Configuring DSR

Technical Note

UPDATED: 25 April 2021

Copyright Notices

Table of Contents

1 Introduction

Direct Server Return (DSR) is a method whereby traffic hits the LoadMaster on the way in and bypasses the LoadMaster on the way out.

The primary advantage of DSR is that the LoadMaster only handles a portion of the work associated with load balancing, specifically the inbound traffic. The servers respond directly to the clients, bypassing the LoadMaster on the way out.

If the particular traffic profile for a site is for every packet in, eight packets are sent out, this would result in the LoadMaster handling around 87% less traffic than it would without DSR.

For DSR to work, the Virtual IP (VIP) address on a Real Server 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. On Windows this involves creating a loopback adapter with specific configuration parameters. Refer to the **Configuring a VIP on the loopback interface on Linux** and **DSR Configuration on Windows** sections for detailed steps on how to do this in both operating systems.

When you create the Virtual Service, enable **Force L4** in **Standard Options** and select **Direct return** as the **Forwarding method** when adding the Real Server. This means that the LoadMaster just routes the packets from a client to a Real Server 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.

The table below shows an example of DSR steps.

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

1.1 Related Firmware Version

Published with LMOS version 7.2.48.4 LTS. This document has not required substantial changes since 7.2.48.4 LTS. However, the content is in sync with the latest LoadMaster LTS firmware.

2 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 <VirtualServiceIPAddress> 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

> If the machine reboots, this configuration will no longer be available. To set this permanently, some Linux configuration files need to be edited. Steps on how to do this vary from distribution to distribution.

The next step is to disable invalid ARP replies. Add the following to the /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

3 DSR Configuration on Windows

For Windows, it is typically best to use the loopback address. However, to use the loopback address, the loopback adapter needs to be added first. To add the loopback adapter for the relevant version of Windows and to configure the VIP of the loopback interface, follow the instructions in the **Add a loopback interface on Windows Server 2012, 2016 and 2019** section.

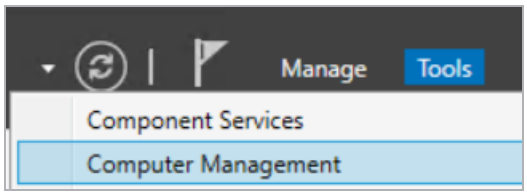
1.

3.1 Add a loopback interface on Windows Server 2012, 2016 and 2019

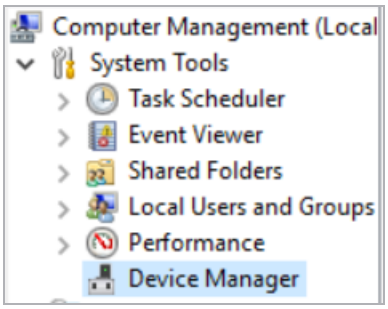
To add a loopback adapter on Windows Server 2012, 2016 and 2019, follow the steps below:

1. Click **Start** and select **Server Manager**.

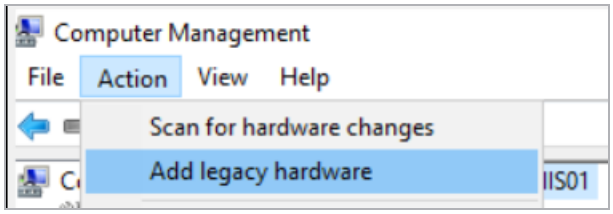
2. Click **Tools** and select**Computer Management**.



