Progress®
Kemp® LoadMaster®

Feature Description Routing

Generated on: 16 September 2024

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 4

Document Purpose 5

Intended Audience 5

Chapter 2: Transparency 6

Scenario 1 – The LoadMaster is Not the Default Gateway 7

Scenario 2 – Clients in the Same Subnet as the Real Servers 8

Chapter 3: Subnet Originating Requests 9

Chapter 4: Use Default Route Only 11

Chapter 5: Routing Best Practices for Two or More Networks 12

Chapter 6: Global LoadMaster Network Options 14

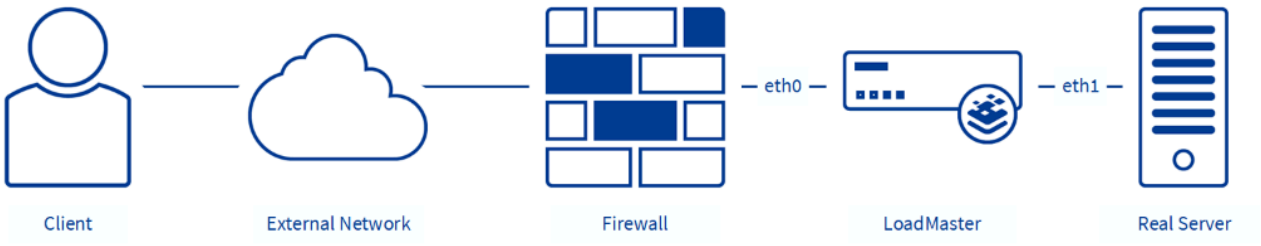
Chapter 7: References 19

1

Introduction

The LoadMaster has various routing-related options, such as transparency, Subnet Originating Requests (SOR), and Use Default Route Only.

When using the LoadMaster, you may experience different routing scenarios. The purpose of this document is to explain the different routing options and how routing can be managed inside a network.



The above network diagram shows an example standard two-armed setup:

- The client has an internal IP address of 192.168.1.x/24
- When it connects to the public site, the firewall will Network Address Translate (NAT) traffic from external networks to another IP address
- In this case, it will NAT the traffic to the 10.10.10.x/24 network
- The Virtual Service (VS) is on 10.10.10.12/24 (eth0 network)
- The Real Server is on 10.15.15.100/24 (eth1 network)

Depending on transparency and SOR, the Real Server may see traffic originating from a different IP address.

Transparency	Subnet Originating Requests	Real Server sees
Disabled	Disabled	VS address
Disabled	Enabled	LoadMaster Real Server-side interface address
Enabled	Disabled	Client IP address
Enabled	Enabled	Client IP address

If transparency is enabled, SOR does not have any effect on the routing of traffic.

Note: Health checks are always sent from the interface of the Real Server network.

Related Links

- Document Purpose
- Intended Audience

Document Purpose

Document Purpose

This document provides information on some of the routing features within the LoadMaster, such as transparency, SOR, and the Use Default Route Only option.

Intended Audience

Intended Audience

This document is intended to be used by anyone interested in finding out more information about routing in the LoadMaster.

2

Transparency

Transparency

Note: Layer 4 is always transparent.

When using **Transparency**, there are some requirements that must be met:

- The Real Server needs to have the LoadMaster as the default gateway (shared IP address when High Availability (HA) is used).
- The clients cannot be on the same subnet as the Real Server.
- The option **Use Address for Server NAT** must be enabled in the Virtual Service Standard Options. If **Subnet Originating Requests** is enabled, the global **Enable Server NAT** must be enabled (**System Configuration > Miscellaneous Options > Network Options**).

Transparency cannot be used with non-local Real Servers.

The diagrams and text below explain why these requirements must be met.

