



## **Appliance Quick Start Guide**

**v7.4**

*Copyright © 2002 – 2013 Loadbalancer.org, Inc.*





## Table of Contents

Loadbalancer.org Terminology.....	4
What is a Virtual IP Address?.....	4
What is a Floating IP Address?.....	4
What are Your Objectives?.....	5
What is the Difference Between a One-Arm and a Two-Arm Configuration?.....	6
What Load Balancing Methods are Supported?.....	6
Direct Routing (DR).....	8
Network Address Translation (NAT).....	9
Source Network Address Translation (SNAT) .....	10
High-Availability Configuration of two Loadbalancer.org Appliances.....	11
Clustered Pair Configuration Methods.....	11
Using the Wizard.....	11
Manual Configuration.....	11
Virtual Appliance.....	12
Supported Hypervisors.....	12
Host Requirements.....	12
Downloading the Appliance.....	12
VMware Hypervisors.....	13
Deploying the Virtual Appliance.....	13
VMware Tools.....	13
Microsoft Hyper-V.....	14
Deploying the Virtual Appliance.....	14
Windows 2008 R2.....	14
Windows 2012.....	16
Linux Integration Services.....	20
Physical Appliance (for reference).....	21
Initial Network Interface Configuration.....	22
Using the Network Setup Wizard.....	22
Using Linux Commands.....	23
Accessing the Web User Interface (WUI).....	24
Configuring the Loadbalancer.org Appliance Using the Web Based Wizard.....	24
Example Answers Using the Wizard for a Two-Arm NAT Configuration (Single Unit).....	25
Appliance Configuration Using the Web User Interface.....	26
Adding Virtual Servers.....	27
Adding Real Servers.....	28
Configuring the Real Servers.....	29
Configuring the Real Servers for Layer 4 NAT Mode.....	29
Configuring the Real Servers for Layer 4 DR Mode (Linux).....	29
Detecting the ARP Problem.....	29
Solving for Linux – Method 1 (using iptables).....	29
Solving for Linux – Method 2 (using arp_ignore sysctl values).....	30
Configuring the Real Servers for Layer 4 DR Mode (Windows).....	31
Configuring IIS to Respond to Both the RIP and VIP.....	31
Resolving ARP issues for Windows server 2000 (applies to DR mode only).....	32
Step 1 – Install the Microsoft loopback adapter.....	32
Step 2 – Configure the loopback adapter.....	33
Resolving ARP issues for Windows server 2003 (applies to DR mode only).....	35
Step 1 – Install the Microsoft loopback adapter.....	35
Step 2 – Configure the loopback adapter.....	36
Resolving ARP issues for Windows server 2008 (applies to DR mode only).....	38
Step 1 – Install the Microsoft loopback adapter.....	38
Step 2 – Configure the loopback adapter.....	38
Step 3 – Configure the strong / weak host behavior.....	40

Resolving ARP issues for Windows server 2012 (applies to DR mode only).....	41
Step 1 – Install the Microsoft loopback adapter.....	41
Step 2 – Configure the loopback adapter.....	41
Step 3 – Configure the strong / weak host behavior.....	43
Verifying netsh Settings for Windows 2008 & 2012.....	44
Configuring the Real Server for Layer 7 SNAT Mode.....	45
IPv6 Support.....	45
Testing the Load Balancer Configuration.....	46
Connection Error Diagnosis.....	46
Health Check Diagnosis.....	47
Appliance Log Files.....	47
Testing High-Availability for a Loadbalancer.org HA-Pair.....	48
Does Your Application Cluster Correctly Handle its Own State?.....	49
Replication Solutions for Shared Data.....	49
Solutions for Session Data.....	49
Persistence.....	49
What do You do if Your Application is Not Stateless?.....	50
Loadbalancer.org Persistence Methods.....	50
Loadbalancer.org Technical Support.....	50
Appendix A – Physical Appliance Front & Rear Panel Layouts (for reference).....	51

