Progress®
Kemp® LoadMaster®

Interface Description LoadMaster CLI

Generated on: 10 March 2025

Copyright

Visit the following page online to see Progress Software Corporation's current Product Documentation Copyright Notice/Trademark Legend: Product Documentation Copyright Notice & Trademarks | Progress

Table of Contents

Chapter 1: Introduction 5

Chapter 2: LoadMaster Console Operation 6

Introduction 6

Initial Setup 7

Troubleshooting Licensing Issues 7

Console Main Menu 8

Configuration Menu Basics 9

Main Menu 9

Quick Setup 10

Service Management (CLI) 12

Local Administration 12

Basic Setup 16

Packet Filter and Blacklists 17

Utilities 18

Reboot 21

Chapter 3: Command Line Interface (CLI) Reference Guide 22

Top level commands 23

Adaptive scheduling command level 24

Health Check Command Level 25

Rules command level 26

Rule Edit command level 26

Virtual Service (VIP) command level 28

Real Server command level 34

Chapter 4: References 36

1

Introduction

Progress Kemp 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.

Progress Kemp 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.

Document Purpose

This document describes the Command Line Interface (CLI) to the LoadMaster. It describes in detail how to configure the various features of the LoadMaster using the CLI.

Note: You cannot configure all LoadMaster options using the CLI. If you cannot find what you are looking for, it might be available using the RESTful or PowerShell API. For more details refer to the RESTful API documentation or PowerShell Interface Description.

2

LoadMaster Console Operation

Refer to the following sections for details on LoadMaster console operation.

Contents

- Introduction
- Initial Setup
- Troubleshooting Licensing Issues
- Console Main Menu
- Configuration Menu Basics
- Main Menu
- Quick Setup
- Service Management (CLI)
- Local Administration
- Basic Setup
- Packet Filter and Blacklists
- Utilities
- Reboot

Introduction

The Command Line Interface allows users to interact with the LoadMaster using a command line shell or a

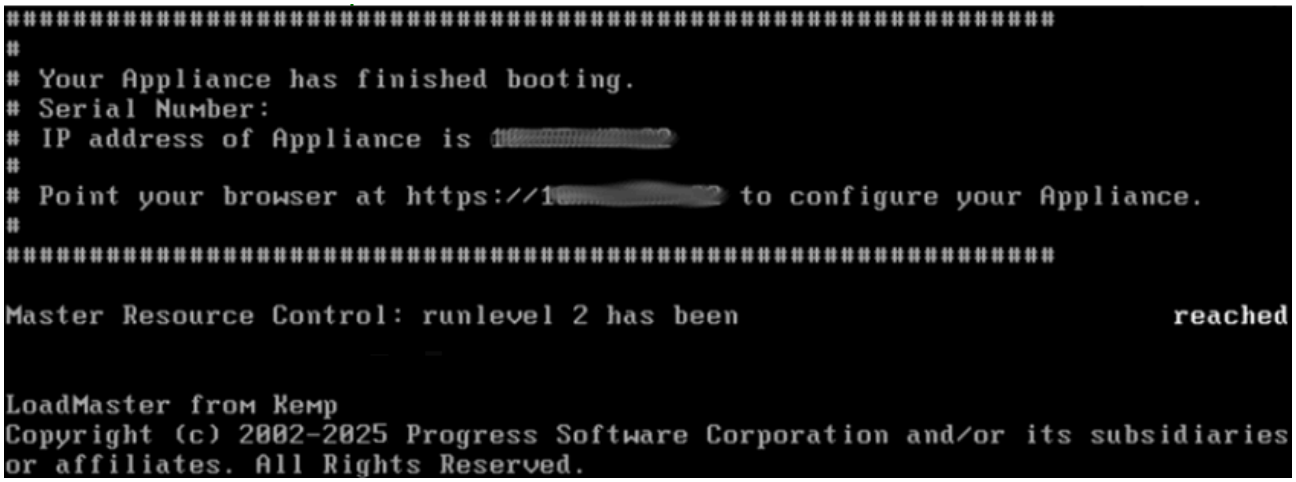
menu-based series of options.