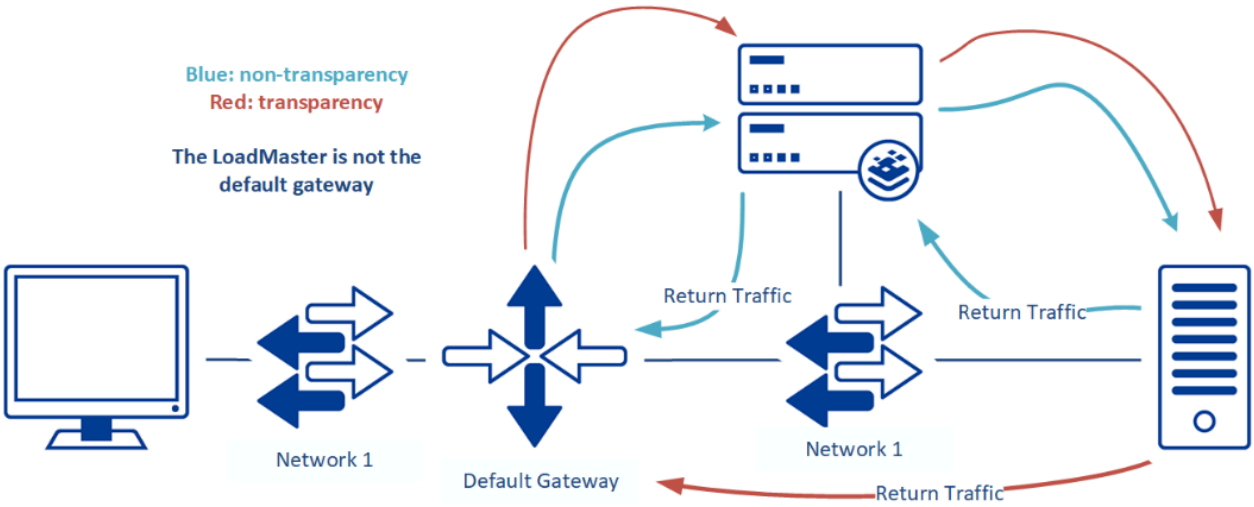
For further information on transparency, refer to the Transparency, Feature Description.

Related Links

- Scenario 1 – The LoadMaster is Not the Default Gateway
- Scenario 2 – Clients in the Same Subnet as the Real Servers

Scenario 1 – The LoadMaster is Not the Default Gateway

Scenario 1 – The LoadMaster is Not the Default Gateway



In the diagram above, neither of the flows have the LoadMaster as the default gateway. To be transparent, the default gateway of the Real Servers must be the LoadMaster. This is true whether the network configuration is one-armed or two-armed.

If the LoadMaster is not the default gateway, there is no way to ensure that traffic passes back through the LoadMaster on the way from the server to the client.

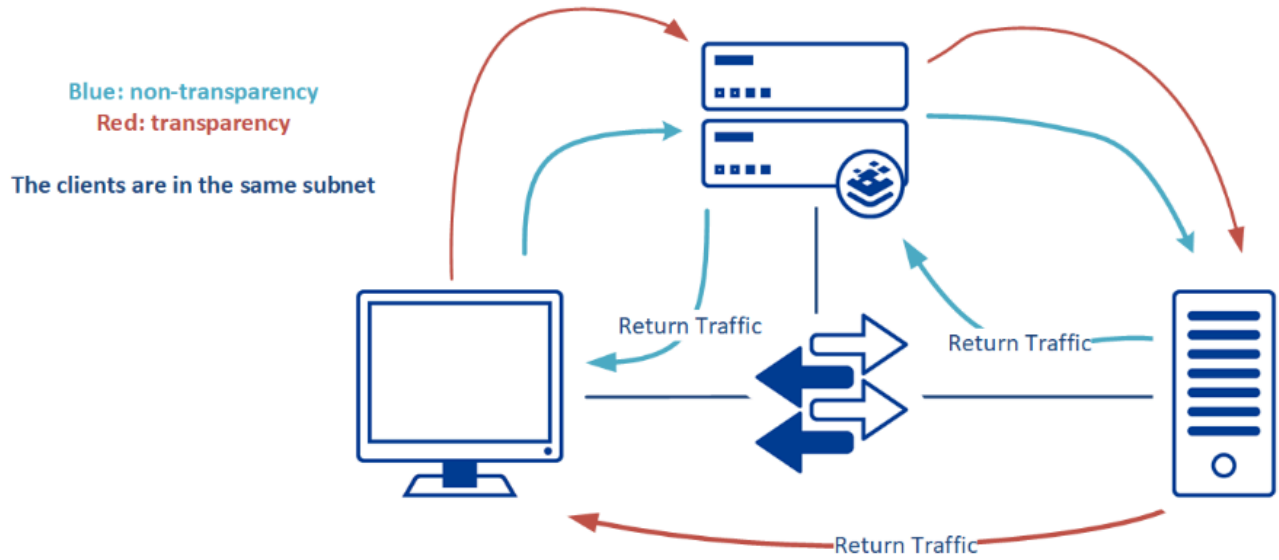
If transparency is enabled and the LoadMaster is not the default gateway, the traffic flows in the following order:

1. Client to VS
2. VS to Real Server
3. Real Server to network default gateway
4. Network default gateway to client

The connection fails between the Real Server and network default gateway. This is due to asymmetric routing. The client gets a response from the default gateway and drops the connection because it expected a reply from the LoadMaster.

Scenario 2 – Clients in the Same Subnet as the Real Servers

Scenario 2 – Clients in the Same Subnet as the Real Servers



Another requirement of transparency is that you must be browsing from a subnet other than that of the Real Servers. Again, it is to ensure that traffic passes in and out of the LoadMaster.

If you are on the same subnet as the Real Server, the return traffic simply goes directly to the client, instead of through the LoadMaster. As a result, the client expects to see traffic come from the IP address of the VS, but instead sees traffic coming from the IP address of the Real Server. When that happens, the client system ignores the traffic.

If transparency is enabled and the clients are in the same subnet as the Real Server, the traffic flows in the following order:

1. Client to VS
2. VS to Real Server
3. Return traffic from Real Server direct to client

The connection fails between the Real Server and the client due to the fact that the clients are in the same subnet as the Real Server.

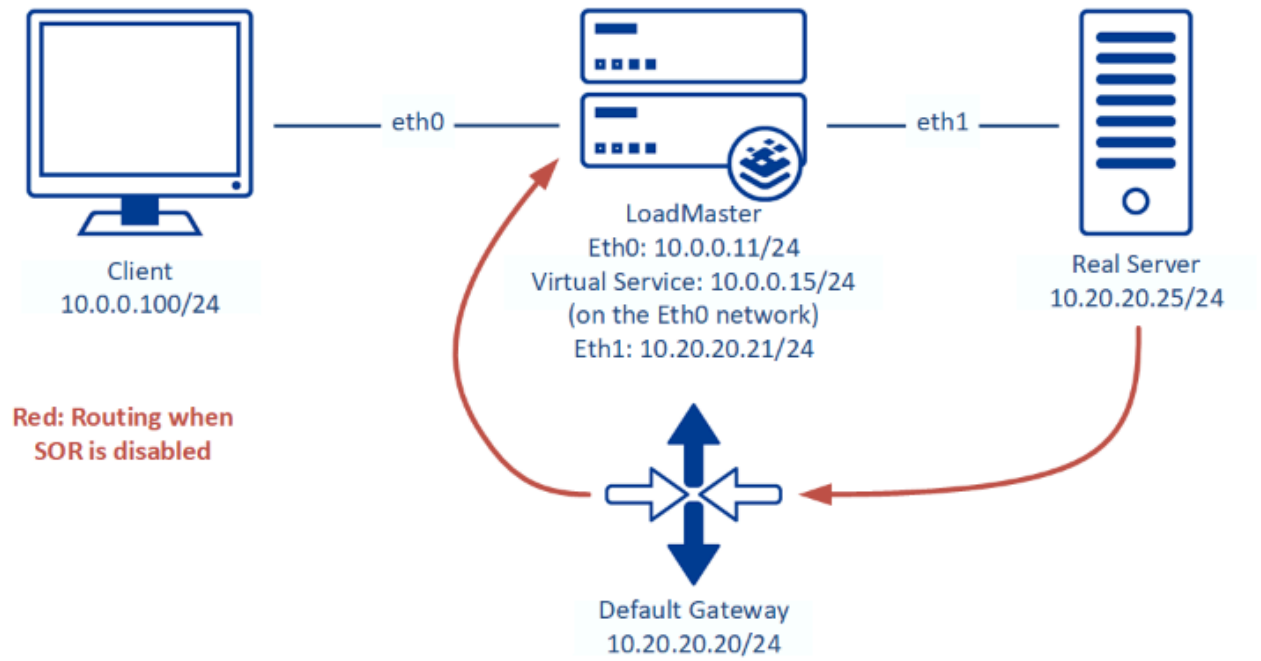
This is due to asymmetric routing. The client gets a response from the Real Server and drops the connection because it expects a reply from the LoadMaster.