## Loadbalancer.org Terminology

<b><u>Acronym</u></b>	<b><u>Terminology</u></b>
<b>Load Balancer</b>	An IP based traffic manager for clusters
<b>VIP</b>	The Virtual IP address that a cluster is contactable on (Virtual Server)
<b>RIP</b>	The Real IP address of a back-end server in the cluster (Real Server)
<b>GW</b>	The Default Gateway for a back-end server in the cluster
<b>WUI</b>	Web User Interface
<b>Floating IP</b>	An IP address shared by the master & slave load balancer when in a high-availability configuration (shared IP)
<b>Layer 4</b>	Part of the seven layer OSI model, descriptive term for a network device that can route packets based on TCP/IP header information
<b>Layer 7</b>	Part of the seven layer OSI model, descriptive term for a network device that can read and write the entire TCP/IP header and payload information at the application layer
<b>DR</b>	Direct Routing is a standard load balancing technique that distributes packets by altering only the destination MAC address of the packet
<b>NAT</b>	Network Address Translation – Standard load balancing technique that changes the destination of packets to and from the VIP (external subnet to internal cluster subnet)
<b>SNAT</b> (HAProxy)	Source Network Address Translation – Load balancer acts as a proxy for all incoming & outgoing traffic
<b>SSL Termination</b> (Pound)	The SSL certificate is installed on the load balancer in order to decrypt HTTPS traffic on behalf of the cluster
<b>MASQUERADE</b>	Descriptive term for standard firewall technique where internal servers are represented as an external public IP address. Sometimes referred to as a combination of SNAT & DNAT rules
<b>One Arm</b>	The load balancer has one physical network card connected to one subnet
<b>Two Arm</b>	The load balancer has two network interfaces connected to two subnets – this may be achieved by using two physical network cards or by assigning two addresses to one physical network card
<b>Eth0</b>	Usually the internal interface also known as Gb0
<b>Eth1</b>	Usually the external interface also known as Gb1

### *What is a Virtual IP Address?*

Most load balancer vendors use the term virtual IP address (VIP) to describe the address that the cluster is accessed from. It is important to understand that the virtual IP (VIP) refers both to the physical IP address and also to the logical load balancer configuration. Likewise the real IP (RIP) address refers both to the real servers physical IP address and its representation in the logical load balancer configuration.

### *What is a Floating IP Address?*

The floating IP address is shared by the master and slave load balancer when in a high-availability configuration. The network knows that the master controls the floating IP address and all traffic will be sent to this address. The logical VIP matches this address and is used to load balance the traffic to the application cluster. If the master has a hardware failure then the slave will take over the floating IP address and seamlessly handle the load balancing for the cluster. In scenarios that only have a master load balancer there can still be a floating IP address, but in this case it would remain active on the master unit only.

## What are Your Objectives?

It's important to have a clear focus on your objectives and the required outcome for the successful implementation of your load balancing solution. If the objective is clear and measurable, you know when you have achieved the goal.

Load balancers have a number of flexible features and benefits for your technical infrastructure and applications. The first question to ask is:

*Are you looking for increased performance, reliability, ease of maintenance or all three?*

<b>Performance</b>	A load balancer can increase performance by allowing you to utilize several commodity servers to handle the workload of one application
<b>Reliability</b>	Running an application on one server gives you a single point of failure. Utilizing a load balancer moves the point of failure to the load balancer. At Loadbalancer.org we advise that you only deploy load balancers as clustered pairs to remove this single point of failure
<b>Maintenance</b>	Using the appliance, you can easily bring servers on and off line to perform maintenance tasks, without disrupting your users



In order to achieve all three objectives of performance, reliability & maintenance in a web based application, your application must handle persistence correctly (see page 49 for more details).

## What is the Difference Between a One-Arm and a Two-Arm Configuration?

The number of 'arms' is normally a descriptive term for how many physical connections (Ethernet interfaces) are used to connect a device to a network. It's very common for a load balancer that uses a routing method (NAT) to have a two-arm configuration. Proxy based load balancers (SNAT) commonly use a one-arm configuration.

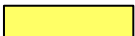


<b>One-Arm</b>	The load balancer has <b>one</b> physical network card connected to <b>one</b> subnet
<b>Two-Arm</b>	The load balancer has <b>two</b> network interfaces connected to <b>two</b> subnets – this can be achieved by using two physical network cards or by assigning two addresses to one physical network card

## What Load Balancing Methods are Supported?

The Loadbalancer.org appliance is one of the most flexible load balancers on the market. The design of the appliance allows different load balancing modules to utilize the core high availability framework of the appliance. Multiple load balancing methods can be used at the same time or in combination with each other.

