="US"
SSL_SERVER_S_DN_CN="Kemp Sales"
SSL_SERVER_S_DN_Email="sales@kemptechnologies.com"
SSL_SERVER_S_DN_L="Limerick, Ireland "
SSL_SERVER_S_DN_O="Kemp Technologies "
SSL_SERVER_S_DN_OU="Mary Rosse House "
SSL_SERVER_S_DN_ST="Administrator"
SSL_SERVER_VERIFY="SUCCESS"
SSL_SERVER_V_END="Jan 16 14:30:35 2005 GMT"
SSL_SERVER_V_START="Jan 18 14:30:35 2000 GMT"
```

Appendix H: API for Agent Based Adaptive Balancing.

Weight <Integer>

This specifies the minimal value of the weight (as a percentage of the static weight).

The adaptive scheduling method will not adjust a server weight below this value.

Help

Prints out a list of the available commands at the adaptive command level.

End

Terminates the CLI session. No changes performed after entering this level will be saved.

Exit

Returns the input to the top command level. Any changes will be written to the configuration file, and the system will be updated accordingly.

Health check command level

The following commands can be performed at the health check command level.

Interval <Integer>

Specifies how often the health of a Real Server should be checked.

Retry <Integer>

Specifies how often the health check of a Real Server should fail before the LoadMaster decides that the Real Server is no longer responding.

Show

Displays the current health check parameters.

Timeout <Integer>

Specifies how long the LoadMaster should wait for a response from a Real Server. The LoadMaster will mark a Real Server as down after Timeout * Retry seconds if no response has been received.

Help

Lists the commands that are available at the health check command level.

End

Terminate the CLI session. Any changes since entering the health check command level will be ignored.

Exit

Leave the health check command level, any changes to the health check parameters will be saved and the system will be configured accordingly.

Rules command level

The following commands can be performed at the rules command level.

Add <Rule-name>

This command creates a new rule <Rule-name>. It also switches into the Rule Edit command level. Upon return to the Rules command level. Further rules may be added.

A rule must be added before a Real Server can use it.

Modify <Rule-name>

This command switches into the Rule Edit command level, so that the rule <Rule-name> can be edited.

Delete <Rule-name>

This deletes the specified rule. The rule will be deleted from all Real Servers to which it has been assigned.

Show [<Rule-name>]

Displays a list of all the rules (if no <Rule-name> parameter) is specified or the specified rule.

Help

Lists the commands that are available at the rules command level.

End

Terminate the CLI session. Any changes since entering the health check command level will be ignored.

Exit

Leave the rules command level, any changes to the rules will be saved and the system will be configured accordingly.

Rule Edit command level

The following commands can be performed at the rule edit command level.

value <string>

This option allows the match string value of the rule to be set. Spaces are significant. By default a string is treated as a regular expression. If <prefix> or <postfix> is set, then the string is treated as a literal string, which is then matched at the start or end of the received URL respectively.

[no] negation

This command inverts (reverts to normal if [no] is specified) the sense of a rule. I.e. If negation is set, the rule will be true if the received URL does NOT match the value of the rule.

[no] prefix

This specifies that the value of the rule should be matched at the start of the received URL.

[no] postfix

This specifies that the value of the rule should be matched at the end of the received URL.

[no] regex+host

This specifies that the value of the rule should be matched against the concatenated hostname and received URL string.

[no] prefix+host

This specifies that the value of the rule should be matched at the start of the concatenated hostname and received URL string.

[no] postfix+host

This specifies that the value of the rule should be matched at the end of the concatenated hostname and received URL string.

Note: If no prefix or postfix option is enabled, the default rule matching will be a regular expression. Specifying **no** to any of the above options reverts the matching back to regular expression matching without any hostname concatenations.

Show

Displays the value of the current rule.

Help

Lists the commands that are available at the rule edit command level.

End

Terminate the CLI session. Any changes since entering the rules command level will be ignored.

Exit

Leave the rule edit command level and return to the rules command level. Modifications will not be saved until after the rules command level is “exited”.

Virtual Service (VIP) command level

The following commands are available at the Virtual Service command level. No changes will be made to the system until the user performs an “exit” from this level. If the VIP has errors, the user will be asked if the VIP should be discarded. If the VIP is discarded, the input will return to the top level. If the VIP is not discarded, the input will remain at the Virtual Service command level, the user may then correct the error.

[no] Adaptive <String>

Specifies whether the Virtual Service should support adaptive health checking. The only current method is “http_rs”. To disable adaptive health checking for a Virtual Service, the command <no adaptive> should be used.

Add <IPspec>

This command adds the Real Server as specified by the <IPspec> to the Virtual Service. It also switches the input into the Real Server command level. Upon return from the Real Server command level, further Real Servers can be added to the Virtual Service.

Address <IPspec>

Specifies the IP address of the Virtual Service.

Delete <IPspec>

Deletes a Real Server as specified by <IPspec> from the Virtual Service. A Virtual Service must have at least one Real Server.

Disable

Disable the Virtual Service. This means that the Virtual Service will accept no new requests.

Enable

Re-enable a Virtual Service. The Virtual Service will again accept new requests.

Follow <Port Spec>

This command only works if the L7 option of the LoadMaster has been enabled. This specifies

Mask <Ipmask>

When using L4 (source IP based persistency), An IP mask may be specified which is used to determine if two IP addresses should be treated as coming from the same source. By default the mask has a value of 255.255.255.255, which means that all IP addresses are different.

10 [no] Name <Name>

Specifies the “name” of the Virtual Service. To delete the name use the command <no name>.

11 Healthcheck <String>

This specifies which health-check method should be used for a given Virtual Service. If the Virtual Service has a well-known port, a health check method will be automatically set. The following health check methods may be specified.

http	Http checking is enabled
https	Https (SSL) checking is enabled
smtp	The (simple mail transfer protocol) is used.
nntp	The (network news transfer protocol) is used.
ftp	The (file transfer protocol) is used.
telnet	The (telnet protocol) is used.
pop3	The (post office – mail client protocol) is used.
imap	The (imap – mail client protocol) is used.
tcp	A basic TCP connection is checked.
dns	A DNS request is sent to the Real Servers port. This checking method is only valid when using a UDP protocol.
udp	A dummy zero length UDP packet is sent to the port.
icmp	An ICMP ping is sent to the Real Server.

[no] Persist <Persist type>

This command specifies which type of connection persistence should be used for a Virtual Service. In no persistency should be specified for the Virtual Service, the command <no persist> should be specified. The following persistency types can be specified. If the L7 option has not been enabled, only the <src> persistency is allowed.

ssl The Session ID in an SSL connection is used to maintain client to Real Server persistency.

cookie Server generated cookies will be used.

active-cookie LoadMaster generated cookies will be used.

url A request for a specific URL will always go to the same Real Server.

host A request to the same virtual host will go to the same Real Server.

src Enables IP based persistency.

cookie- src Server generated cookies will be used. If the client does not return a cookie, the clients' IP address will be used.

active- cook-src A LoadMaster generated cookie will be used. If the client does not return the cookie, the clients' IP address will be used.

cookie- hash All connections with the same set of cookies will always be sent to the same Real Server. If no cookies are sent, normal scheduling will occur.

Port <Port spec>

Specifies the IP port to be used for the Virtual Service. If no health check mechanism has been specified and the port is a well-known port, the relevant health check mechanism will be selected.

Precedence <rule-name> <number>

The precedence of the rule <rule-name> is set to <number>. A value of 1 moves the rule to the start of the rule list. I.e. this rule is checked first. A higher value moves the rule to the respective position in the rule. If a <default> rule is specified for a Real Server, its precedence will always be lower than any user defined rules. I.e. a <default> rule will always be checked after every other rule.

Protocol <tcp/udp>

Protocol to be used for the Virtual Service. This may be <tcp> or <udp>. By default the protocol will be set to <tcp>.

Ptimeout <Integer>

Specifies how long the LoadMaster should remember the persistency information associated with a connection. This value is specified in seconds.

Schedule <schedule method>

This allows the scheduling method between the Real Servers to be specified.

The following scheduling methods may be specified:

rr round robin (default).

wrr weighted round robin.

lc least connection.

llc weighted least connection.

Server <IPspec>

This command enters the Real Server command level for the specified Real Server.

The Real Server must already be assigned to the Virtual Service.

cache

Enable caching

compress

Enable compression

urlverify

Enable IPS

dfltgw

Configure the VS default gateway

Show

Displays all the parameters of the current Virtual Service.

Help

Prints out a list of commands at the Virtual Service command level.

End

Terminate the CLI session. No changes made in the Virtual Service command level (or lower) will be saved.

Exit

Return the input to the top level. Any changes to the Virtual Service will be saved. If an error is detected in the Virtual Service, the system reports the error and asks if the Virtual Service should be discarded. If the Virtual Service is not discarded, the input remains at the Virtual Service level, where any corrections may be made.

Real Server command level

At this command level, a specific Real Server may be configured. The following commands are available at this level.

Addrule <Rule-name>

This command adds the rule <Rule-name> to a Real Server. If this is the first assignment of <Rule-name> to a Real Server on the current Virtual Service, the rule will be placed on the precedence list as the lowest user defined rule I.e. checked after all other rules. Use the Virtual Service command Precedence to change the precedence order.

Delrule <Rule-name>

This command removes the association of rule <Rule-name> from the Real Server. If there are no more instances of the rule associated with the Virtual Service, the rule will be deleted from the Virtual Service precedence list.

Disable