3

Subnet Originating Requests

Subnet Originating Requests

When Subnet Originating Requests is enabled, the LoadMaster changes the originating IP address of the traffic. Normally, the traffic is seen being sent from the VS address. With SOR enabled, traffic is seen as being sent from the local interface address. This is needed in two-armed setups when SSL offloading is enabled.



The example diagram above is explained as follows:

- Traffic flows from the client to the VS to the Real Server
- The Real Server sees traffic originating from the 10.0.0.15/24 VS and replies using its default gateway
- The default gateway responds to the LoadMaster using the eth0 network 10.0.0.x/24
- With SOR enabled, the Real Server sees traffic originating from the eth1 interface (10.20.20.21) and replies directly to the LoadMaster

We recommend enabling SOR by default when creating VSs, unless you require transparency.

Currently, SOR does not work with non-local Real Servers. If non-local Real Servers are being used with SOR, the Real Servers see traffic as originating from the VS address.

4

Use Default Route Only

Use Default Route Only

In certain situations, it may be necessary to force the LoadMaster to always respond to certain client requests through an alternate gateway. This typically happens in a two-armed network configuration when a client that resides on LoadMaster's Real Server network connects to a VS using the VS IP address.

Because the LoadMaster 'knows' the network on which the client IP address resides, by default it attempts to respond to the client directly over the Real Server network, rather than responding through the gateway associated with the VS IP. On the client side, you will see broken connections; when the client sees the response on the local Real Server network, it rejects it because it is expecting a response from the VS IP (not the LoadMaster's IP on the local network).

The **Use Default Route Only** option (**System Configuration > Miscellaneous Options > Network Options**) enables you to work around this problem by getting the LoadMaster to use manually defined routes for specific clients instead of responding to them over directly connected networks.

Manual (or static) routes are defined on the **System Configuration > Network Setup > Additional Routes** page. For example, you have a client IP of 192.168.1.120 and it is sending requests to a VS IP of 172.16.0.30. In doing so, the client is routing the request through a firewall/gateway at 172.16.0.50, which sends the traffic on to the LoadMaster. In this case, you would add a route that specifies a client IP of 192.168.1.120 and a gateway of 172.16.0.50 so that the LoadMaster knows the 'correct' way to talk to this client.

By also enabling **Use Default Route Only**, the LoadMaster now honors the route you entered by sending traffic destined for the client at 192.168.1.120 through the gateway at 172.16.0.50, instead of using the Real Server network to talk directly to the client.

5

Routing Best Practices for Two or More Networks

When the LoadMaster is deployed in two or more networks, it is important to keep routing correct. This section contains some tips on best practices to ensure the LoadMaster is routing accurately.

The LoadMaster's User Interface (UI) is the central point of administration. If needed, you can change the UI interface. Often, customers set the UI to a management-specific subnet. You can configure this in **Certificates & Security > Remote Access**. Before setting the **Allow Web Administrative Access** option, ensure to set the **Admin Default Gateway** for the subnet that the UI is being moved to.

Note: It is critical to the security of your appliance that you use a dedicated network interface for management traffic; refer to the LoadMaster Hardening Technical Note for further details.

