Progress®
Kemp® LoadMaster®

Feature Description Transparency

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 5

Document Purpose 6

Intended Audience 6

Chapter 2: Transparency 7

Implications of Network Transparency 8

Layer 4 and Layer 7 9

Direct Server Return 9

Transparency Requirements 9

Enable Layer 7 Transparency 11

Transparency Considerations 11

Cloud Transparency 12

Chapter 3: Non-Transparency 14

Subnet Originating Requests 15

Chapter 4: Alternate Source Addresses. 16

Chapter 5: Troubleshooting. 18

Unable to Connect to Real Servers using Remote Desktop Protocol (RDP) 18

One-Arm Setup. 19

Two-Arm Setup. 19

Chapter 6: References 21

1

Introduction

Introduction

To place a load balancer in a network effectively and utilize Layer 7 functionality, two things need to happen:

- Traffic needs to flow through the load balancer on the way in
- Return/response traffic needs to flow through the load balancer on the way out

To meet the requirements above there are two options; Layer 7 (L7) Transparency or L7 Non-Transparency. When a packet arrives at the LoadMaster, the source IP address of the packet is that of the client and the destination IP address is that of the Virtual Service. When L7 Transparency is enabled the packet is passed to the Real Server with the same source IP address of the packet but with the destination IP address changed to be the that of the Real Server.

With L7 Non-Transparency when the packet is being sent to the Real Server the LoadMaster will change the destination IP address of the packet to be the Real Server (as it does in L7 Transparent Mode) but it will also change the source IP address from the original client IP address to the IP address of the Virtual Service.

Related Links

For details, see the following topics:

- Document Purpose
- Intended Audience

Document Purpose

Document Purpose

This document serves as an explanation of network transparency, its implications and other related concepts.

Intended Audience

Intended Audience

This document is intended to be used by anyone who is interested in learning more about transparency and the LoadMaster.

2

Transparency

Transparency

Refer to the following sections for details on transparency.

Related Links

For details, see the following topics:

- Implications of Network Transparency
- Layer 4 and Layer 7
- Direct Server Return
- Transparency Requirements
- Enable Layer 7 Transparency
- Transparency Considerations
- Cloud Transparency

Implications of Network Transparency

Implications of Network Transparency

To decide whether or not network transparency is needed, ask this question: does the IP address of the client requests need to appear in the logs?

If the answer is yes, then network transparency may be required (other options may be to use **X-Forwarded-For** or Direct Server Return). If transparency is required, the LoadMaster will need to be configured and the network will need to be designed in a certain way, which this document will describe.

If the answer is no, then there is a little more flexibility in how the network can be configured.

The table below shows a matrix of the advantages and disadvantages of transparency.

Pro/Con	Transparent	Non-Transparent
Pro	Preserves the source IP address	Can browse from the same subnet as the Real Server
Pro	Works with Layer 4 (L4) and L7	No need to change the default gateway
Con	Cannot browse from the same subnet as the Real Servers	The source IP address is not preserved (but X-Forwarded-For header can be used)
Con	The default gateway must be the LoadMaster	Only available for L7
Con	Cannot have non-local Real Servers	
Con	Cannot use with SSL re-encryption	

The transparency settings are based on making sure that traffic moves from the Real Server back to the client through the LoadMaster. This type of symmetric routing, that is, going in and out of the LoadMaster, is an inherent requirement of all load balancers (with the exception of employing direct server return, a feature which the LoadMaster supports, which has its own set of limitations).

Layer 4 and Layer 7

Layer 4 and Layer 7

The LoadMaster makes a differentiation between L4 and L7 handling. This refers to Layer 4 and Layer 7 of the OSI model. Layer 4 involves TCP/UDP ports, and Layer 7 refers to the higher-level awareness of the LoadMaster, such as with HTTP cookies, SSL acceleration, and content switching. For all Layer 4 Virtual Services, the only behaviour available is transparent networking.

Layer 4 is any load balanced traffic that does not involve cookie persistence, SSL acceleration, content switching or content switching rules. Layer 4 does include SRC (source IP) address persistence.

Virtual IP Address	Prot	Name	Layer
10.154.11.71:80	tcp	Example L7	L7
10.154.11.73:80	udp	Example L4	L4

It is possible to tell if a Virtual Service is using L4 or L7 handling by looking at the Virtual Service in **Virtual Services** and **View/Modify Services** in the main menu of the LoadMaster Web User Interface (WUI). It will indicate what layer it is operating on in the **Layer** column.

Any time any cookie persistence, SSL acceleration, or content switching options are used, the traffic automatically becomes L7.