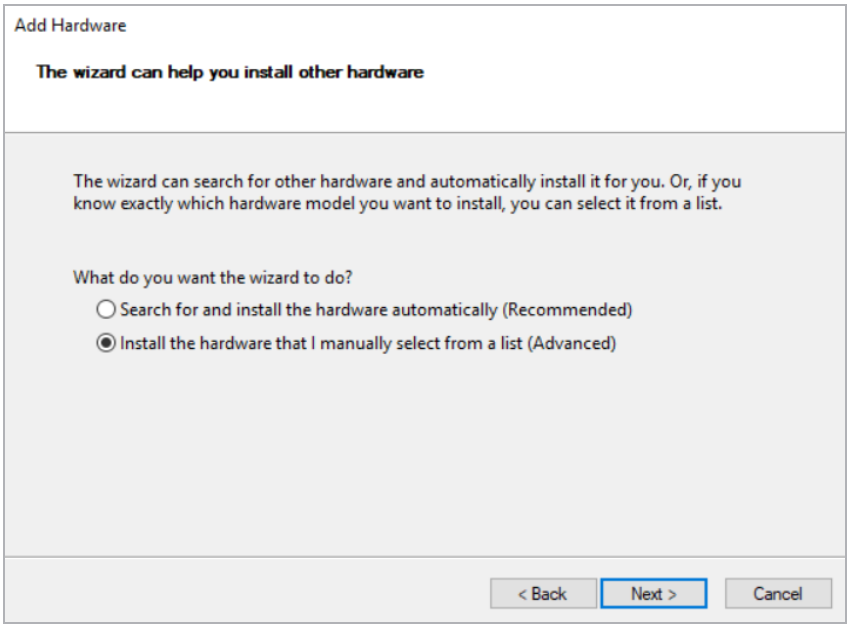
3. Click **Device Manager**.