Disables the current Real Server. The Real Server will only be disabled in the current Virtual Service. If the Real Server is accessed via a different Virtual Service, then this Virtual Service will not be affected.

Enable

Re-enable the current Real Server on this Virtual Service. If the Real Server has been disabled on multiple Virtual Services, these Virtual Services will not be affected.

Forward <forwarding method>

This specifies the forwarding method, which should be used to access the Real Service.

This can be either <nat> or <route>. By default the forwarding method is <nat>, <route> should only be selected when using “direct service return”.

Port <portspec>

Specifies which port on the Real Server should be used. If no port is specified, then the port from the Virtual Service will be used.

Show

Display the parameters for the current Real Server.

Weight <integer>

Specifies the weighting for the Real Server. This can be used when using the various scheduling methods that utilize the weighting of a Real Server.

Help

Lists the commands at this level.

End

Terminate the CLI session. No changes made in the VIP and Real Server command levels will be saved.

Exit

Return to the Virtual Service command level. No changes will be saved until the editing of the current Virtual Service has been completed.

Appendix D. Example of a Content Rule

One way to redirect the root of a webserver. Below is the new text for the copy paste.

Brief explanation: the regex is '^/\$' which matches '/' and only '/' - When you negate this rule, it allows EVERYTHING except '/' (the root). The request will then slip thru the cracks and hit the redirect.

==Redirect for Webserver Root==

Typically, this is better to configure this sort of redirect on your Real Servers, however you can utilize Content Switching to get the same result.

- 1) Create a rule in Rules & Checking > Content Rules
- 2) Use the following settings for your rule
Rule Name: Redirect_Root
Rule Type: Content Matching
Match Type: Regular Expression
Match String: ^/\$
- 3) Navigate to your Virtual Service
- 4) Turn on Content Switching under Advanced Properties
- 5) Apply the Redirect_Root rule to each of your Real Servers
- 6) Configure your Not Available Redirection Handling
Error Code: 302 Found
Redirect URL: <http://%h/<directory>>

Since there is no longer any Real Server to handle cases which do not match the rule, they are handled by the redirection. This means that ANY request to a URL which does not start with the string specified in the rule will be redirected.

If you have multiple directories which are allowed, you must repeat the process for each directory.

Appendix E. Error Codes

Following is a list of commonly encountered error codes for the LoadMaster.

General Messages

- **printk**

The `kernel: printk: x messages suppressed` are messages that the previous message was repeated x times (this conserves space in the log files). This message is not a problem on it's own. If there are no other messages in the logs which indicate a problem, then there is nothing to worry about.

- **l4d: HTTP/1.1 Checker: RS x.x.x.x:80 Host:y.y.y.y connection closing!**

When using HTTP/1.1, the host should not close the connection at the end of each request. This warning is displayed when the response to the checker request indicates that the host closed the connection. It is not really an error, but an indication that the RS could be better configured.

- **L7: RS Failed (x.x.x.x:p:y.y.y.y:p) - Dropping persist**

This message occurs while trying to connect a persisting connection to an RS. If it discovers that the RS is down, the persist information is considered invalid - it should be cleaned out and dropped. The service will then perform normal scheduling for the new connection.

- **CPU0 not a capable Intel processor**

With regard to the 'microcode: CPU0 not a capable intel processor' message this is a normal operation. The LM-[____] has a VIA chip and not an Intel CPU so this is expected. As our firmware runs on a variety of hardware platforms, this is part of the detection stage of bootup. That message is completely normal for a LM-[____].

- **VIA PadLock not detected.==**

With regard to the 'padlock: VIA PadLock not detected.' message this is a normal operation. The LM-[____] has an Intel CPU and not a VIA chip so this is expected. As our firmware runs on a variety of hardware platforms, this is part of the detection stage of bootup. That message is completely normal for a LM-[____].

- **L4d: HTTP/1.1 Checker - Connection Closing==**

l4d: HTTP/1.1 Checker: RS <RS IP>:<PORT> Host: <VS> connection closing!

Those messages are indicative that you have HTTP 1.1 healthchecks turned on, but you have KeepAlive turned off on your Real Server. The LoadMaster is simply making note of the fact that it is receiving 'Connection: close' from the Real Server. These are purely informational messages and do not indicate any sort of failure or malfunction.

- **/usr/sbin/cron: (root) MAIL (mailed 55 bytes of output but got status 0x0001)==**

This message is generated by an internal process, it doesn't have any bearing on the performance of the LoadMaster. This message will be addressed and removed in a future release of the firmware. It doesn't have anything to do with SMTP or any LoadMaster configuration.

L7: Connection Time Out Messages

- **L7: Connection Timed Out**

The 'kernel: L7: Connection timed out' are normal messages resulting from an L7 timeout. It's likely that users are idle and the connections timeout as a result. In most production environments, those messages are noise. They are only notable if there's a big change in

frequency (unaccompanied by a big change in web site traffic level) or if they correlate in time with user reported hangs/drops.

- **L7: Connection timed out (x.x.x.x:p->y.y.y.y:p-<nodest>)[0] (waiting for initial client request)**

"Waiting for initial client request" occurs when the client connects but does not send any data. The client in question is x.x.x.x, the VS is y.y.y.y, the third address is the RS. In this case, the RS has not been selected, since there has been no data from the client that can be used to determine which to select.

- **L7: Connection timed out (x.x.x.x:p->y.y.y.y:p->z.z.z.z:p)[0] (unconnected)==**

"Unconnected" timeouts are a result of connection attempts which were not completed to the real server. LoadMaster has determined which real server should take the connection and has initiated a TCP connection to the server, however the server did not respond. This may be due to a failed real server which has not been marked as failed by the health check. It could also be caused by a very slow response time.

- **L7: Connection timed out (x.x.x.x:p->y.y.y.y:p->z.z.z.z:p)[0] (connected)**

"Connected" timeouts indicate that the connection to the real server has been established and that data may have been transferred. The connection was disconnected because the idle timeout has been reached. This type of timeout is normal and is mostly the result of clients simply abandoning the connection.

The default for the timeout is 660s. This timeout can be found in System Configuration > Miscellaneous Options > L7 Configuration. The 'L7 Connection Timeout (secs)' is the global value for this timer. If it is set to 0, it will use the default value. This value can be overridden by the 'Idle Connection Timeout' in each virtual service.

- **L7: Real Server Connect attempt failed (x.x.x.x:p->y.y.y.y:p)**

This message indicates that the server was unreachable for client connections even though the healthcheck is passing. This can be due to several factors. Most likely the health check is not operating at a high enough level, the healthcheck considers the server up whereas in reality the server is not ready to accept connections. This can also happen if the server has just gone down and the healthcheck has not yet failed. In wildcard services, a client could be connecting on a port which the server is not listening on

HA Messages

- **Bad Digest**

These messages indicate that there is a conflict in HA checks. This commonly occurs when there is more than one set of clustered devices on a subnet. If you have other devices utilizing CARP or VRRP, you will need to set the HA Virtual ID to a unique value for your LoadMaster pair.

You can change this in System Configuration > Miscellaneous Options > HA Parameters. You will need to change this to the same value for both units individually.

- **PAM-warn**

The logs you were seeing are completely normal and are a result of the LoadMaster's inter-HA communications. Every time a configuration file is changed, the change is mirrored to the partner unit securely. If you have Inter-HA L4 or L7 updates enabled, there's even more reason for the updates as each new connection's information is kept active across the pair to maintain seamless transitions in the event of a failover.

Enhanced Messages

- **Healthcheck Failed Messages**

These messages are available in 5.1 and forward to document the specific reason why a server failed the healthcheck.

"Timeout waiting for data"	Connected, but server took too long to send back any data.
"Timeout waiting for connection"	Probably only seen when checking "remote" machines, or if machine has just failed (ARP still valid).
"Connection Failed - unreachable host"	There is no route to the host, machine is probably down, or a network failure.
"Connection Failed - server unavailable"	Machine is available but the application is not running (connection refused).
"Connection Failed - Failed SSL negotiation"	TCP connection ok, but the SSL_connect failed.
"Connection Failed - async TCP connect failed"	The system was too congested to start a connection request.
"Response did not match"	If doing a match, this is a failure.
"EOF or Incorrect data received"	No or invalid data received from server.
"Bad HTTP status received"	When doing a GET/HEAD and the response code is not 200 (or 401 or 301 or 302).

- **__ratelimit**

The `kernel: __ratelimit: x callbacks suppressed` is a kernel log message that indicates that a log message has been repeated. It is similar to the `last message repeated x times` They conserve log space by condensing multiple messages into one line. This message is not a problem on it's own. If there are no other messages in the logs which indicate a problem, then there is nothing to worry about.

Appendix F. Configuring Real Servers for the DSR Configuration

The VIP address on a Real Servers must be configured so that the server does not respond to arp requests on the VIP address.

For Linux with a recent 2.4 kernel, this can be done by creating the VIP as an IP alias on the loopback interface.

When you create the VS and assign the respective Real Servers to it, select “route” as the forwarding method to the Real Servers. This means that the LoadMaster just routes the packets from a client to a RS without modifying the IP addresses. The Real Server accepts requests for the VIP destination address because it has configured the VIP as an IP alias. The Real Server will then reply to the IP address of the requesting client with the source IP address of the reply set to the VIP.

Step	Source IP	Destination IP	MAC Address
1	216.139.43.10	195.30.70.200	Dest: 00:00:00:00:00:aa
2	216.139.43.10	195.30.70.200	Dest: 00:00:00:00:00:bb
3	195.30.70.200	216.139.43.10	Source: 00:00:00:00:00:bb

Configuring a VIP on the loopback interface on Linux

On a linux machine the “ifconfig –a” command will look something like this:

```
root@RS1 $ ifconfig -a
eth0    Link encap:Ethernet HWaddr 00:00:00:00:00:bb inet addr: 195.30.70.11 Bcast:
195.30.70.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:96561817 errors:526
dropped:0 overruns:5 frame:0 TX
packets:97174301 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:100 Interrupt:10
Base address:0x4000
lo      Link encap:Local Loopback inet addr:127.0.0.1 Mask:255.0.0.0 UP LOOPBACK
RUNNING MTU:3924 Metric:1 RX packets:3985923
errors:0 dropped:0 overruns:0 frame:0 TX packets:3985923 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
```

To create an additional loopback interface with an IP alias use the “ifconfig” command like this:

```
root@RS1 $ ifconfig lo:1 195.30.70.200 broadcast 195.30.70.200 netmask 255.255.255.255
root@RS1 $ ifconfig lo:1
lo:1    Link encap:Local Loopback inet addr:195.30.70.200 Mask:255.255.255.255 UP
LOOPBACK RUNNING MTU:3924 Metric:1
```

The next step is to disable invalid ARP replies. Add the following to your /etc/sysctl.conf file:

- net.ipv4.conf.all.arp_ignore=1
- net.ipv4.conf.eth0.arp_ignore=1
- net.ipv4.conf.eth1.arp_ignore=1
- net.ipv4.conf.all.arp_announce=2
- net.ipv4.conf.eth0.arp_announce=2

- net.ipv4.conf.eth1.arp_announce=2

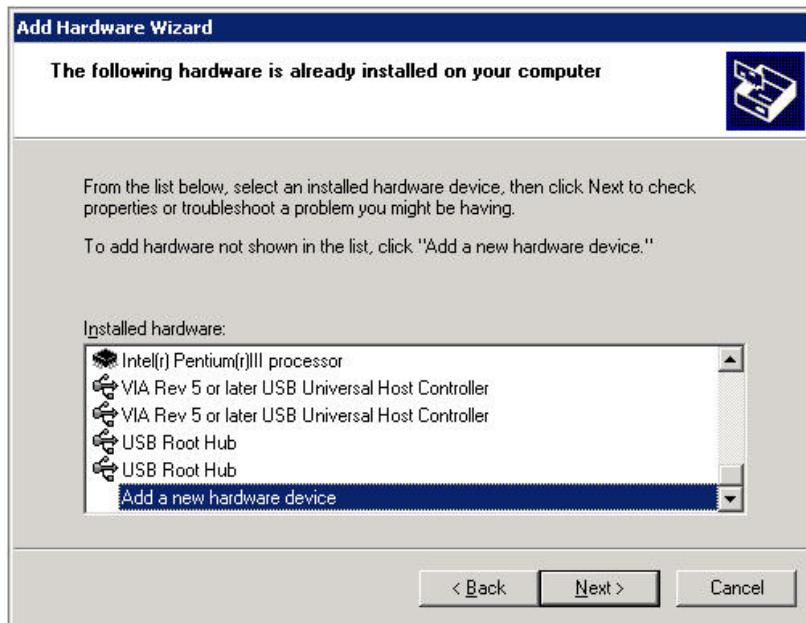
DSR Configuration on Windows

For Windows, it's typically best to use the loopback address. However, to use the loopback address, you'll need to add the loopback adapter.

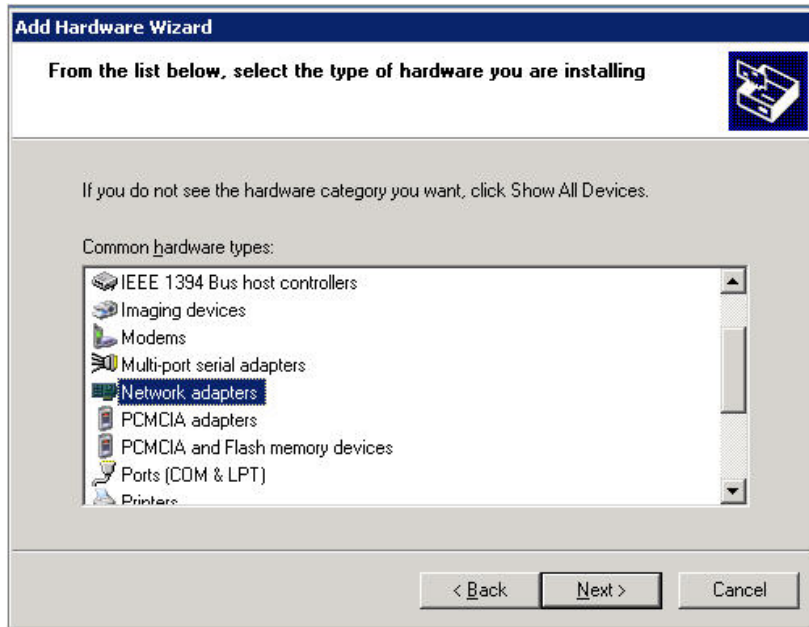
In the Windows control panel, select **Add Hardware**



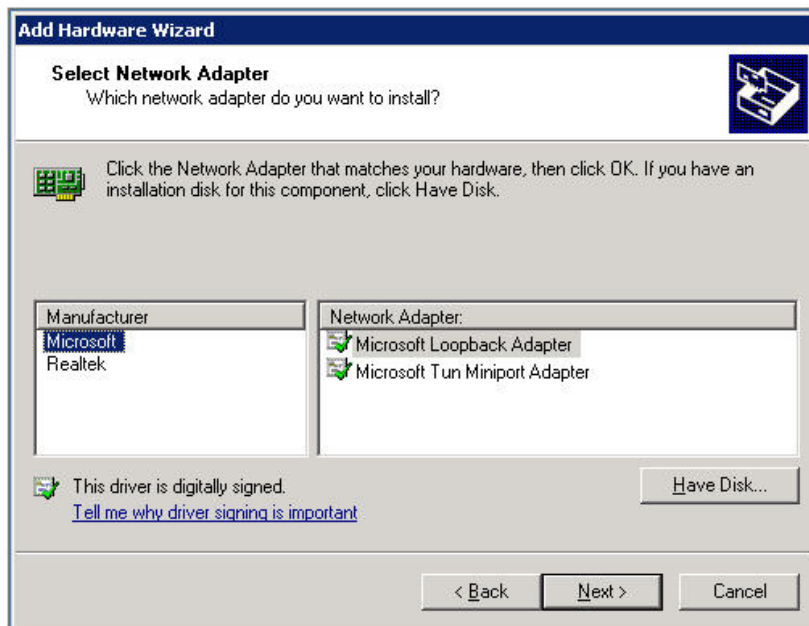
Click on **Next**, and the wizard may try to discover any new network devices. When it asks “is the hardware connected?” Select **Yes** and click on **Next**. You'll see a list of hardware. Scroll down and select **Add a new hardware device**.



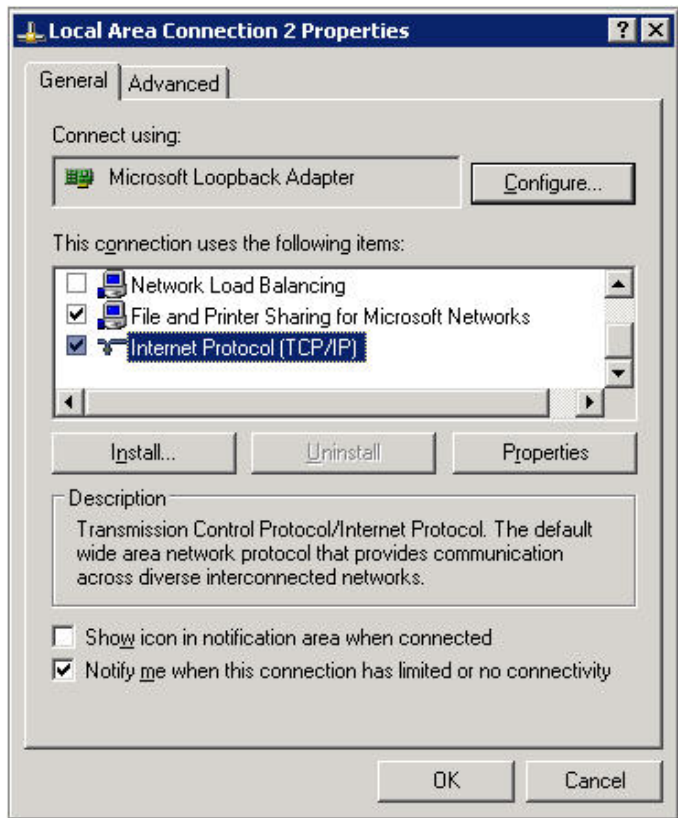
In the next screen, select the manual add option. You'll see a list of devices, and select **“Network adaptors”**.



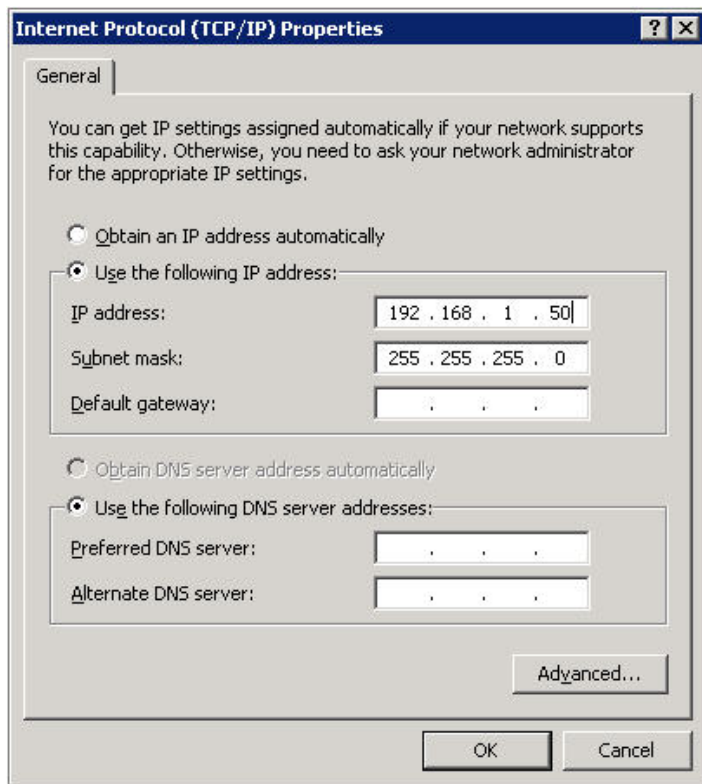