Layer 4	DR (Direct Routing)	Ultra-fast local server based load balancing <b><i>Requires handling the ARP issue on the real servers</i></b>	1 ARM
Layer 4	NAT (Network Address Translation)	Fast Layer 4 load balancing, the appliance becomes the default gateway for the real servers	2 ARM
Layer 4	TUN	Similar to DR but works across IP encapsulated tunnels	1 ARM
Layer 7	SSL Termination ( <i>Pound</i> )	Usually required in order to process cookie persistence in HTTPS streams on the load balancer <b><i>Processor intensive</i></b>	1 or 2 ARM
Layer 7	SNAT (Source Network Address Translation: HAProxy)	Layer 7 allows great flexibility including full SNAT and WAN load balancing, cookie insertion and URL switching <b><i>Not as fast as Layer 4</i></b>	1 or 2 ARM

### Key:

-  Recommended for high performance fully transparent and scalable solutions
-  Recommended if HTTP cookie persistence is required, also used for numerous Microsoft applications such as Terminal Services (RDP cookie persistence) and Exchange, that require SNAT mode
-  Only required for Direct Routing implementation across routed networks (rarely used)

### Loadbalancer.org Recommendation:

Where feasible, one-arm direct routing (DR) mode is our recommended method because it's a very high performance solution with little change to your existing infrastructure.



Sometimes it's not possible to use DR mode. The two most common reasons being: if the application cannot bind to the RIP & VIP at the same time; or if the host operating system cannot be modified to handle the ARP problem (see page 29-44 for more details).

A second option is Network Address Translation (NAT) mode. This is a fairly high performance solution but it requires the implementation of a two-arm infrastructure with an internal and external subnet to carry out the translation (the same way a firewall works). Network engineers with experience of hardware load balancers will have often used this method.

The third option is Source Network Address Translation (SNAT) mode using HAProxy. If your application requires that the load balancer handles cookie insertion, RDP cookies, Session Broker integration or SSL termination then this option is appropriate. This can be deployed in one-arm or two-arm mode and does not require any changes to the application servers. HAProxy is a high-performance solution that operates as a full proxy, but due to this it cannot perform as fast as the layer 4 solutions.



If your application doesn't maintain its own state information then you may need to use cookie insertion to maintain server persistence (affinity).

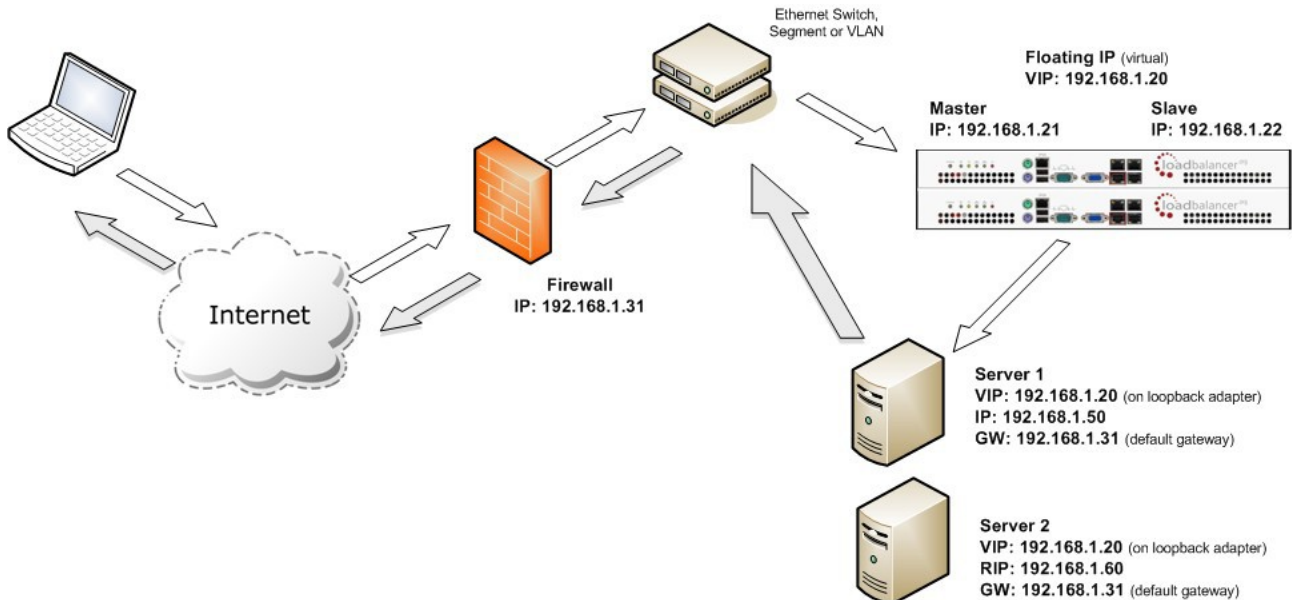
The following sections describe these configurations in more details.