4. Click the computer name, click **Action** from the top menu bar and select **Add Legacy Hardware**.

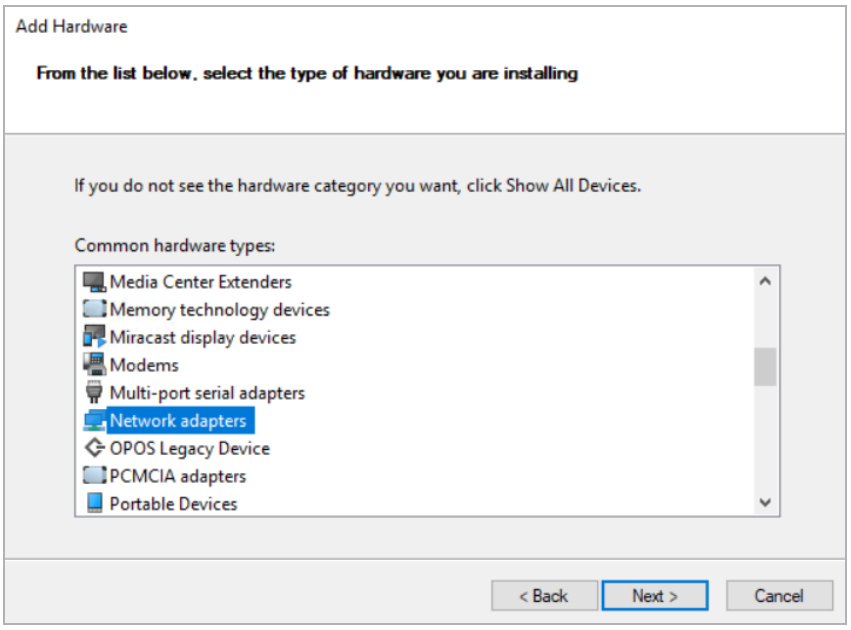


5. Click **Next**.

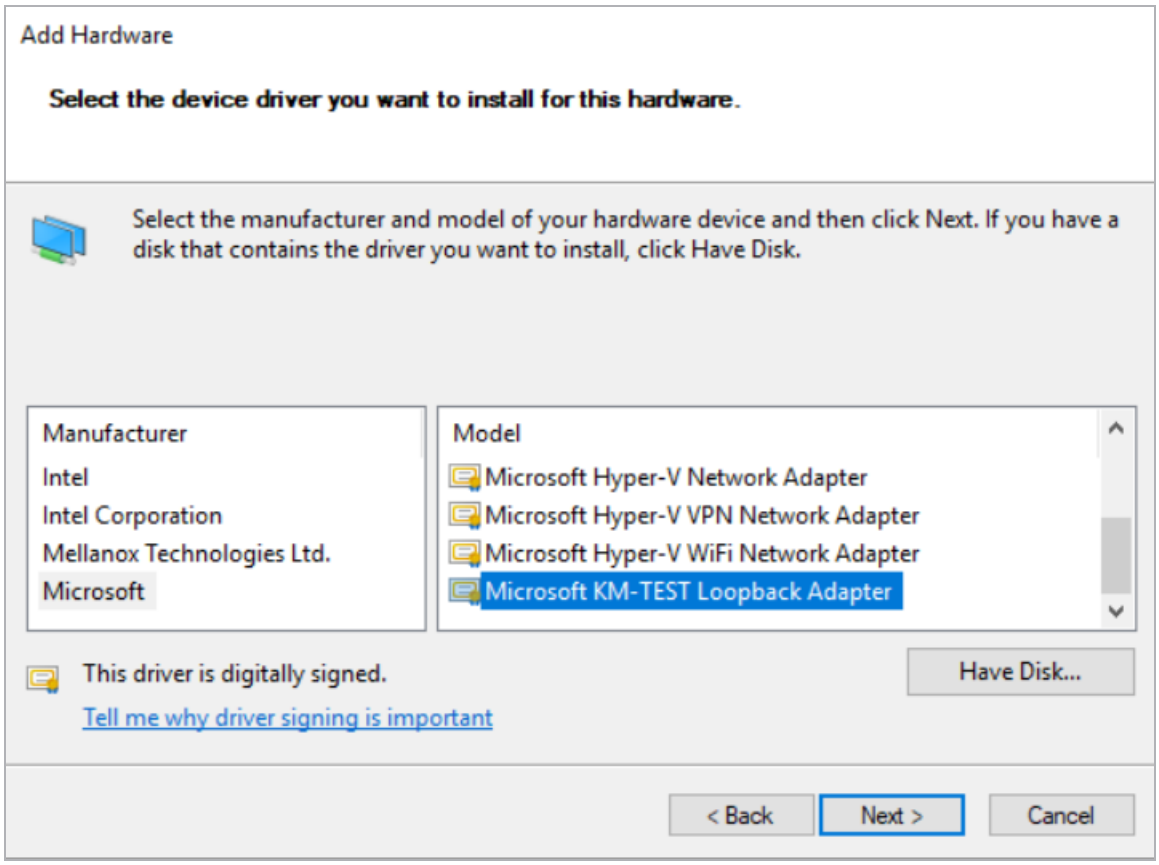


6. Select **Install the hardware that I manually select from a list (Advanced)**.

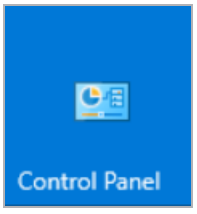
7. Click **Next**.



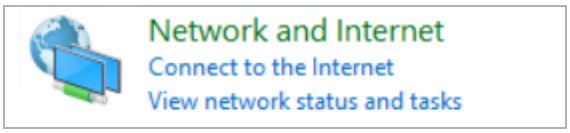
8. Select **Network adapters**.
9. Click **Next**.
10. Select **Microsoft** on the left.



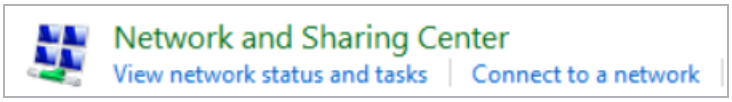
11. Select **Microsoft KM-TEST Loopback Adapter** on the right.
12. Click **Next**.
13. Click **Next** again.
14. Click **Finish**.
15. Click **Start** and select **Control Panel**.



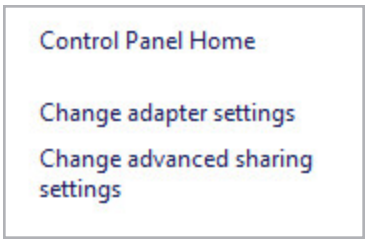
16. Click **Network and Internet**.