On the next screen, you'll see a list of manufacturers of network interface. Select **“Microsoft,”** then **“Microsoft Loopback Adapter”** and click on **“Next”**.



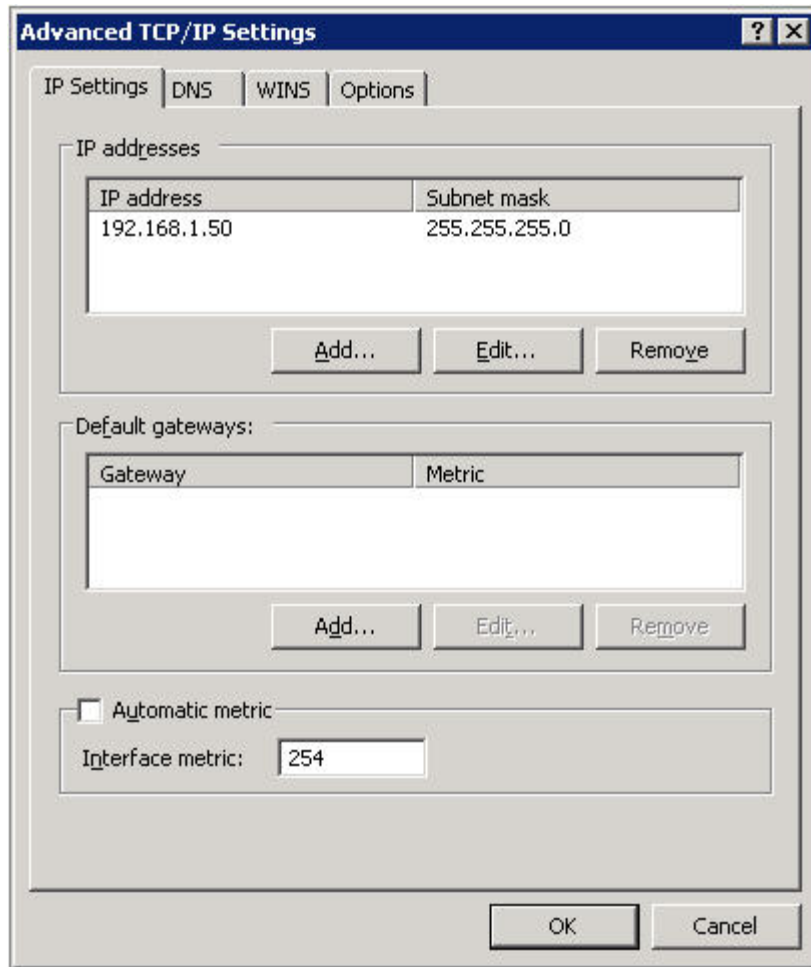
After the installation is complete. You'll have a new network interface in your **Network Connections** menu in the **Control Panel**. It may be named something like **“Network Connection 4”**, so it might help to rename it to something like **“loopback”**. Go into the **properties** of this interface, and select **“TCP/IP”**.



The TCP/IP properties window will be brought up, and this is where you configure the **Virtual Service IP** address. If your Virtual Service IP address is 192.168.1.50, then you would put it in the IP address field. Then click on “**Advanced...**”.



Uncheck the on the “**Automatic metric**” checkbox and enter “**254**” for interface metric. **This is an important step.** This will disable this server so that it will not respond to ARP requests for the MAC address for the Virtual Service IP. Click “**OK**” to activate the change.



Click on “**OK**” and close to complete the task.

Configuring a VIP on the loopback interface on Windows Server 2000

Start->Settings->Control Panel->Add/Remove Hardware

Add/troubleshoot a device->Next

Add a new device->Next

No, select from list->Next

Network Adapters->Next

Select "Microsoft" as Manufacturer->select "MS Loopback Adapter"->Next->Finish

To configure the just-created Loopback Adapter:

Start->Settings->Control Panel->Network and Dial up Connections

Right click on new adapter selecting properties

Only "Internet Protocol" needs to be selected (i.e., remove selection of "Client for MS Networks" and "File and Printer sharing")

TCP/IP Properties->enter IP address of virtual server (the loopback adapter gets the same address as in the LoadMaster VS IP)

Do not enter a default gateway

Advanced->Set Interface Metric to 254 (this step is important so that the loopback adapter is prevented from responding to ARP requests)

OK and save all changes.

Configuring a VIP on the loopback interface on Windows Server 2003