Direct Server Return

Direct Server Return

Direct Server Return (DSR) is a method whereby the LoadMaster only handles the inbound traffic flow. The servers respond directly to the clients, bypassing the LoadMaster on the way out.

For further information on Direct Server Return, refer to the **Configuring DSR, Technical Note** on the Documentation Page.

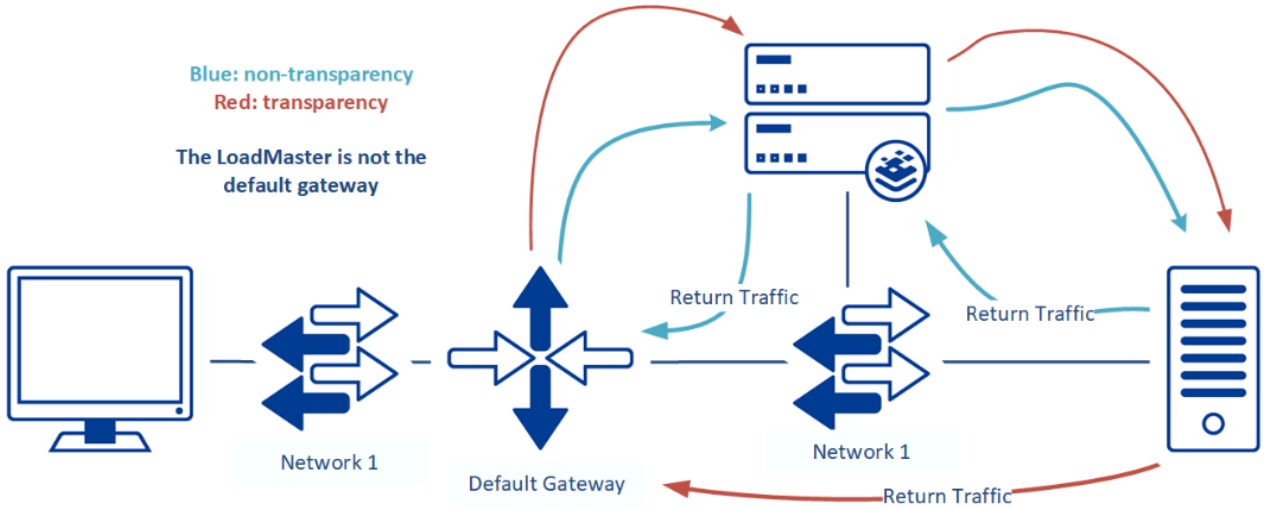
Transparency Requirements

Transparency Requirements

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

- The Real Server needs to have the LoadMaster as the default gateway
- The clients cannot be on the same subnet as the Real Server