17. Click **Network and Sharing Center**.



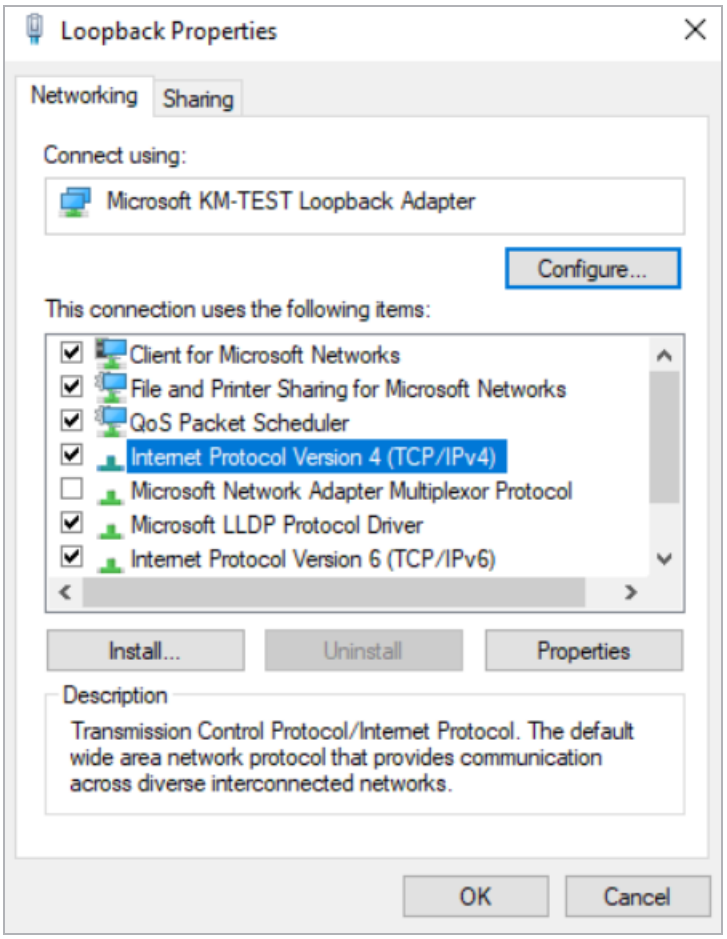
18. Click **Change adapter settings**.



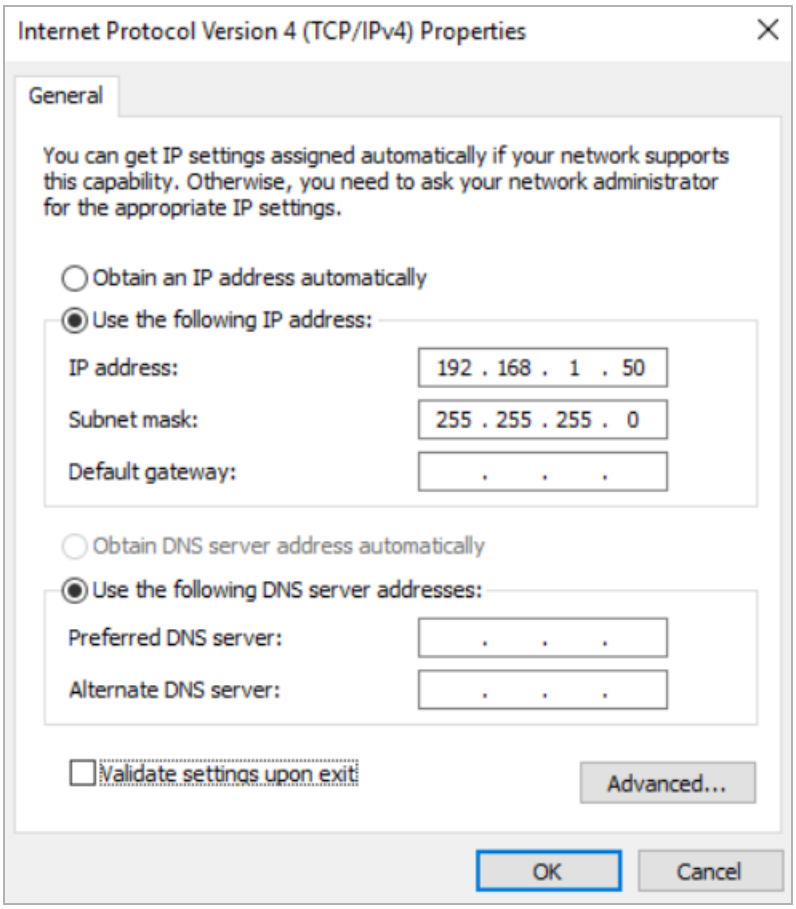
It is a good idea to rename the adapters so that they are distinguishable, for example; rename the new adapter to **loopback** and the real network adapter to **network**.