**IMPORTANT NOTE** – If you are using Microsoft Windows real servers (i.e. back-end servers) make sure that Windows NLB (Network Load Balancing) is completely disabled to ensure that this does not interfere with the operation of the load balancer.

## Direct Routing (DR)

The one-arm direct routing (DR) mode is the recommended mode because it's a very high performance solution with little change to your existing infrastructure. *NB. Foundry networks call this Direct Server Return and F5 call it N-Path.*

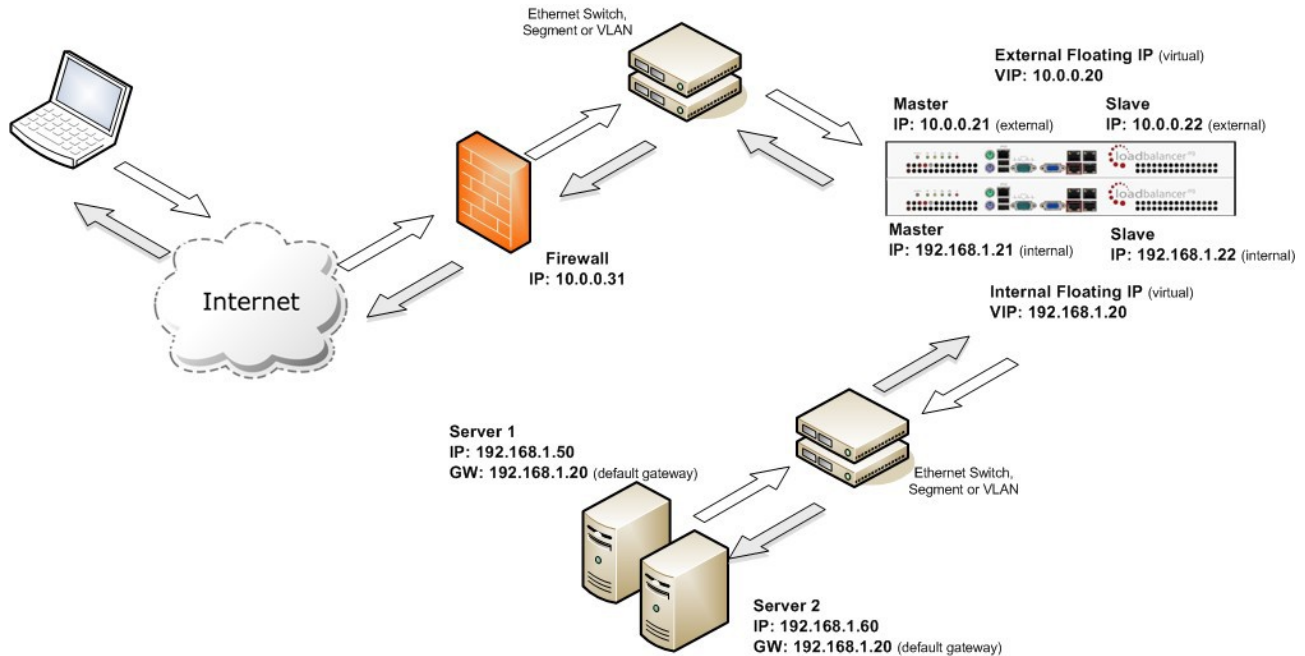


- Direct routing works by changing the destination MAC address of the incoming packet on the fly which is very fast
- However, this means that when the packet reaches the real server it expects it to own the VIP. This means you need to make sure the real server responds to both its own IP and the VIP, but does not respond to ARP requests for the VIP. Please refer to page 29-44 for more details on resolving the ARP problem
- On average, DR mode is 8 times quicker than NAT for HTTP, 50 times quicker for Terminal Services and much, much faster for streaming media or FTP