Start->Settings->Control Panel->Add Hardware

In the Welcome window, click **Next**.

In the “Is the hardware connected?” Window, select **Yes, I have already connected the hardware**, and click **Next**.

In the “The following hardware is already installed on your computer window” dialog, in the list of installed hardware, select **Add a new hardware device**, and click **Next**.

In the “The wizard can help you install other hardware window” dialog, select **Install the hardware that I manually select from a list**, and click **Next**.

From the list of hardware types, select the type of hardware **Network adapters**, and click **Next**.

In the Select Network Adapter window, make the following selections:

Manufacturer: Select **Microsoft**.

Network Adapter: Select Microsoft Loopback Adapter.

Click **Next**.

In the “The wizard is ready to install your hardware window” dialog, click **Next**.

In the “Completing the Add Hardware Wizard” dialog, click **Finish**.

Restart your computer.

To configure the just-created Loopback Adapter:

Right-click **My Network Places** on the desktop and choose **Properties**. This displays the **Network Connections Control Panel**.

Right-click the connection that was just created. This is usually named "Local Area Connection 2". Choose **Properties**.

On the General tab, select Internet Protocol (TCP/IP), and click Properties.

In the **Properties** dialog box, click Use the following IP address and do the following:

IP Address: Enter IP address of virtual server (the loopback adapter gets the same address as in the LoadMaster VS IP)

Do not enter a default gateway

OK and save all changes.

Restart the computer.

Configuring a VIP on the loopback interface on Windows Server 2008 R2

For Windows, it's typically best to use the loopback address. However, to use the loopback address, you'll need to add the loopback adapter. This is added through the Device Manager. The screen shots below are

shown for Windows 7 and in the text it will reflect Windows 7. However where a difference occurs between Windows XP, that will be added in parenthesis.