Changing the LoadMaster's default gateway to a different interface may be required at some point. Often using the DMZ-facing interface is the best way to configure the LoadMaster. To accomplish this, first select the **Enable Alternate GW support** check box in **System Configuration > Miscellaneous Options > Network Options**.

Once **Enable Alternate GW support** is enabled, you can select the appropriate interface and **Use for Default Gateway** can be selected. When you select this option, you are automatically redirected to a page to update the default gateway IP address.

Each Virtual Service can also be configured with its own gateway. You can do this in the **Advanced Properties** section of the Virtual Service modify screen. This means you can send Virtual Service responses through a gateway specific to each Virtual Service. Ensure that the gateway is within the same subnet as your Virtual Service.

In addition to configuring a gateway for each of the Virtual Services, ensure that responses are sent out on the correct interface. Enabling the **Use Default Route Only** check box will accomplish this. This option is also located in **System Configuration > Miscellaneous Options > Network Options**.

Without forcing the use of the **Use Default Route Only** option, this scenario can result in asymmetrical routing, which may affect users on networks directly connected to the LoadMaster who can access Virtual Services located on a different interface of the LoadMaster (particularly where a stateful firewall is used).

After you configure all of these settings and features, the LoadMaster should be able to route all traffic appropriately.

6

Global LoadMaster Network Options

This section outlines the global network options available in the LoadMaster UI and why you would need to change or enable these options. These options are located in the UI at **System Configuration > Miscellaneous Options > Network Options**.

Enable Server NAT

This option allows the LoadMaster to NAT connections coming from the Real Servers on route to the internet. After enabling the global **Enable Server NAT** check box, the **Use Address for Server NAT** check box appears for each Virtual Service in the **Standard Options** section.

By default, the LoadMaster NATs Real Server connections to the IP address of the interface designated to reach the internet. If using HA, the shared IP address of the interface facing the internet will be the NATed IP address. If the same Real Servers are configured on multiple Virtual Services (with Server NAT enabled) then connections to that respective Virtual Service are NATed, based on the destination port, to that Virtual Service's IP address.

This option is most useful for services such as SMTP, when the LoadMaster is in a public domain and when the service requires a reverse DNS check to see if the source IP address sent from the LoadMaster is the same as the Mail Exchange (MX) record of the sender.

Connection Timeout (secs)

Sets the time (in seconds) that a connection can be idle before it is closed. This is independent from the Persistence Timeout value set on the Virtual Service when Persistence is enabled. The allowed values are: 0, 60-86400. By default, this is set to 660 seconds. Setting the value to 0 will default it back to 660 seconds. The value set globally does not override any pre-existing, manually configured **Idle Connection Timeout** values that are set in the **Standard Options** section of individual Virtual Services.

The reason for altering this option is to change the default Idle Connection Timeout for Virtual Services.

It may be required for idle connections to remain active, without closing for some services such as Remote Desktop or web services with payment checkouts, for example.

Enable Non-Local Real Servers

When adding a Real Server to a Virtual Service and you get the error message **Real Server not on available network**, this means that the Real Server IP address you are trying to add does not belong to a network that has been configured on one of the LoadMaster's interfaces. This is a non-local Real Server and you must select the **Enable Non-Local Real Servers** check box to add it.

A non-local Real Server is one that resides on a network that is not local to the LoadMaster, when the LoadMaster does not have an arm or network interface that has been configured in the Real Server's network. The LoadMaster uses its **Global Default Gateway** to communicate with the non-local Real Server instead. Hence, the appropriate routing between the LoadMaster's global gateway and the Real Server's network must be in place beforehand.

When adding a non-local Real Server to a Virtual Service, you will see a check box called **Allow Remote Addresses**.

Select the **Allow Remote Addresses** check box and then proceed to add the non-local Real Server IP address as normal. Enabling non-local Real Servers prevents the need to configure multiple local interfaces on the LoadMaster for the respective Real Server networks.