19. Configure the loopback adapter with the Virtual Service IP.

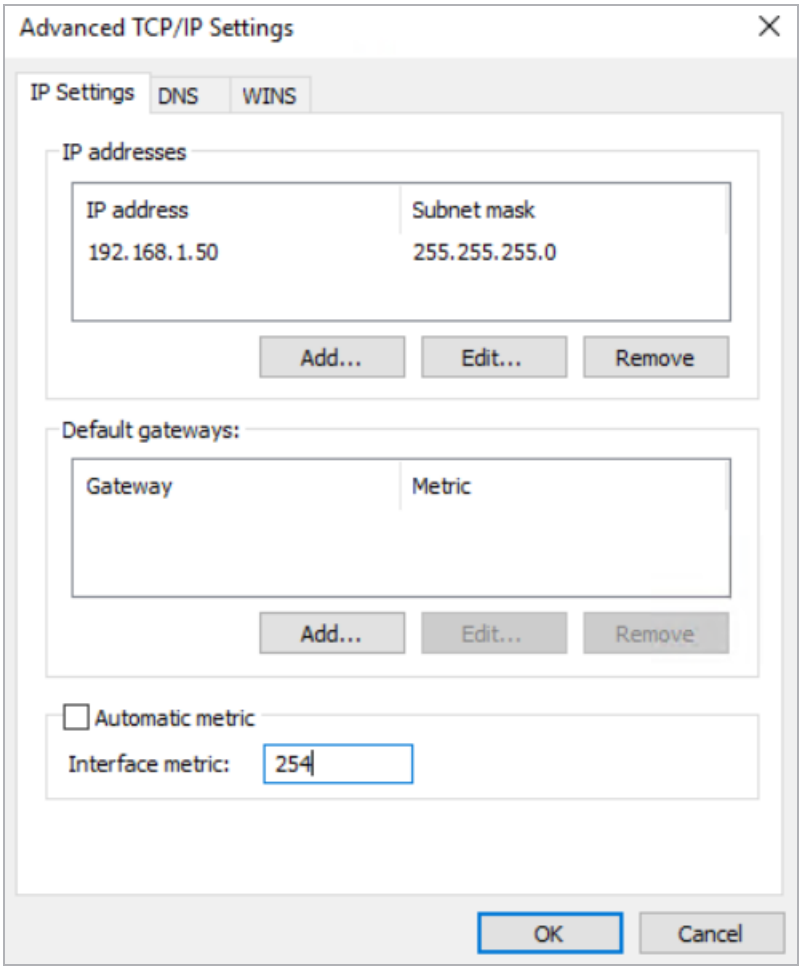
    a) Right-click the loopback interface and select **Properties**.



b) Select **Internet Protocol Version 4 (TCP/IP)** and click **Properties**.



c) The TCP/IP properties window will appear. This is where the Virtual Service **IP address** can be configured. Enter the Virtual Service **IP address** and click **Advanced...**.



d) In Advanced TCP/IP Settings, remove the check from the **Automatic metric** checkbox.

e) Enter **254** in the **Interface metric** text box.

> Setting the **Interface metric** 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.

f) Click **OK** to activate the change.

g) Click **OK** and **Close**.

Ensure the “network” adapter is the actual network adapter that will send and receive traffic.

20. On the Windows command line, run the following commands:

netsh interface ipv4 set interface "network" weakhostreceive=enabled

netsh interface ipv4 set interface "loopback" weakhostreceive=enabled

netsh interface ipv4 set interface "loopback" weakhostsend=enabled

3.1.1 Loopback Adapter Configuration for IPv6

On the Windows command line, run the following commands:

- netsh interface ipv6 set interface LAN weakhostreceive=enabled
- netsh interface *ipv6 *set interface Kemp-SMTP-LOOPBACK weakhostreceive=enabled
- netsh interface *ipv6 *set interface Kemp-SMTP-LOOPBACK weakhostsend=enabled

In the loopback adapter properties:

- **IPv6 address:** *<IPAddressOf TheVIP>*
- **Subnet prefix length:** 128

In Advanced Properties, set the **Interface metric** to **254**.

If you want IPv6 DSR, you must have the IPv6 address as the primary address on the interface. Additional addresses may be IPv6 or IPv4, as required.

References

Unless otherwise specified, the following documents can be found at http://kemptechnologies.com/documentation.

Web User Interface (WUI), Configuration Guide

Last Updated Date

This document was last updated on 25 April 2021.