If you have a hardware LoadMaster, you will need a PC to connect using a COM+ (Console) port with a terminal emulation application, or a standard VGA and keyboard. Use 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 be 115200,8,N,1.

Starting with LoadMaster Version 7.2.47, it is possible to connect directly to the LoadMaster serial console in all cloud deployments that support direct serial console access (AWS, for example, currently does not provide direct access to the console). Access to the console allows you to use the CLI and to reset the 'bal' administrative password, as explained in this document. [In previous releases, cloud users could only use the CLI over SSH, and could not use the console to reset the administrative password.]

Initial Setup



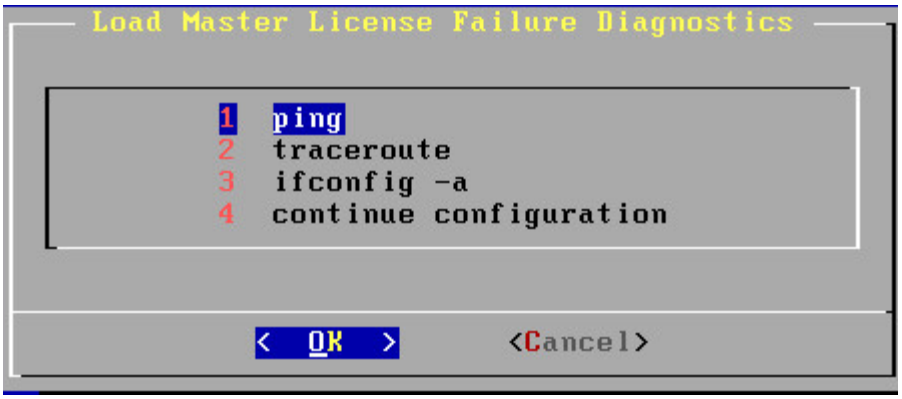
After initially deploying and powering on a LoadMaster, ideally the IP address of the LoadMaster will be obtained using DHCP.

If the IP address has not been obtained using DHCP, or if the address details of the LoadMaster need to be changed, the console can be used to configure the IP address of the LoadMaster, the default gateway address and the name server addresses. To go through this menu, simply log in to the console using the default username and password (**bal** and **1fourall**).

Troubleshooting Licensing Issues

After configuring the address details and accessing the LoadMaster using the Web User Interface (WUI), the LoadMaster must be licensed. For further information on licensing, refer to the Licensing, Feature Description.

If licensing fails for any reason, various debug options will become available on both the WUI and the console. These options can be used to troubleshoot problems that may occur when trying to license the LoadMaster.



If licensing fails for any reason, a diagnostics menu appears when the LoadMaster console is accessed. This menu has the following options:

- **Ping:** Performs a ping on the specified host. The LoadMaster tries to auto-detect what type of ping to use (ping for IPv4 and ping6 for IPv6). If this auto-detection does not work, you are asked which ping to use.
- **Traceroute:** Performs a traceroute of the specific host.
- **Ifconfig:** Displays raw ifconfig output.
- **Continue configuration:** Use this option to reconfigure the address details of the LoadMaster.

Console Main Menu

After a LoadMaster has been successfully licensed, the console main menu is displayed whenever the console is accessed.

If an **SSH Pre-Auth Banner** is set, the banner message is displayed before initially logging in using SSH.

Many features of the LoadMaster can be configured using the menu system. You can use the menu system by logging into the console as "bal", or by remotely logging into the system using the SSH protocol.

Note: 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: As of LoadMaster firmware version 7.2.48.4 Long Term Support (LTS) and 7.2.53, RSA keys are no longer supported for SSH access to the LoadMaster. If you are using RSA keys for SSH access and you are upgrading to one of these versions (or above) you must move to another key type. There are two key types available as an alternative to the RSA keys: ecdsa-sha2-nistp384 and ssh-ed25519.

If the password for "bal" has been forgotten, you can log in on the console as **pwreset**. The password is **1pwreset**. This resets the password for "bal" to **1fourall** until the LoadMaster is rebooted. If unit is rebooted without the password being changed, the password resets to its old (unknown) value. It is thus strongly advised that you change the password using the configuration menu before the next reboot.