Enable Alternate GW support

When disabled, the Global Default Gateway is set to eth0 by default. To allow another interface to be used as the Default Gateway, select the **Enable Alternate GW support** check box first. After enabling this option, you will see the **Use for Default Gateway** check box on all interfaces on your LoadMaster.

Once you select a new interface as the Default Gateway, you are automatically directed (as of firmware version 7.2.41.1 and higher) to configure a new Default Gateway IP Address for the new interface network. On older firmware versions, you may loose UI access if the appropriate routing to the new interface is not pre-configured on the network level. Local access (using a client on the new interface's network to connect to the new interface's IP address directly, with no need to be routed over a gateway) may be required. Refer to the following Knowledge Base article for details on allowing **Administrative WUI Access** over multiple interfaces: How to Enable WUI access for multiple interfaces.

This option may be required if a migration of interfaces is needed (especially involving the migration of the management interface) where the current global default gateway resides.

Enable TCP Timestamps

If this option is enabled, the LoadMaster includes a timestamp in the SYN of a TCP connection to the Real Servers.

If you need to know the round trip time of the TCP packets for troubleshooting, enabling timestamps helps to achieve this. However, be aware that there is a small security risk of using timestamps - the up-time of a Real Server can be estimated to determine whether security packages that require a reboot have been applied or not.

TCP timestamps should be disabled by default and you should not enable them unless instructed by a Progress Kemp Support Engineer for troubleshooting purposes.

Enable TCP Keepalives

This option is enabled by default on new firmware versions. It is designed to improve the reliability of long lived TCP connections such as SSH. The LoadMaster uses TCP keepalives to check if a client with an open TCP connection is still active or has possibly failed. This option is not normally required for HTTP/HTTPS connections.

Keepalives are non-invasive and can be enabled without risk. However, be aware that extra network traffic is generated by this option. If you require any long lived TCP connection to remain active (with the connection socket remaining open) then TCP keepalives are recommended.

Enable Reset on Close

When enabled, this option allows the LoadMaster to close a TCP connection by sending a TCP RESET instead of the conventional TCP handshake close method [FIN, ACK].

This may be required to close a TCP connection more swiftly by not waiting for the final confirmation FIN, ACK from the client or Real Server.

Subnet Originating Requests

This is the global option for enabling Subnet Originating Requests (SOR) on all configured Virtual Services and/or SubVSs.

The purpose of this setting is to change the source IP address of the connections between the LoadMaster and Real Servers. When enabled, SOR uses the IP address of the LoadMaster (the shared/management IP address in HA mode configurations) that is set on the interface that the Real Server is reachable on.

For example, the Real Server is configured on the same subnet/network as eth1 on the LoadMaster. With SOR enabled, the server sees packets sourcing from the eth1 interface IP address if the LoadMaster is in single mode. If the LoadMaster is in HA mode, the Real Server sees packets sourcing from the HA shared/management IP address.

SOR is normally required in two-armed configurations where the Virtual Service is on a different network to the Real Server. This can help to prevent back-end asymmetric routing. For more information on SOR, refer to the Subnet Originating Requests section.

Enforce Strict IP Routing

The **Enforce Strict IP Routing** option operates in a similar way to the **Packet Routing Filter** option in **System Configuration > Network Setup > Packet Routing Filter**.

You would only need to enable **Enforce Strict IP Routing** if you want to only allow IP frames to be received from a host (a Real Server, for example) over an interface on the LoadMaster where the initiating connection was originally made.

For example, a connection to a Real Server from the LoadMaster is made over interface 1 (eth0). With **Enforce Strict IP Routing** enabled, response IP frames returned from the same Real Server will only be accepted on eth0.

Handle non HTTP Uploads

The LoadMaster has been optimized with HTTP workloads in mind. Enabling the **Handle non HTTP Uploads** option allows non-HTTP uploads to work correctly. For example, FTP uploads may require this option to be enabled.

Enable Connection Timeout Diagnostics

By default, this option has been disabled to prevent excess logs from being generated on the LoadMaster.