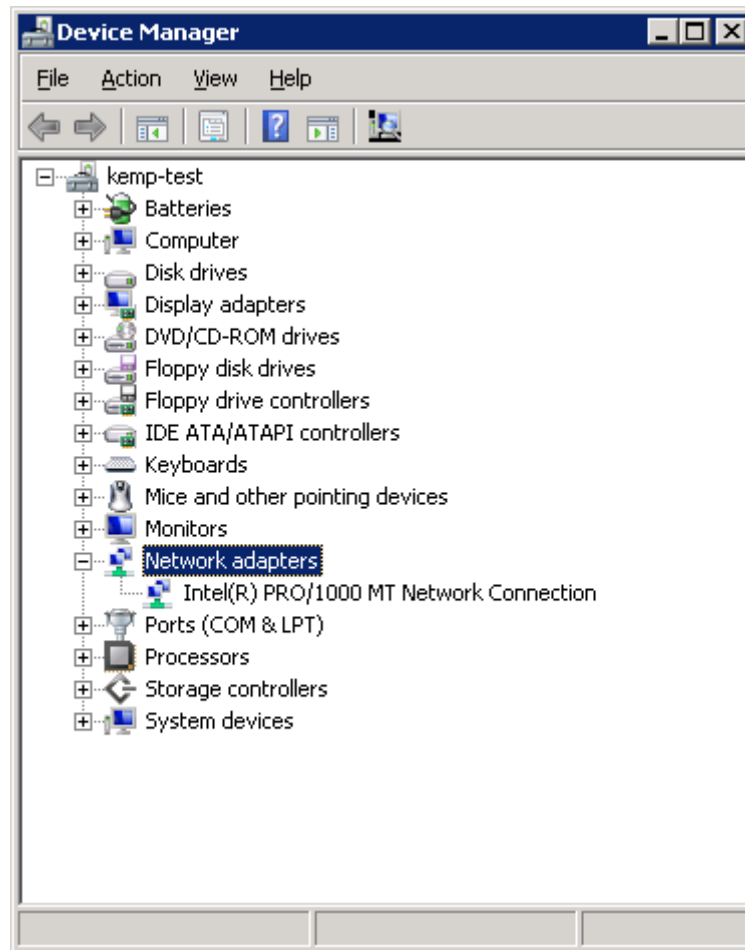
To reach the device manager in Windows XP.

On the desktop, right click My Computer, select the Hardware tab and click the Device Manager button.

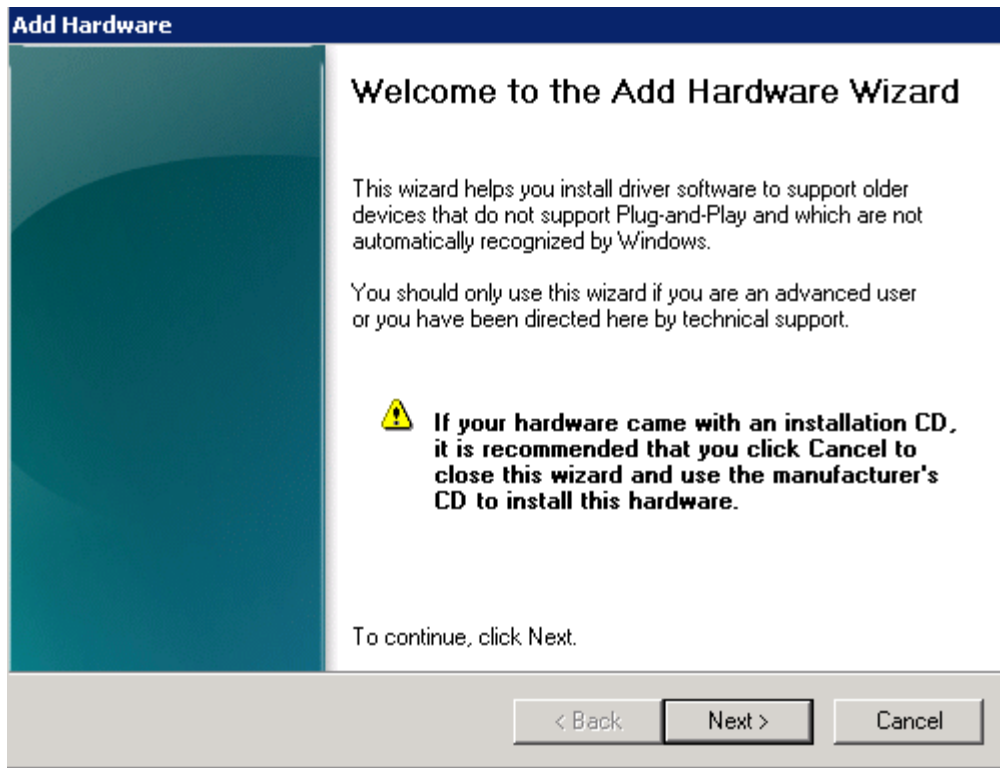
To reach the device manager in Windows 7.

Go to Start, click Control Panel –make sure you have small icons selected- and click Device Manager.

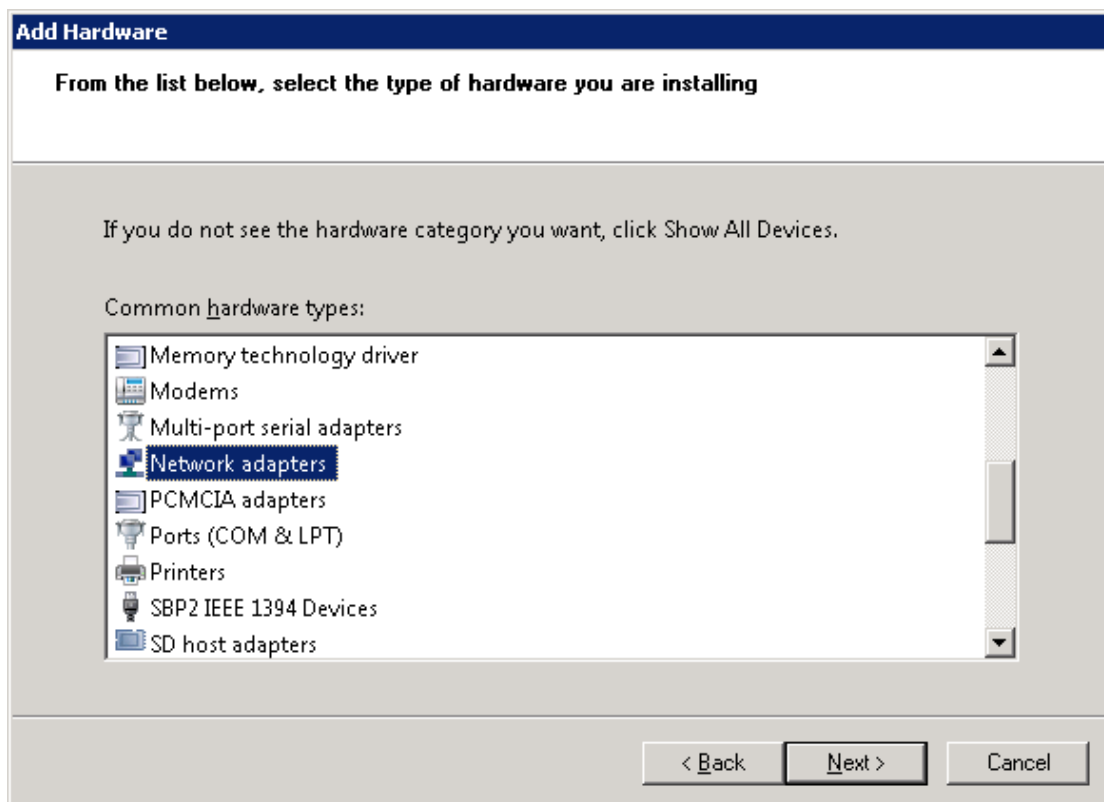
You will be shown a window as below.



Select **Network Adapters** in the window, click on the menu item **Action** and select **Legacy Hardware (Add Hardware)**. The window below will show.

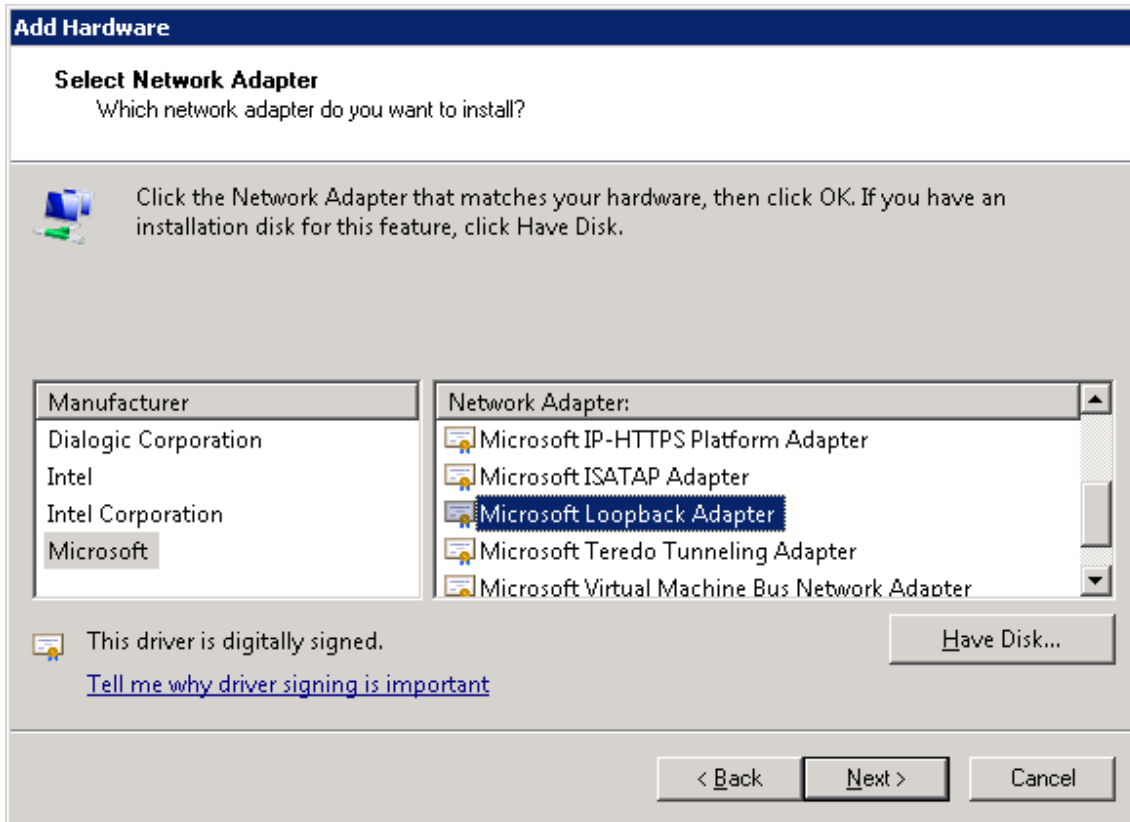


Click **Next** and on the next screen select the radio button that states; **Install the hardware that I manually select from a list (Advanced)**. Click **Next** and you should see the screen below.

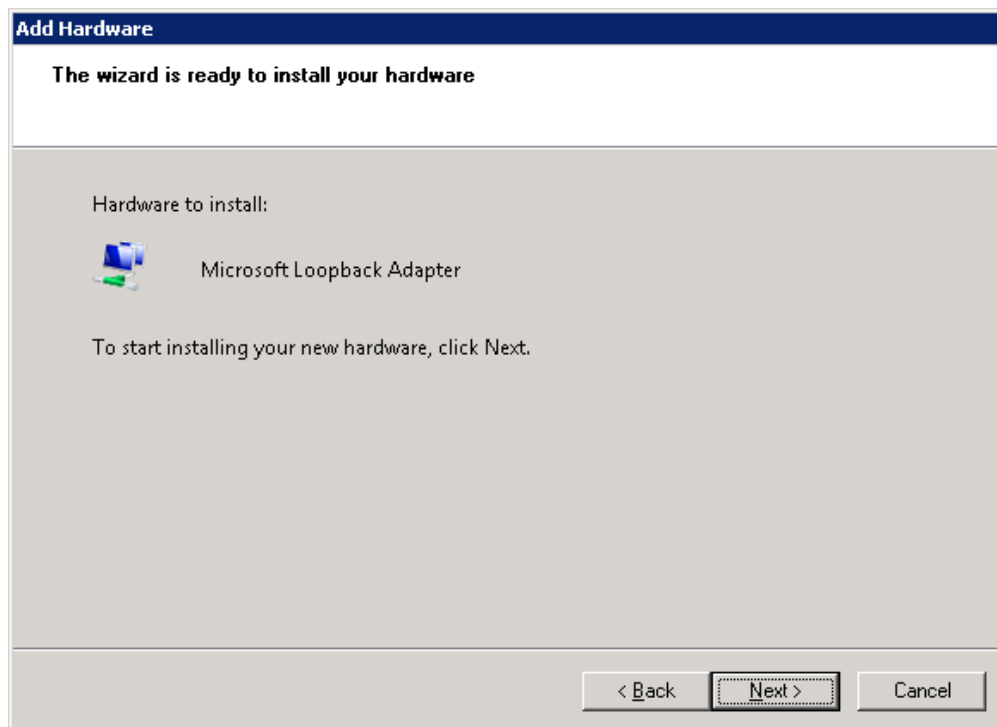


Scroll down the list of devices and select **Network Adapters**.

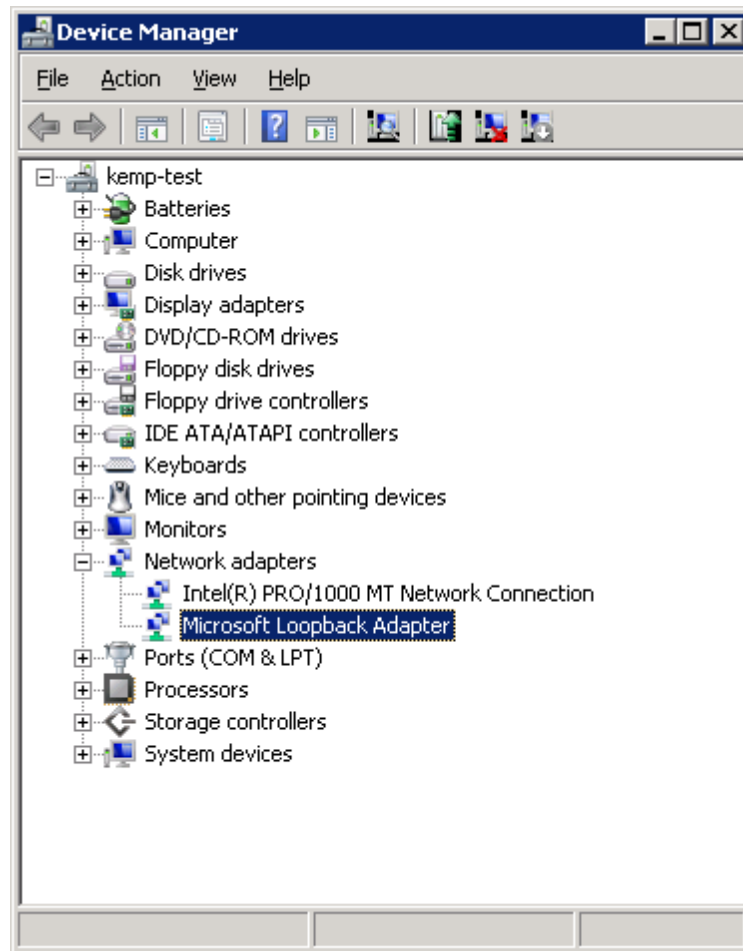
Scroll down the left-hand pane and select **Microsoft**, then scroll down the right-hand pane and select **Microsoft Loopback Adapter**.



Click **Next** and you will be ready to install the Loopback Adapter. Click **Next** again.

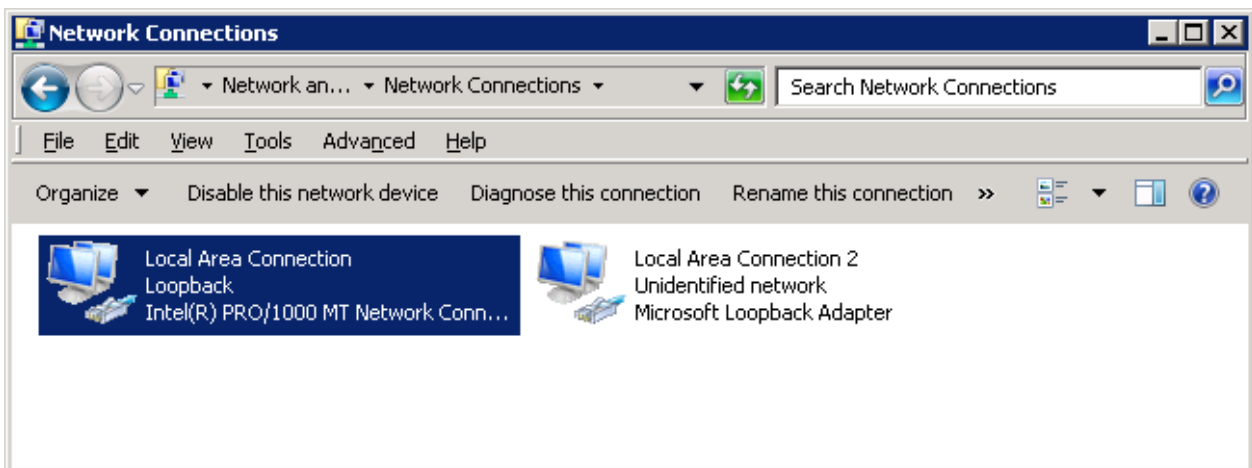


You will see a screen that shows the adapter was successfully installed. Click Finish and go back to the Device Manager screen, which should look like the screen below where you now have an additional network adapter, the Loopback.



Locate the new Loopback adapter in **Network Connections** from the Control Panel. Confirm the network configuration.

A good idea is to rename the adapters so they are readily distinguishable, for example rename the new adapter to "loopback" and the real network adapter to "network".



Configure the loopback adapter with the Virtual Service IP.



Make sure the “network” adapter is the actual network adapter that will send and receive traffic.

On the Windows command line run:

```
netsh interface ipv4 set interface "net" weakhostreceive=enabled
netsh interface ipv4 set interface "loopback" weakhostreceive=enabled
netsh interface ipv4 set interface "loopback" weakhostsend=enabled
```

Appendix G: Headers Added by LoadMaster When ‘Clientz Certificates and Add Headers’ Option is Selected

When the Client Certificates and add Headers option is selected in the Client Certificates drop-down while enabling SSL Acceleration, a number of headers are added. The following list describes the headers that are added to the https request by LoadMaster.

```

SSL_CLIENT_A_KEY="rsaEncryption"
SSL_CLIENT_A_SIG="md5WithRSAEncryption"
SSL_CLIENT_I_DN="/C=US/ST=Administrator/L=Limerick, Ireland/O=Kemp
Technologies/OU=Mary Rosse House/CN=MMC CA"
SSL_CLIENT_I_DN_C="US"
SSL_CLIENT_I_DN_CN="MMC CA"
SSL_CLIENT_I_DN_L=" Limerick, Ireland "
SSL_CLIENT_I_DN_O=" Kemp Technologies "
SSL_CLIENT_I_DN_OU=" Mary Rosse House "
SSL_CLIENT_I_DN_ST="Administrator"
SSL_CLIENT_M_SERIAL="05"
SSL_CLIENT_M_VERSION="3"
SSL_CLIENT_S_DN="/C=US/O= Kemp Technologies /OU= Mary Rosse House
/ST=Administrator/L= Limerick, Ireland /0.9.2342.19200300.100.1.1=jar/CN=Kemp
Sales/Email=sales@kemptechnologies.com"
SSL_CLIENT_S_DN_C="US"
SSL_CLIENT_S_DN_CN="Kemp Sales"
SSL_CLIENT_S_DN_Email="sales@kemptechnologies.com"
SSL_CLIENT_S_DN_L="Limerick, Ireland "
SSL_CLIENT_S_DN_O="Kemp Technologies "
SSL_CLIENT_S_DN_OU="Mary Rosse House "
SSL_CLIENT_S_DN_ST="Administrator"
SSL_CLIENT_VERIFY="SUCCESS"
SSL_CLIENT_V_END="Jan 16 14:30:35 2005 GMT"
SSL_CLIENT_V_START="Jan 18 14:30:35 2000 GMT"

```

```

SSL_SERVER_A_KEY="rsaEncryption"
SSL_SERVER_A_SIG="md5WithRSAEncryption"
SSL_SERVER_I_DN="/C=US/ST=Administrator/L=Limerick, Ireland/O=Kemp
Technologies/OU=Mary Rosse House/CN=MMC CA"
SSL_SERVER_I_DN_C="US"
SSL_SERVER_I_DN_CN="MMC CA"
SSL_SERVER_I_DN_L=" Limerick, Ireland "
SSL_SERVER_I_DN_O=" Kemp Technologies "
SSL_SERVER_I_DN_OU=" Mary Rosse House "
SSL_SERVER_I_DN_ST="Administrator"
SSL_SERVER_M_SERIAL="05"
SSL_SERVER_M_VERSION="3"
SSL_SERVER_S_DN="/C=US/O= Kemp Technologies /OU= Mary Rosse House
/ST=Administrator/L= Limerick, Ireland /0.9.2342.19200300.100.1.1=jar/CN=Kemp
Sales/Email=sales@kemptechnologies.com"
SSL_SERVER_S_DN_C="US"
SSL_SERVER_S_DN_CN="Kemp Sales"
SSL_SERVER_S_DN_Email="sales@kemptechnologies.com"

```

```
SSL_SERVER_S_DN_L="Limerick, Ireland "  
SSL_SERVER_S_DN_O="Kemp Technologies "  
SSL_SERVER_S_DN_OU="Mary Rosse House "  
SSL_SERVER_S_DN_ST="Administrator"  
SSL_SERVER_VERIFY="SUCCESS"  
SSL_SERVER_V_END="Jan 16 14:30:35 2005 GMT"  
SSL_SERVER_V_START="Jan 18 14:30:35 2000 GMT"
```

Appendix H: API for Agent Based Adaptive Balancing

For adaptive scheduling the LoadMaster periodically checks the system load on all the servers in the farm. Each server machine has to provide a file that contains a numeric value in the range between 0 and 102 representing the actual load on this server (0 = idle, 99 = overload, 101 = server down, 102 = administratively disabled). The LoadMaster retrieves this file by an HTTP GET operation. It is the servers' job to provide the actual load in the ASCII file. There are no prerequisites, though, how the servers evaluate this information.

There are some conditions that must hold:

- An ASCII file must exist with a number between 0 and 99 in the first line.
- The file must be accessible to an HTTP GET from the LoadMaster.
- The URL must be the same on all servers.
- The URL must match the entry "URL for adaptive scheduling" as set in the "Check Parameters" under the Rules & Checking panel.

The following is an example script to determine and present the load information on a LINUX server:

```
get load() {
  awk '/^cpu0/ {printf "%d %d %d %d\n", $2, $3, $4, $5}' \
  /proc/stat > /tmp/cpuload
  read USR SYS IOWAIT IDLE < /tmp/cpuload
  # echo $USR $SYS $IOWAIT $IDLE
}

INTV=5
DOCUMENTROOT=/usr/local/httpd/htdocs/
LOADFILE="$DOCUMENTROOT/load"

main() {
  while true; do
    USR1=$USR
    SYS1=$SYS
    IOWAIT1=$IOWAIT
    IDLE1=$IDLE
    get load
    SUM=$(( $USR+$SYS+$IOWAIT+$IDLE ))
    PUSR=$(( (USR-USR1)/$INTV ))
    PSYS=$(( (SYS-SYS1)/$INTV ))
    PIOWAIT=$(( (IOWAIT-IOWAIT1)/$INTV ))
    PIDLE=$(( (IDLE-IDLE1)/$INTV ))
    echo "$(( 100-PIDLE ))" > $LOADFILE
    sleep $INTV
  done
}
get load
main
```

Here is an example of a C program to determine and present the load information on a MS Windows NT or 2000 server:

```

#include <windows.h>
#include <stdio.h>
#include <conio.h>
#
#define CPU 0 0 /*processor 0*/
#define INTERVAL MS 3000 /*three seconds as interval*/

/*counter path for Windows NT 4.0 and 2000*/
#define COUNTER_PATH NT TEXT("\\\\%s\\Prozessor(%d)\\%% Prozessorzeit
(
v
HQUERY hQuery
F
yo
{
TCHAR c name[MAX_COMPUTERNAME_LEN
TCHAR counter path
DWORD ctrType;
DWORD size=MAX_COMP
HCOUNTER hCounter;
PDH STATUS pdhStatus;

if(!GetCo
{
fprintf(stderr
.
exit

pdhStatus = PdhOpenQuery(0,0
if(pdhStatus!=NO

if((GetVersion() & 0xFF) >= 5)
sprint
else
sp

pdhStatus=PdhAddCounter(hQue
if(pdhStatus!=NO
exit{

while(
{
fp=fopen(COU
if(!fp
{
fprintf(stderr,"ERROR: Couldn't open counter file!\n");
.
exit
}

pdhStatus=PdhCollectQueryDat
if(pdhStatus!=NO
exit(1);
pdhStatus =
PdhGetFormattedCounterValue(hCounter, PDH_FMT_DOUBLE, &ctrType, &fmt
fprintf(fp, TEXT{
fclose(fp);
.
Sle
}

yo
if(hQuery!=INVALID_HANDLE_VALUE
.

```

This example code is a program that obtains the CPU load counter from Windows 2000. It uses the Performance Data Helper (PDH) API, and must be linked to the pdh.lib.

The PDH Dynamic Link Library (DLL) pdh.dll must also be installed on the system.

Modify the counter paths for Windows 2000 dependent on the installed language.

Glossary

Access Code: An Access Code will be generated during the initial setup of the LoadMaster. You must contact your KEMP Technologies representative for your 30-day evaluation license or your full purchased license key.

AFE: Application Front End, a combination of features which are caching, compression and intrusion prevention.

Balancer: A network device or logic that distributes inbound connections with a common source address across a farm of server machines.

Farm Side: The LoadMaster network interface to which the server farm is connected.

Flat-based: The VIPs and the Real Servers are defined on the same subnet.

HA: Highly Available or High Availability (used interchangeably)

ICMP: Internet Control Message Protocol

IMAP: Internet Message Access Protocol

IPS: Intrusion Prevention System

MAT: MAC Address Translation

MIB: Management Information Base: A database of object definitions (also known as OIDs). Contains the details necessary for an SNMP manager to monitor the objects defined.

NAT: Network Address Translation

NAT-based: The request destination IP is modified by the LoadMaster to one of the Real Server IP addresses. Reply traffic from the Real Server must be routed through the LoadMaster so that the reply source IP can be changed to the VIP.

Network Side: The LoadMaster network interface over which requests to the server farm are typically made.

One-armed: Only one Ethernet interface is used for inbound and outbound traffic. (Used interchangeably with Flat-based.)

POP3: Post Office Protocol (email client protocol)

RS: Real Server: Physical server machines which make up a server farm.

Service: A Service is an application that is connected to the network.

Shared IP: In a LoadMaster HA configuration, the shared (floating) IP address is the “guaranteed available” address for a specific interface (e.g., eth0, eth1).

SCP: Secure copy command of SSH

SNMP: Simple Network Management Protocol: A network protocol used to manage TCP/IP networks. This protocol provides functions that enable you to access the data object whose definitions are given in the MIB.

S-NAT: Network Address Translation for a source IP address.

SSH: Secure Shell Protocol

Two-armed: The VIP is defined on a different subnet than the Real Servers.

UTC: Universal Time Coordinated (aka GMT).

VIP: Virtual IP Address: The IP address of a service defined on the LoadMaster.

VS: Virtual Service: An entry on the LoadMaster over which a service being hosted in the server farm can be reached.

WUI: Web User Interface: Used to perform LoadMaster administration via a web browser.

Index

- A**
- Adaptive Balancing, 19, 148
 - AFE, 25, 106, 150
- B**
- Backup, 39, 40, 43, 61, 95, 114
 - Bonding, 40
- C**
- Caching, 25, 27, 75
 - Certificate, 29, 30, 39, 57, 59, 60, 61, 62, 95
 - CLI, 33, 113, 114, 123, 124, 125, 126, 129, 130
 - Console, 112, 113
 - Content Rule, 82
 - Content Switching, 23, 31, 32, 53, 55, 74, 75, 77
 - Cookie, 22, 72
- D**
- DSR, 12, 14, 17, 136
- F**
- FIPS, 97
- H**
- HA, 14, 37, 42, 43, 44, 93, 94, 99, 107, 108, 109, 112, 113, 114, 115, 116, 118, 119, 120, 122, 150
 - Health Checking, 33, 34
- I**
- ICMP, 34, 44, 77, 78, 93, 120, 127, 150
 - IP Address transparency, 12, 14
 - IPS, 25, 26, 76, 129, 150
- L**
- L7, 22, 26, 38, 44, 47, 71, 103, 104, 109, 117, 118, 119, 123, 127
 - L7 Transparency, 71, 117
 - License- How to get one, 42
- M**
- MAC, 17, 135, 139, 150
 - MS Exchange 2010, 9
- N**
- NAT, 12, 14, 23, 45, 71, 77, 150
- O**
- One-Armed, 12, 13
- P**
- Persistence, 20, 21, 22, 23, 24, 63, 71, 76
- R**
- Real Server, 14, 19, 23, 25, 26, 27, 34, 35, 36, 45, 47, 52, 61, 64, 65, 75, 76, 77, 78, 80, 83, 99, 104, 123, 124, 125, 126, 127, 128, 129, 130, 150
 - Restore, 43, 61, 95, 114
- S**
- SMTP, 33, 34, 101, 116, 122
 - S-NAT, 12, 14, 45, 117, 150
 - SNMP, 37, 98, 99, 100, 118, 122, 150
 - SNORT, 25, 26, 76
 - SSL, 9, 23, 24, 25, 29, 35, 39, 43, 56, 57, 59, 60, 61, 64, 65, 73, 76, 78, 95, 114, 121, 122, 127
- V**
- Virtual Services, 12, 14, 25, 27, 28, 29, 33, 34, 39, 44, 51, 52, 55, 56, 57, 64, 65, 66, 69, 71, 75, 76, 83, 84, 104, 114, 117, 123, 129
 - VLAN, 40, 41, 91

Document History

Date	Change	Reason for Change	Version	Resp
Aug-2011	Initial release		6.0-8 v.1.0	CJM
Oct-2011	Update backups and templates.	New features.	6.0-15 v.2.0	CJM
Nov-2011	Updates per SWRN	Bug fixes	6.0-17 v.1.0	CJM
Dec-2011	Copyright additions plus V6 changes	For compliance and to match new GA.	6.0-22 v.3.0	CJM
Jan-2012	Feature updates	To match release	6.0-28 v.1.0	CJM
Mar-2012	Formatting, content reorganization and minor content changes	To reorganize the document and make it more user-friendly.	6.0-28 v.2.0	DD
Mar 2012	Updates as per 6.0-28a release Updates to rectify a number of documentation issues	Re-enabled features and rectifying issues	6.0-28a v.1.0	DD