Note: Using **pwreset** only changes the password temporarily for the console. It does not reset the WUI password.

Configuration Menu Basics

The configuration menu system has a number of hierarchical menus split into functional groups. You can navigate around the menus by using the Up and Down cursor keys, or by using the "+" and "-" keys. You can also enter the number for menus with numeric entries.

Using "q"<CR> or "ESCAPE" or using the [CANCEL] button returns you to the previous menu.

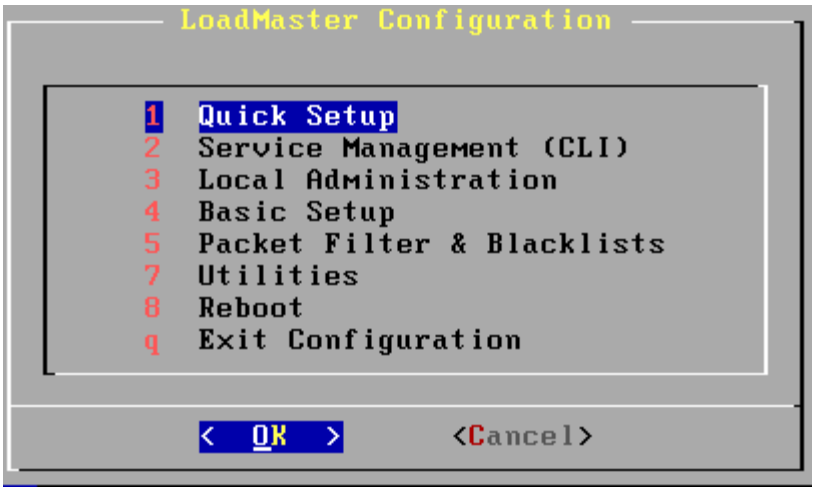
To access the [OK], and [CANCEL] buttons, use the TAB key to toggle between the menu and the buttons.

If you use the [CANCEL] button from the main menu, all changes made to the configuration are ignored.

Using the [OK] button from the main menu performs the menu point, which is currently highlighted.

Note: When the LoadMaster is configured in a High Availability (HA) cluster and you are logged into the standby machine, you should only configure the local IP interfaces, change the local password, and perform a backup/restore. All other configuration parameters should only be changed on the active machine.

Main Menu



The following options are available on the initial CLI menu.

Quick Setup

Quick setup allows you to quickly configure a LoadMaster; only the most important parameters needed by the LoadMaster are set up.

Service Management (CLI)

This menu point starts a Command Line Interface (CLI), which lets you administer the Virtual Services that are available on the LoadMaster.

Local Administration

This menu allows you to administrate options such as password, time, backups, and so on, within the LoadMaster

Basic Setup

From this menu option you can configure various aspects of the LoadMaster such as interfaces, hostname, DNS, and so on.

Packet Filter and Blacklists

From this menu you can manage Access Control Lists.

Utilities

A variety of utilities can be administered such as Software Upgrades, determining the Transfer Protocol used, License Updates and configuring a number of diagnostic tools.

Reboot

Selecting the Reboot option enables you to reboot the LoadMaster.

Exit Configuration

Exits the menu.

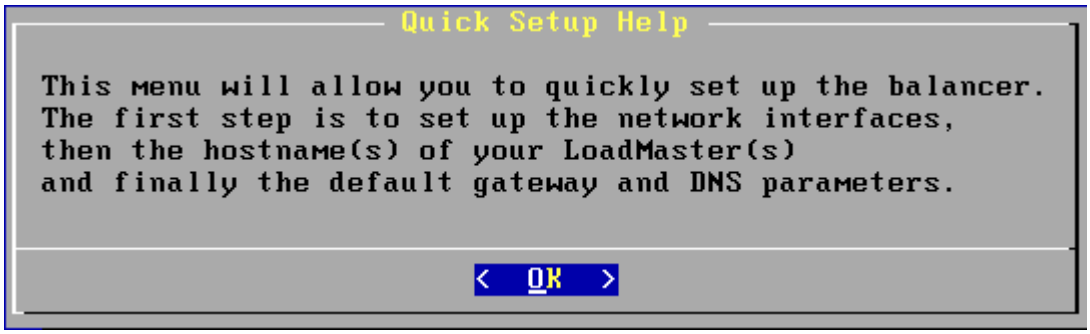
These options are discussed in more detail in subsequent sections of this document.