When troubleshooting any potential Connection Timeout issues on the LoadMaster, enabling this option adds more diagnostic information about the timed-out connection to the system logs. Only enable this option when requested to do so by a Progress Kemp Support Engineer.

Legacy TCP Timewait handling

Enabling the **Legacy TCP Timewait handling** option reverts back to the legacy mode of reusing TCP timewait connections. This restores the default settings of tcp_tw_recycle and tcp_tw_reuse. The new method of reusing TCP timewait connections has been optimized for systems with a large number of connections. Hence, it is not normally recommended to enable **Legacy TCP Timewait handling** unless instructed by a Progress Kemp Support Engineer.

Enable SSL Renegotiation

This setting is enabled by default in new firmware versions. It enabled the LoadMaster to permit clients to automatically renegotiate during an SSL handshake in the event of a timeout or error occurring. Disabling this option causes the SSL connection to terminate if a renegotiation is requested by the client.

Force Real Server Certificate Checking

By default, the LoadMaster does not check the SSL certificate provided by the Real Server when traffic is being re-encrypted between the LoadMaster and the Real Server. Enabling the **Force Real Server Certificate Checking** option forces the LoadMaster to verify the SSL certificate on the Real Server before establishing a successful SSL connection. This may cause a slowdown in SSL connections being established under high traffic conditions.

Size of SSL Diffie-Hellman Key Exchange

This option dictates the strength of the shared key to be generated between the client and the LoadMaster, using the Diffie-Hellman Key exchange method for all SSL transactions on the LoadMaster. Currently, the highest configurable key size is 2048 bits (2k keys). Selecting the larger key size improves security but it may have a negative impact on performance under high SSL traffic loads.

Use Default Route Only

This setting works best in conjunction with a **Default Gateway** configured on the Virtual Service in the **Advanced Properties** section. The **Use Default Route Only** option is a way of overriding the LoadMaster's default routing metric order preference. It is important to know that the LoadMaster's routing metric order preference by default is as follows:

0. Locally connected interface

1. Static/additional routes (if defined)

2. Default Gateway assigned to a Virtual Service (if defined)

3. Global Default Gateway

When **Use Default Route Only** is enabled, and a Default Gateway has been added to a Virtual Service, local traffic is no longer routed out of their respective local interface on the LoadMaster (as per metric 0 above). Local traffic (in addition to non-local traffic) is now forcefully routed out of the **Default Gateway** set

on the Virtual Service.

Example 1 - **Use Default Route Only** disabled:

This example is for a two-armed setup involving a client on the eth0 network (192.168.0.0/24) with the Virtual Service and Real Server on the eth1 network (10.0.0.0/16).

Note: The same applies to a one-armed setup.

If **Use Default Route Only** is disabled and the **Default Gateway** for the eth1 network is assigned to the Virtual Service, the response from the server returns to the LoadMaster on eth1. Then, the response from the LoadMaster back to the client is routed out of eth0 (the local interface connected to the client).

Example 2 - **Use Default Route Only** enabled:

This example has the same layout as described in Example 1, but **Use Default Route Only** is enabled and with the **Default Gateway** of the eth1 network configured on the Virtual Service, the return traffic to the client is no longer routed on eth0 (the local interface of the client). It is now routed out of the eth1 gateway, as specified on the Virtual Service.

This option may be needed to prevent potential asymmetric routing or to force all response traffic back out to a certain gateway for security/routing purposes. As you may have noticed from the examples above, enabling the **Use Default Route Only** option has an implication on the LoadMaster's preferred routing metrics.

When troubleshooting, if you notice that you cannot access your Virtual Service from a certain client or network, this is likely because the routing has not been configured correctly. Enabling or disabling **Use Default Route Only**, along with assigning a **Default Gateway** to your Virtual Service, may be a potential solution.

HTTP(S) Proxy

You can specify a HTTP(S) proxy here, when required to do so. When configured, all outbound response HTTP/HTTPS traffic is sent to this proxy from the LoadMaster. The current supported format for enabling this option is IPAddress:Port.

7

References

References

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

Transparency, Feature Description