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

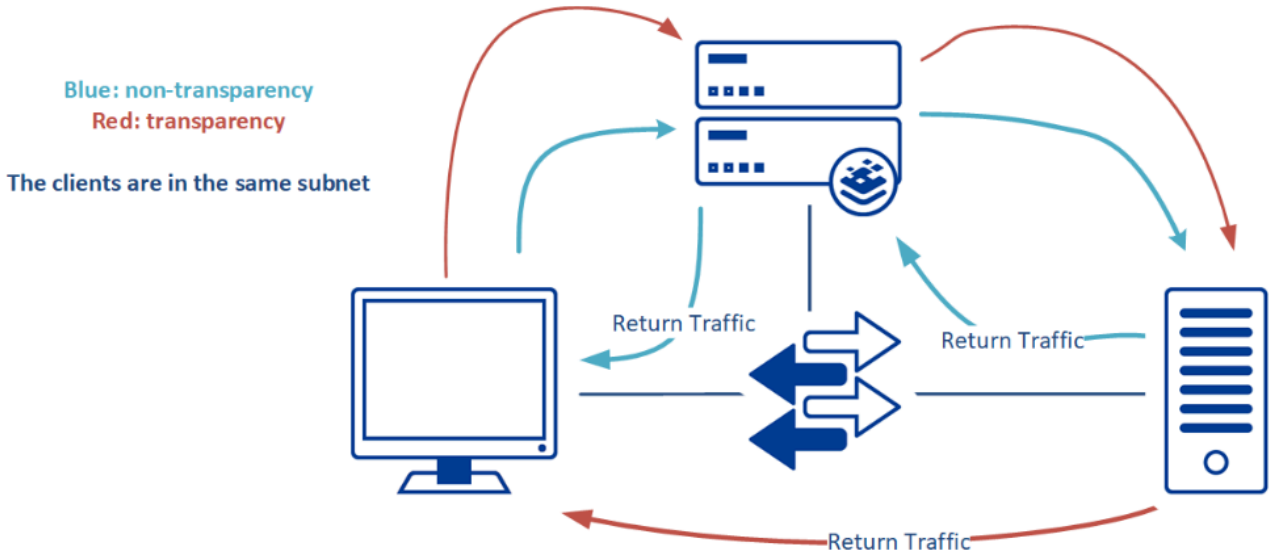


In the diagram above, neither of the flows have the LoadMaster as the default gateway. In order to be transparent, the default gateway of the Real Servers must be the LoadMaster. This is true whether the network configuration is one-armed or two-armed. If the LoadMaster is not the default gateway, there is no way to ensure that traffic passes through the LoadMaster on the way from the server to the client, and the LoadMaster cannot do its job.

Here is the flow of traffic if transparency is enabled and the LoadMaster is not the default gateway:

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

The connection will fail between the Real Server and network default gateway.



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 will simply go directly to the client, instead of through the LoadMaster. As a result, the client is expecting to see traffic come from the IP address of the Virtual Service, but instead will see traffic coming from the IP address of the Real Server. When that happens, the client system ignores the traffic.

Here is the flow of traffic if transparency is enabled and the clients are in the same subnet as the Real Server:

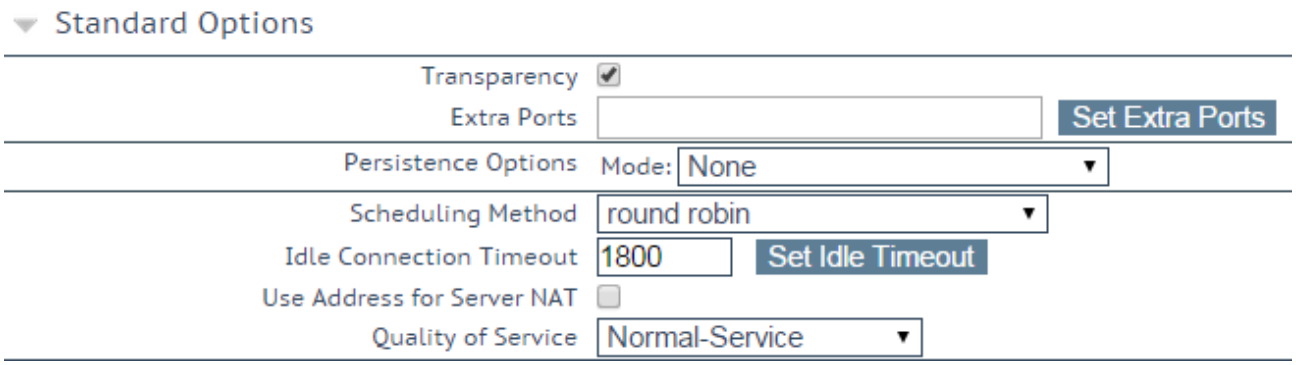
1. Client to Virtual Service
2. Virtual Service to Real Server
3. Return traffic from Real Server direct to client

The connection will fail between the Real Server and the client due to the fact that the clients are in the same subnet as the Real Server (the client expects a response from the Virtual Service address (not the Real Server address)).

Enable Layer 7 Transparency

Enable Layer 7 Transparency

Each L7 Virtual Service has the capability of being transparent or non-transparent. If the service is an L7 service, whether it is using some of the L7 handling features, or if it is forced, the following check box will appear in the **Standard Options** section of the Virtual Service modify screen.



This check box governs the transparency setting for the specific Virtual Service. When it is ticked, transparency is enabled.