Quick Setup

Quick setup automatically begins when you log in to the LoadMaster for the first time and the license key has been validated. It can also be started by selecting option 1 from the main menu.

Quick setup allows you to quickly configure a LoadMaster. Only the most important parameters needed by the LoadMaster are set up. After 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:



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 use.

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

Ethernet IP address(s) – eth0

You are 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.

For example, 192.168.200.12/24

If no network specifier is given, you are asked to specify the netmask. This may be input as either a network specifier (for the above example /24.) or as a “dotted quad” (for example, 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 is then requested. This must be on the same network as the primary IP address of eth0 (as previously configured).

Ethernet IP address(s) – eth1

You are 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(es) on eth0.

Hostname

You must now set the hostname of the LoadMaster. 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.

Name Server IP Addresses

Enter a space-separated list of name server IP addresses. Up to three DNS servers may be specified (Addresses must be in “dotted quad” syntax).

Domain List

You can also provide a list of space-separated search domains. You can specify up to six domains.

Default Gateway

Enter the IP address of the default gateway. This must be an IP address on the network.

Reboot

You must reboot the LoadMaster to activate any changes made.

Service Management (CLI)

This menu point starts a Command Line Interface (CLI), which lets you administer the Virtual Services that are available on the LoadMaster.



To leave the CLI, you can use the ESCAPE or CTRL-D keys.

Local Administration

Selecting option **3**, **Local Administration**, in the Main Menu brings up the **Local Administration** screen.



This menu performs administration tasks for the current LoadMaster. The following options are available:

Set Password

You can use this option to 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.

Note: 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, 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 you to set the local date, time, and time zone.

A list of time zones is given; the current time zone is always at the start of the list. You can select a different time zone if required.

The date should be entered in the following format:

22-12-03 (Year-Month-Day)

Followed by the time in the following format:

10:57:15 (Hours:Minutes:Seconds)

Note: The default time zone for the LoadMaster is UTC.

Backup/Restore

Selecting the Backup/Restore option opens a screen with two options:

- **Save Backup to Remote Host**
- **Restore Backup from Remote Host**

When option 1 is selected, the backup process begins. The following information is requested:

- The host IP address where the backup will be stored
- The username on the backup host
- The filename of the backup

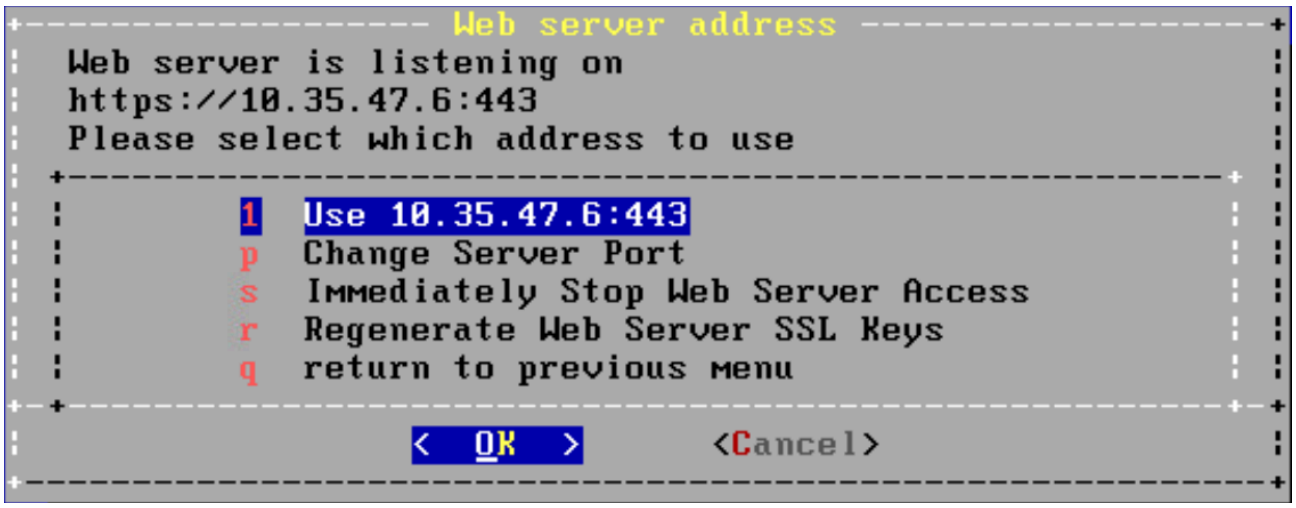
Note: The backup server machine must run an FTP daemon or an SSH daemon.