- Load balanced services can be configured directly on the interface (normally eth0) with no additional IP address. However, when using a clustered pair, all load balanced virtual services **must** be configured on a floating IP to enable failover & failback between master & slave
- The virtual server and real servers must be in the same switch fabric / logical network. They can be on different subnets, provided there are no router hops between them. If multiple subnets are used, an IP address in each subnet must be defined on the load balancer
- Port translation is not possible in DR mode i.e. having a different RIP port than the VIP port
- DR mode is transparent, i.e. the real server will see the source IP address of the client
- Administration of the load balancer is via any active IP address (on port 9080)



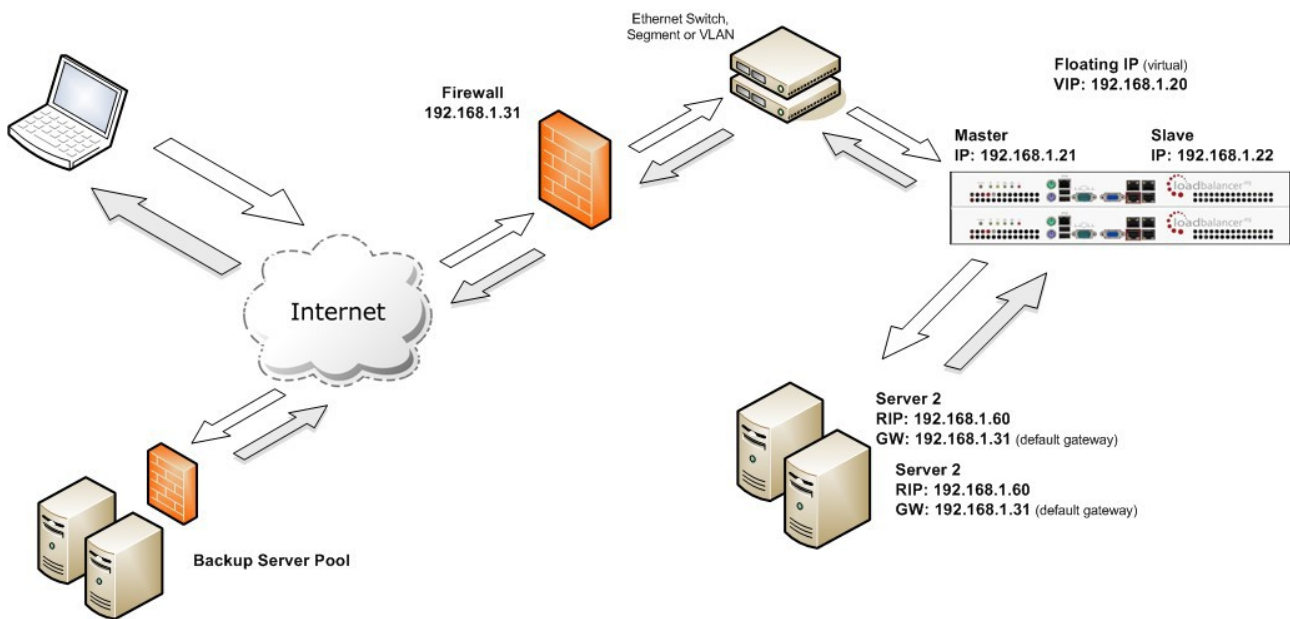
## Network Address Translation (NAT)

Sometimes it's not possible to use DR mode. The two most common reasons being: if the application cannot bind to RIP & VIP at the same time; or if the host operating system cannot be modified to handle the ARP problem. The second choice is Network Address Translation (NAT) mode. This is also a fairly high performance solution but it requires the implementation of a two arm infrastructure with an internal and external subnet to carry out the translation (the same way a firewall works).