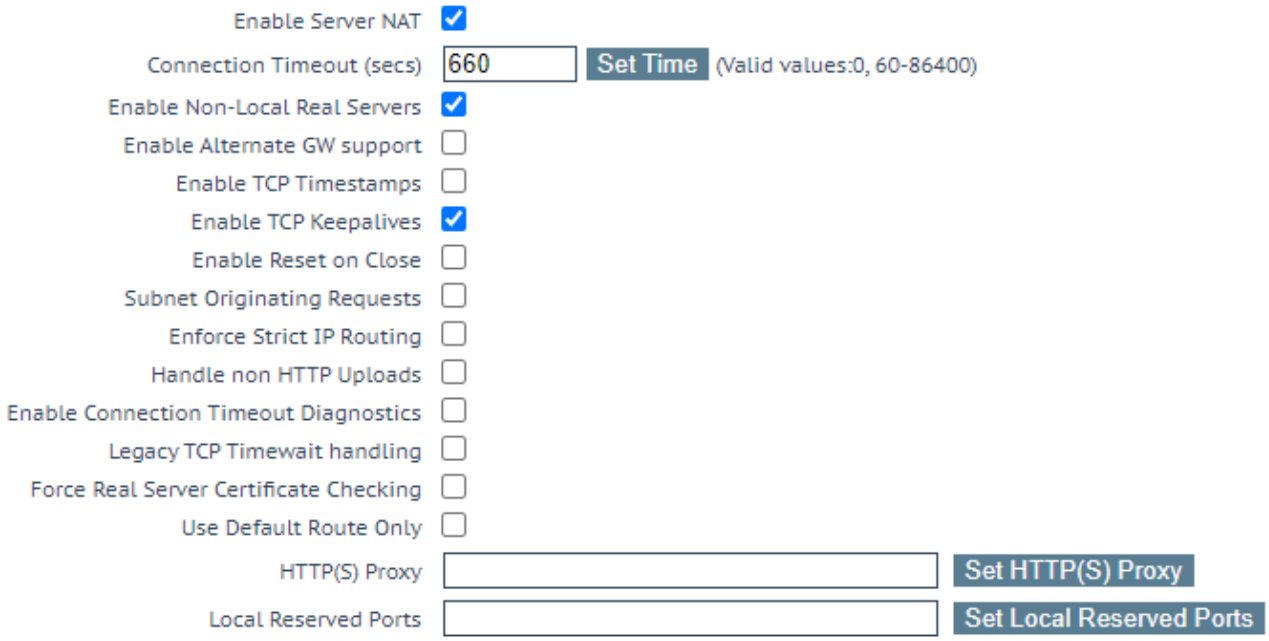
Even if transparency is disabled in the LoadMaster configuration, Layer 4 traffic is always transparent.

Transparency Considerations

If using a single-armed configuration (that is when the Virtual Services and the Real Servers are on the same subnet) and employing transparency, SNAT (Source NAT) should be disabled. SNAT is the mechanism that allows servers behind the LoadMaster to make outbound connections in a two-armed configuration. It acts

much like an office firewall, by “masquerading” the outbound connections as coming from a public IP address. In a single-armed configuration, SNAT is not necessary, although it normally does not interfere with regular operations.

There is an exception - when using transparency, the LoadMaster is the default gateway for the Real Servers, and you want to access the Real Servers directly. SNAT will “break” connections directly to the servers by attempting to masquerade those connections, so SNAT should be disabled.



To disable SNAT, go to **System Configuration > Miscellaneous Options > Network Options** in the WUI. Simply uncheck the **Enable Server NAT** box, and SNAT is disabled. Servers will now be directly accessible.

Cloud Transparency

Cloud Transparency

If you can set the Real Server to route return traffic to the LoadMaster interface, transparency can be set for the Virtual Service. Using routing tables may be required to prevent asymmetric routing.

Note: Transparency currently cannot be used in conjunction with cloud High Availability (HA) because there is no shared IP address.

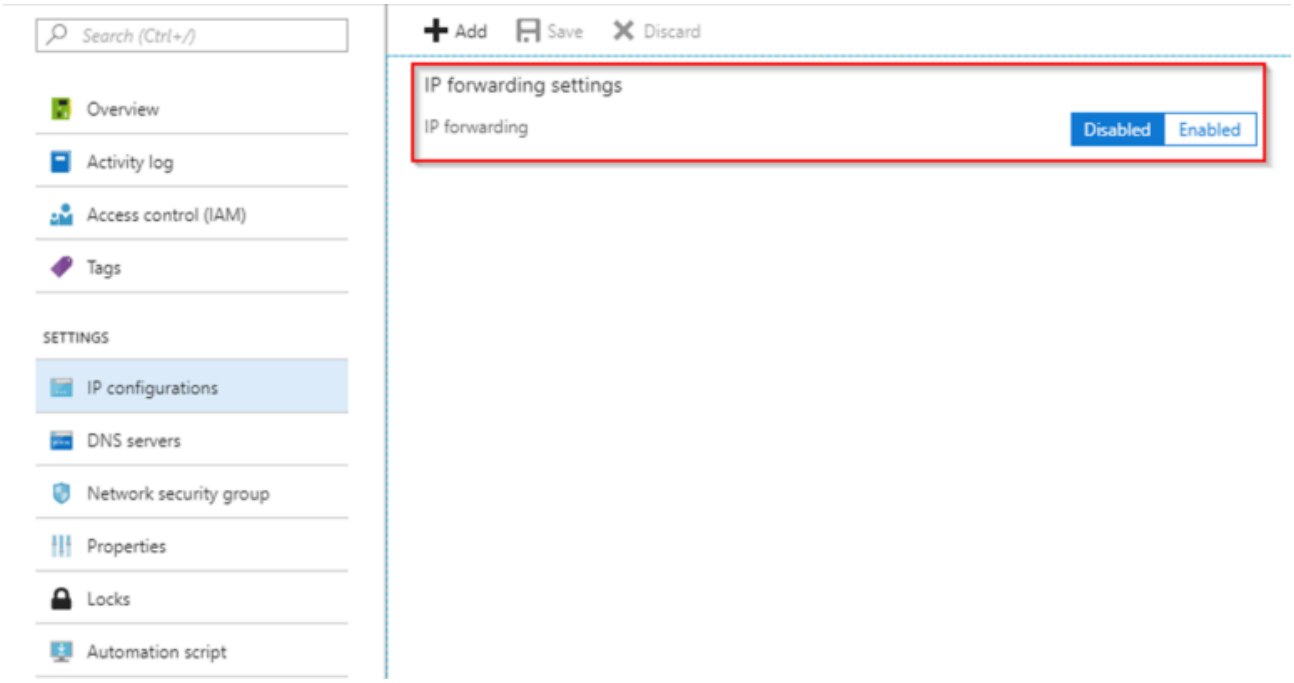
If you are seeing the following scenario:

- With transparency disabled, the LoadMaster sends traffic to a healthy Real Server as normal and the Real Server responds.
- With transparency enabled, the LoadMaster sends traffic to a healthy Real Server as normal. However, no traffic is seen on the Real Server.

This is due to **IP forwarding** in Azure or source/destination checks in Amazon Web Services (AWS).

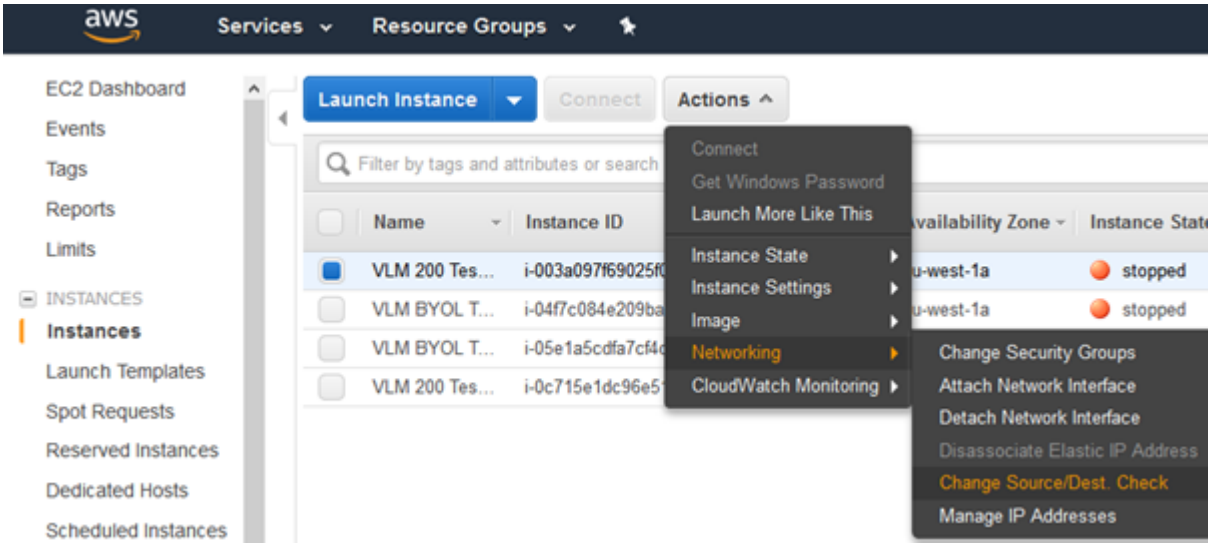
For further information on IP forwarding in Azure, refer to the following Microsoft content: Enable or disable IP forwarding.

You can find this in the Azure portal by going to: **Home > <*Virtual LoadMaster (VLM)*> > Networking > <*VLM NIC/Interface*> > IP configurations**.



Set **IP forwarding** to **Enabled**.

For further information on **Source/Destination Checks** in AWS, refer to the following AWS content: Disabling Source/Destination Checks.