When option 2 is selected, the backup restore process begins. The following information is requested:

- The host IP address where the backup will be stored
- The username on the backup host
- The filename of the backup
- What is to be restored - the options include:
- 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

Note: 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.

Web Address



The LoadMaster is delivered with the WUI configured to be only accessible using the “network” side address.

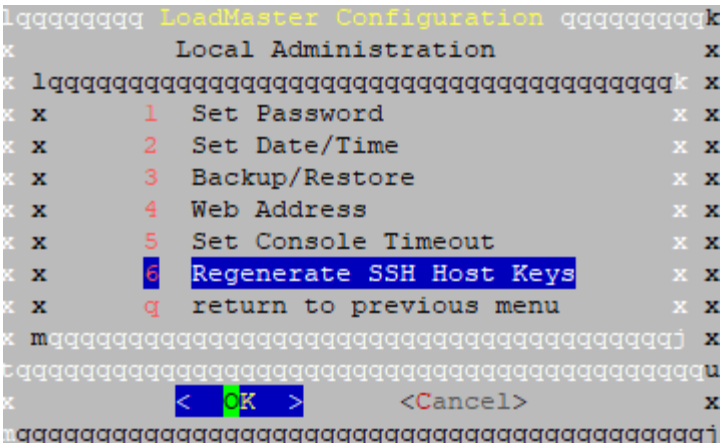
When the **Web Address** option is selected, a number of options appear:

- **Use <IP address:Port>:** This displays the IP address that will be used by the LoadMaster WUI. Depending on the value that the IP address is set to, this could be a network side or the farm side IP address. To change the IP address, go to the **Basic Setup** menu item and use the **Network Configuration** option. For more information, refer to the Basic Setup section.
- **Change Server Port:** Change the port used by the interface.
- **Immediately Stop/Start Web Server Access:** With this option you can disable or enable access to the LoadMaster WUI.
- **Regenerate Web Server SSL Keys:** This option resets the SSL certificates for the WUI. In a HA environment, the certificates get reset for both the local and shared WUI. Therefore, this needs to be run on both LoadMasters in a HA pair (to remove the local certificate). The certificate on the shared WUI will be corrected on both machines after the first invocation.
- **Restore Admin WUI access to default mode:** Reset the cipher set to the default WUI cipher set (as defined on the **Certificates & Security > Cipher Sets** page). The option **Certificates & Security > Remote Access > Self-Signed Certificate Handling** will also be reset to the default value (**RSA Self-Signed Certs**). This option is designed to restore access to the WUI in the event the cipher settings are misconfigured.
- **Confirm switch out of CC mode:** This option only appears when the LoadMaster is in a specific state. If **Self-Signed Certificate Handling** (in **Certificates & Security > Remote Access** in the WUI) is set to an EC mode and Random Number Generation (RNG) fails (for example, if the hardware does not support it like on legacy systems) a message will display on the home screen saying **Could not start CC mode - system disabled** and the WUI is unusable. This also generates a critical log message saying **Cannot initialize RNG, CC mode disabled** and an authlog saying **Failed to start RNG, CC mode not started**.To get out of this mode, you must select the **Confirm switch out of CC mode** option. This allows the system to work as usual (but not in Common Criteria (CC) mode).

Set Console Timeout

Use this option to set the idle timeout for the console (in minutes).

Regenerate SSH Host Keys



Host keys are kept in sync on High Availability (HA) machines.

Note that in GEO Partnering mode, SSH host keys are not automatically synchronized, because GEO does not use a shared IP address and the information exchange between partners does not depend on SSH access.

Note: Amazon Web Services (AWS) sets its own host key so the regenerate SSH host keys functionality is not available on AWS LoadMasters.

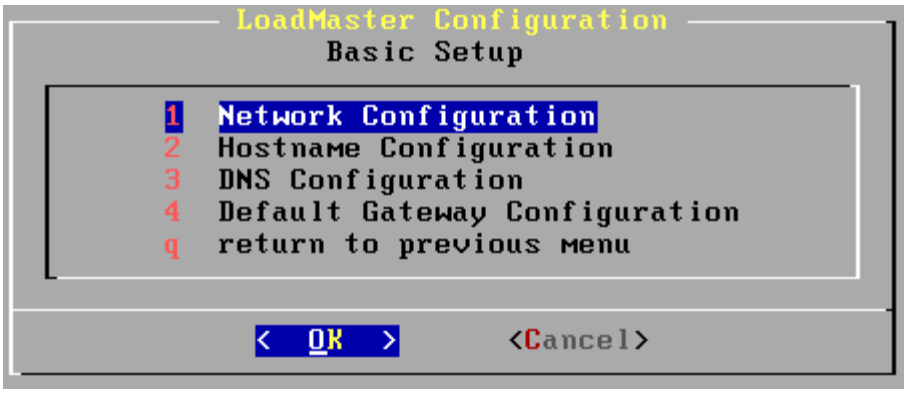
Note: On Azure, there are two authentication mechanisms; password and SSH key. If you have chosen password authentication, it is possible to use the regenerate SSH host keys functionality in the LoadMaster. If you are using Azure SSH key authentication, the regenerate SSH host keys functionality in the LoadMaster is not available.

When you regenerate the LoadMaster's host key, the **$HOME/.ssh/known_hosts** on all current SSH clients must be updated with the new public key.

The SSH key on LoadMaster firmware versions prior to 7.2.51 (or on LTS versions prior to 7.2.48.3) is always the same. When you upgrade to 7.2.51 (or 7.2.48.3 LTS) or downgrade from 7.2.51 (or 7.2.48.3 LTS), the SSH key will change. After upgrading to 7.2.51 (or 7.2.48.3 LTS), the key is regenerated and will stay the same on 7.2.51 (or 7.2.48.3 LTS) and above until you regenerate it again.

Basic Setup

Selecting the **Basic Setup** option in the main menu opens the **Basic Setup** screen.



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, that is,. the optional interfaces will be designated as eth0 and eth1. For more information on this topic 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.

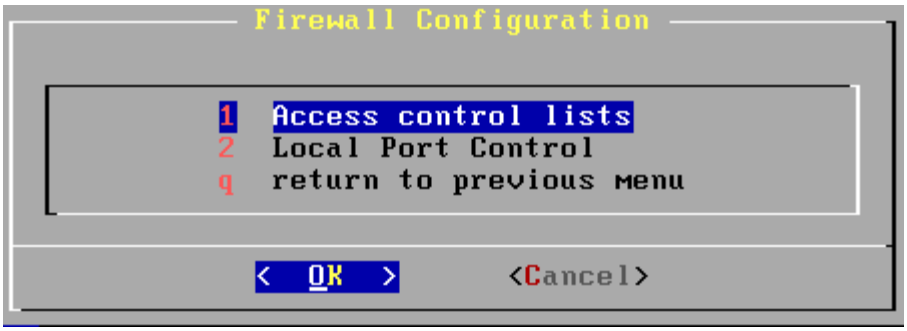
Up to six search domains may also be specified.

Default Gateway Configuration

The LoadMaster requires a default gateway through which it can communicate with the Internet. Enter the IP address of the default gateway here. This must be an IP address on the network.