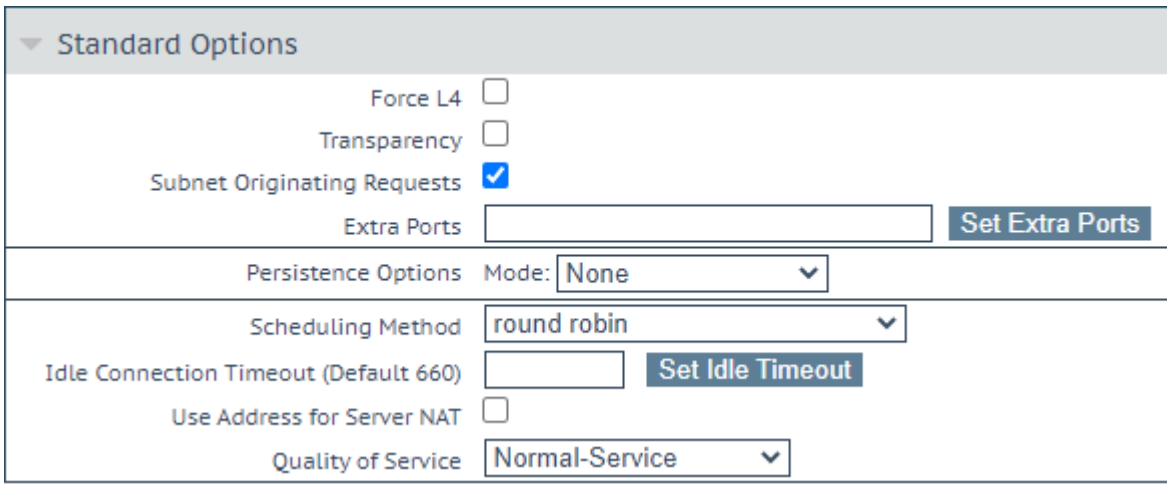
You can find this in the AWS portal by selecting the EC2 instance (the LoadMaster) and going to: **Actions > Networking > Change Source/Dest. Check**. This must be disabled.

3

Non-Transparency

Non-Transparency

There are two main benefits to using non-transparency. The first benefit is that it allows you to browse your Virtual Service when the client is on the same subnet. The other advantage is that the LoadMaster does not need to be the default route in a one-armed configuration. Traffic is forced through the LoadMaster on the way out by making the request appear as if it came from the LoadMaster itself (which is why the IP address is hidden).



Transparency is disabled by default in the LoadMaster.

If cookie persistence, content switching or SSL acceleration is employed for a given Virtual Service, the

Force L4 option disappears. As mentioned previously, the chief disadvantage is that the source IP address of the client is hidden, although for HTTP and HTTPS offloaded/re-encrypted Virtual Services it is forwarded in a separate HTTP header. Refer to the following Knowledge Base article for further details: How to Add an X-Forwarded-For Header and Configure IIS Logging.

Note: If the client is local to the Virtual Service, transparency is automatically disabled. If using two VLANs and the netmasks of the two VLANs do not differentiate between them, the LoadMaster decides the client is local and disables transparency. This is not only the case with VLANs - it can also happen when using the same networks on multiple interfaces.

Related Links

For details, see the following topics:

- Subnet Originating Requests

Subnet Originating Requests

Subnet Originating Requests

There is a check box called **Subnet Originating Requests** in **System Configuration > Miscellaneous Options > Network Options**. When transparency is turned off for a Virtual Service, the source IP address of the connections to the Real Servers is the Virtual Service. When the **Subnet Originating Requests** check box is selected, the source IP address will look like the local interface address on the Real Server's subnet.