Packet Filter and Blacklists

Selecting the **Packet Filter and Blacklists** option from the Main Menu opens the **Firewall Configuration** screen.



Access Control Lists

The LoadMaster supports a "blocked list" and "allowed list" Access Control List system. Any host or network entered into the blocked list is blocked from accessing any service provided by the LoadMaster whereas any host or network entered into the allowed list is allowed to access any service provided by the LoadMaster. The allowed list is used to 'punch holes' in the blocked list.

The LoadMaster also has a packet filter. When enabled, the packet filter blocks all IP packets that are not directed at a configured port.

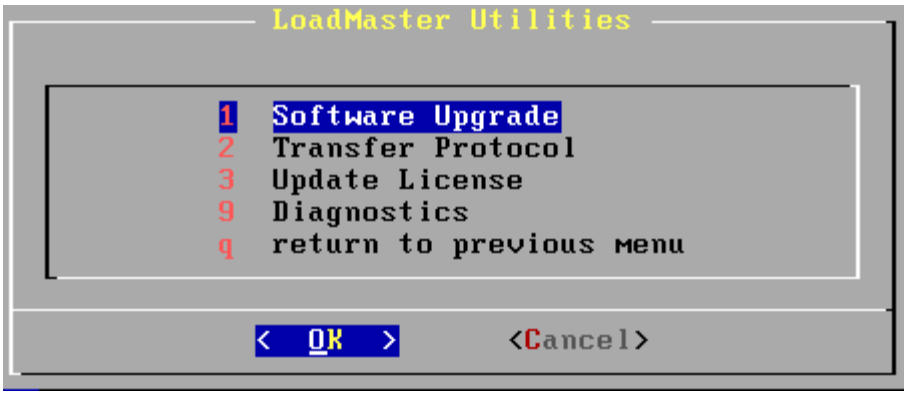
The Access Control list is only enabled when the packet filter is enabled. By default the Access Control List is disabled. This means that all source IP addresses are accepted by the LoadMaster.

The following options are available when you select the Access Control Lists option:

- **Enable Access Control Lists:** Use this toggle option to activate or deactivate the Packet Filter/Access Control List.
- **Show blocked addresses:** Lists the content of the current blocked list.
- **Add address to blocked list:** Add a host or network IP address to the blocked list. IPv4 and IPv6 addresses are allowed. A network is specified by using a network specifier, for example, specifying 192.168.200.0/24 blocks all hosts on the 192.168.200 network.
- **Delete address from blocked list:** Delete an IP address or network from the blocked list.
- **Show allowed addresses:** Lists the content of the current allowed list
- **Add address to allowed list:** Add a host or network IP address to the allowed list.
- **Delete address from allowed list:** Delete an IP address or network from the allowed 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

Selecting the **Utilities** option from the Main Menu opens the **LoadMaster Utilities** screen.



Software Upgrade

Using this option, you can install or remove patches for the operating software of the LoadMaster. A number of options are available when the Software Upgrade option is selected:

- Install Update

  With this option, you can download a patch 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 is displayed and you are asked to confirm if the patch should be installed. A copy of the current operating software is saved before the patch is installed. You can recover this software 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.

- Reset to Factory Defaults

  Reset the configuration of the appliance with the exception of the license information, usernames, and passwords.

Transfer Protocol

This option allows you 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 using the menu system and not using 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.

License Management

This option permits the input of a new license key, for example, when updating from an evaluation to a full license. Progress Kemp recommends rebooting after updating the license.

Diagnostics

This menu allows the user to perform diagnostic functions on the LoadMaster. The following options are available

- Ping Host

  You can "ping" a remote host.

- Self Test

  Tests that the Layer 4 and Layer 7 daemons are running correctly.

- View Log Files

  Allows you to view various messages (boot.msg, warning messages, standard messages, and the HA logfile) in a terminal view.

- Software Versions

  Displays the software version running on the LoadMaster.

- Enable Diagnostic Login

  Allows root access to the kernel. An ‘Xroot key’ is also supplied that enables temporary (six hours) xroot access

  ---

  Note: 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.