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

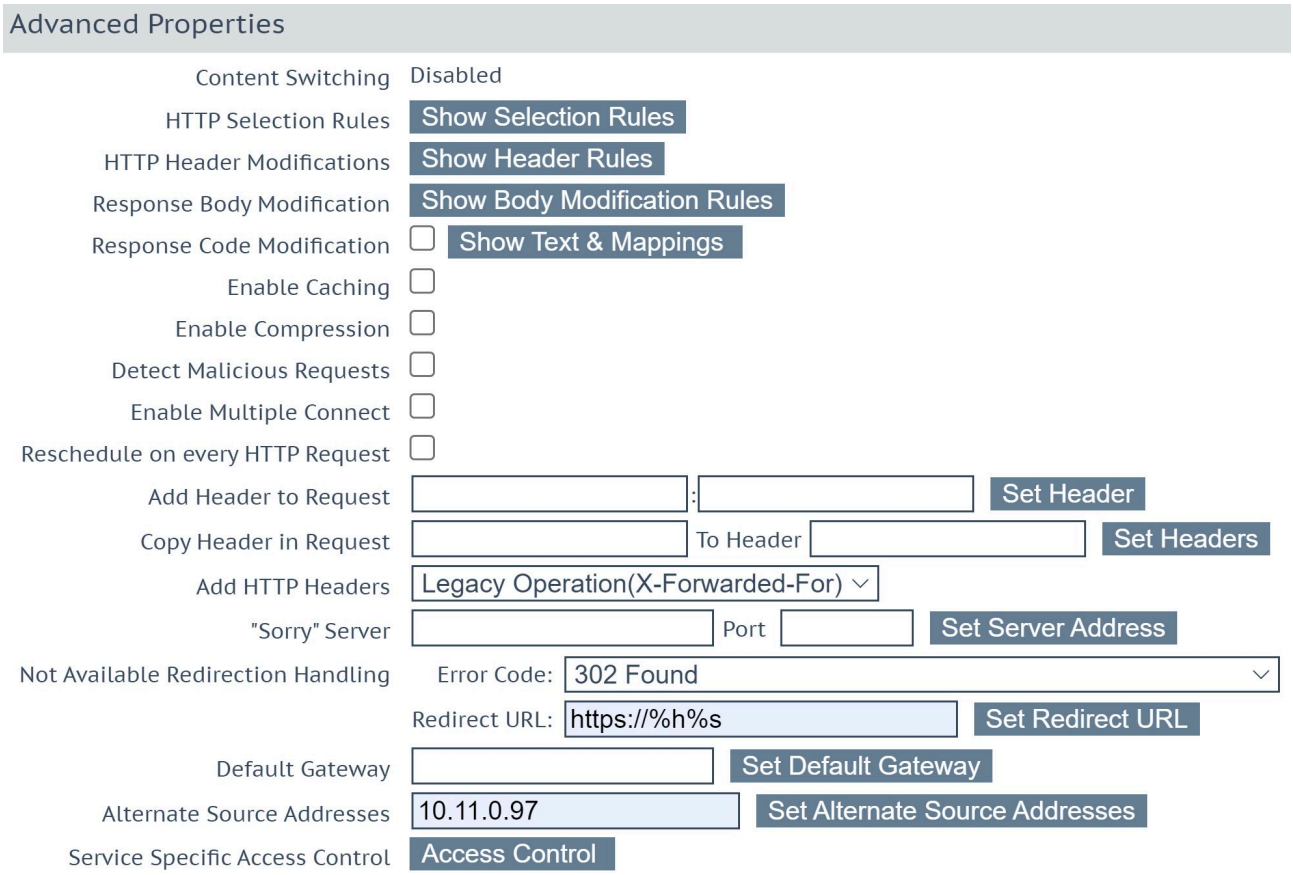
Transparency takes precedence over SOR. If transparency is enabled, SOR is not used and does not have any effect on the routing of traffic.

4

Alternate Source Addresses

Alternate Source Addresses

If required, alternate source addresses can be specified per Virtual Service.



This field is available in the **Advanced Properties** section of the Virtual Service modify screen.

Note: This option is only available if the **Allow connection scaling over 64K Connections** option is enabled in the **System Configuration > Miscellaneous Options > L7 Configuration** screen.

If no list is specified, the LoadMaster will use the IP address of the Virtual Service as its local address. Specifying a list of **Alternate Source Addresses** ensures that the LoadMaster will use these addresses instead.

Using an **Alternate Source Address** will allow more source ports to be used. With one IP address we are limited to 64,000. In order to use more, at least two additional IP addresses must be added in this field. One of the IP addresses can be the Virtual Service address.

5

Troubleshooting

Troubleshooting

Refer to the following sections for details on how to troubleshoot issues relating to transparency.

Related Links

For details, see the following topics:

- Unable to Connect to Real Servers using Remote Desktop Protocol (RDP)

Unable to Connect to Real Servers using Remote Desktop Protocol (RDP)

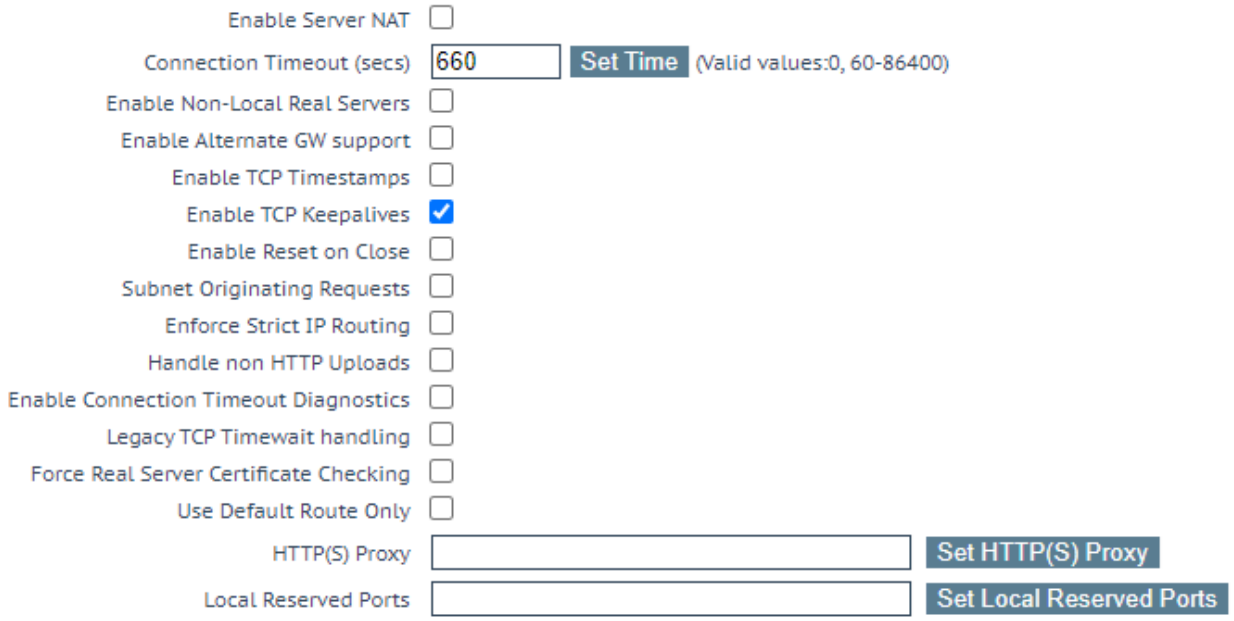
Unable to Connect to Real Servers using Remote Desktop Protocol (RDP)

After enabling transparency, RDP connections may not work. To resolve this problem, refer to the relevant section below depending on your setup.

One-Arm Setup

If you have a one-arm setup – disable Server Network Address Translation (SNAT). This will allow access to Real Servers using RDP. To do this, follow the steps below in the LoadMaster:

1. In the main menu of the LoadMaster WUI, select **System Configuration > Miscellaneous Options > Network Options**.



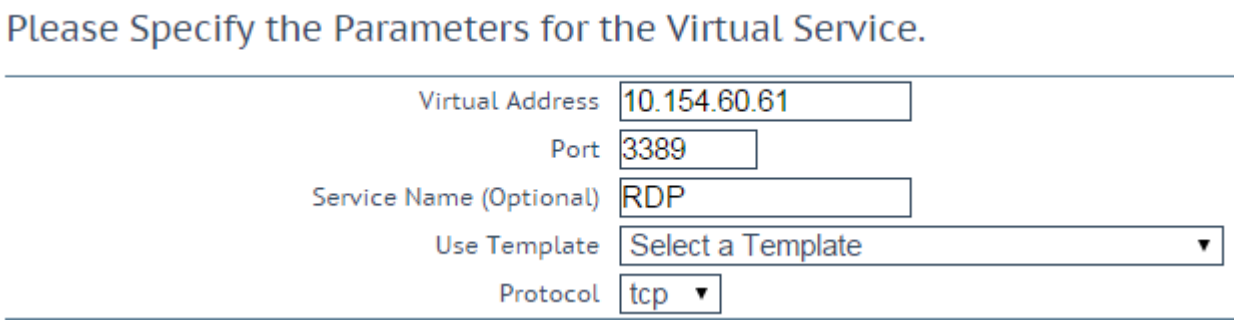
2. Remove the tick from the **Enable Server NAT** check box.

Two-Arm Setup

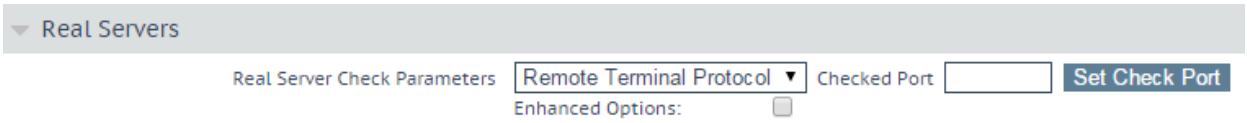
Two-Arm Setup

If you have a two-arm setup – create an RDP Virtual Service by following the steps below in the LoadMaster WUI:

1. In the main menu, select **Virtual Services > Add New**.



2. Create a Virtual Service on port **3389**.



3. Expand the **Real Servers** section and add the Real Server to be accessed.

After this Virtual Service has been created, the Real Server is accessible using RDP.

6

References

References

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

Web User Interface (WUI), Configuration Guide

Configuring DSR, Technical Note