- Disable Diagnostic Login

  Disables the diagnostic login.

- Diagnostic Shell

  Opens a shell where you can perform diagnostic operations on the LoadMaster kernel.

  Telnet can be used as a troubleshooting tool for testing connectivity from within the Diagnostic Shell.

Note: This should only be done with the assistance of a Progress Kemp Engineer.

Reboot

Selecting the Reboot option enables you to reboot the LoadMaster.



If you select the **Yes** option, the LoadMaster reboots.

3

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:

Protocol	Port
DNS	53
FTP	21
HTTP	80
IMAP4	143
LDAP	389
POP2	109
POP3	110
SMTP	25

Protocol	Port
SNMP	161
SSL	443
TELNET	23
TFTP	69

Contents

- Top level commands
- Adaptive scheduling command level
- Health Check Command Level
- Rules command level
- Rule Edit command level
- Virtual Service (VIP) command level
- Real Server command level

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.

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.

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. Please note that UDP health checks are not supported via the console.

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.

Incquery

Append the query string to the URL before performing a match

Nocase

Ignore case when comparing strings.

Header <string>

The header field name must be matched. If no header field name is set, the default is to match the string within the URL.

Rules can be matched based on the Source IP of the client by entering ‘src-ip’ within the **Header Field** input field. The header field will be populated by the source IP of the client.

Replacement <string>

The value of the header field to be replaced.

Type <string>

- **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

Mustfail

If this rule is matched, then always fail to connect.

Onlyonflag <integer>

Only try to execute this rule if the specified flag is se

Setonmatch <integer>

If the rule is successfully matched, set the specified flag

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.

[no] Name <Name>

Specifies the “name” of the Virtual Service. To delete the name use the command <no name>.

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.

Health Check Method	Description
http	HTTP checking is enabled
https	HTTPS (SSL) checking is enabled
smtp	The Simple Mail Transfer Protocol (SMTP) is used.
nntp	The Network News Transfer Protocol (NNTP) is used.

Health Check Method	Description
ftp	The File Transfer Protocol (FTP) 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.

Check Parameters

In LoadMaster firmware version 7.2.52, the check **Interval**, **Timeout**, and **Retry Count** settings can be configured on each Virtual Service or SubVS. If any of these parameters are set to 0 they inherit the global value. Previously, these were just global settings

[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.

Persistency type	Description
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.
- **wlc**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

[no] esplog <integer>

Configure what types of logging is allowed

- 0 - Off
- 1 - User Access
- 2 - Security
- 3 - User Access + Security
- 4 - Connection
- 5 - User Access + Connection

- 6 - Security + Connection
- 7 - All

[no] inauth <integer>

Configure how clients attempting to connect to the LoadMaster are authenticated

- 0 – None: no client authentication is required
- 1 - Basic Authentication: standard Basic Authentication is used
- 2 - Form Based: clients must enter their user details within a form to be authenticated on the LoadMaster

[no] **outauth <integer>**

Configure how the LoadMaster is authenticated by the Real Servers

- 0 – None: no authentication is required
- 1 - Basic Authentication: standard Basic Authentication is used

Note:outauth is restricted by inauth.

Value can only be the same or none.

Form Based auth can use any

Right now the only available option is Basic

addvia <integer>

- 0 - Legacy Operation
- 1 - X-Forwarded-For
- 2 - None
- 3 - X-ClientSide
- 4 - X-ClientSide (No Via)
- 5 - X-Forwarded-For (No Via)
- 6 - Via Only

[no] excludedir [<string>]

List virtual directories specified within this field will not be pre-authorized on this Virtual Service and will be passed directly to the relevant Real Servers.

[no] smtpallow [<string>]

List all the permitted domains that are allowed to be received by this Virtual Service

[no] altaddress [<IPspec>]duplicate <IPspec>[no] extraports <integer>[no] sslaccel[no] mtype [<string>]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.

4

References

Unless otherwise specified, the following documents can be found at https://docs.progress.com/.

Web User Interface (WUI), Configuration Guide

LoadMaster, Product Overview

Licensing, Feature Description

RESTful API, Interface Description