- In two-arm NAT mode the load balancer translates all requests from the external virtual server to the internal real servers
- It's a good idea to use *eth1* as your external network and *eth0* as internal, otherwise you will need to change the *autonat* setting in *Edit Configuration > Layer 4 – Advanced Configuration*
- The real servers must have their default gateway configured to point at the load balancer. When master & slave units are used, a floating IP must be used to enable failover
- Real servers are automatically given access to the Internet through the load balancer (via autonat)
- Load balanced services can be configured directly on the interface (normally *eth0*) with no additional IP address. However, when using a clustered pair all load balanced virtual services must be configured on a floating IP to enable failover & failback between master & slave
- Normally the virtual server and real servers should be located on different subnets within the same logical network (i.e. no router hops) and the load balancer should have an IP address in each subnet. *NB. It is possible to have real and virtual servers in the same subnet – please refer to the Advanced NAT topic in Section F of the administration manual. NB. It is possible to have the real servers located on routed subnets, but this would require a customized routing configuration on the real servers and is not recommended*
- If you want real servers to be accessible on their own IP address for non-load balanced services, e.g. SMTP or RDP, you will need to setup individual SNAT and DNAT firewall script rules for each real server. Please refer to the Advanced NAT Considerations section in the administration manual for more details
- You can also configure the load balancers in one-arm NAT mode, but in order to make the servers accessible from the local network you need to change the routing configuration on the real servers. Please refer to the Advanced NAT Considerations section in the administration manual for more details.
- NAT mode is transparent, i.e. the real server will see the source IP address of the client
- Administration of the load balancer is via any active IP address (on port 9080)

## Source Network Address Translation (SNAT)



If your application requires that the load balancer handles cookie insertion then you need to use the SNAT configuration. This mode is also used with numerous Microsoft applications such as Terminal Services (using RDP cookies or Integrated with Connection Broker) and Exchange that require SNAT mode.

This mode also has the advantage of a one arm configuration and does not require any changes to the application servers. However, as the load balancer is acting as a full proxy it doesn't have the same raw throughput as the routing based methods.

The network diagram for the Layer 7 HAProxy SNAT mode is very similar to the Direct Routing example except that no re-configuration of the real servers is required. The load balancer proxies the application traffic to the servers so that the source of all traffic becomes the load balancer.

- As with other modes a single unit does not require a Floating IP, although it is recommended to make adding a slave unit easier
- SNAT is a full proxy and therefore load balanced real servers do not need to be changed in any way
- Because SNAT is a full proxy any server in the cluster can be on any accessible subnet including across the Internet or WAN
- SNAT is not transparent by default, i.e. the real servers will not see the source IP address of the client, they will see the load balancers IP address. If required, this can be solved by either enabling TPROXY on the loadbalancer, or leveraging the X-forwarded-For header. See the administration manual for more details.



For detailed configuration examples, please refer to section D in the administration manual.

## High-Availability Configuration of two Loadbalancer.org Appliances

Loadbalancer.org's recommended configuration is to use a clustered pair of load balancers to provide a highly available and resilient load balancing solution. In this configuration, the pair communicates via a heartbeat to determine if the master node is active. Should the master node suffer a failure, the slave will immediately take over any resources hosted on the shared floating IP addresses.



Using a single load balancer introduces a single point of failure for your infrastructure so it is strongly recommended to use two appliances in a clustered pair.

### *Clustered Pair Configuration Methods*

There are two ways to configure a clustered pair; either by using the wizard or configuring the units manually.

#### Using the Wizard

If the wizard is used, the slave is configured first and then the master. This ensures that both units can first communicate via the selected link (via a serial cable – the default, or over the network), and also that settings that are configured on the master are correctly replicated to the slave.



For more details on using the wizard and an example, please refer to pages 24-25.

#### Manual Configuration

If the master is configured first without using the wizard and the slave is added later, the following points should be considered:

- The hostname of the unit to be used as the slave must be set to 'lbslave' using *Edit Configuration > Hostname & DNS* in the WUI
- The IP address of the slave must be defined on the master using *Edit Configuration > Hostname & DNS* in the WUI
- The **Force full slave sync** option in *Edit Configuration > Hostname & DNS* should be checked prior to clicking **Update** – this will ensure that all configured services are correctly replicated over to the slave unit
- Once the IP address is set and synchronization has occurred, it's important to restart heartbeat on both units to ensure heartbeat starts cleanly. This can be done using *Maintenance > Restart Services* in the WUI



For more details please refer to the configuration examples in section D of the administration manual.

## Virtual Appliance

The following sections detail the various VA's available, where they can be downloaded and how they are deployed.

## Supported Hypervisors

Currently, the Virtual appliance is available for the following hypervisors:

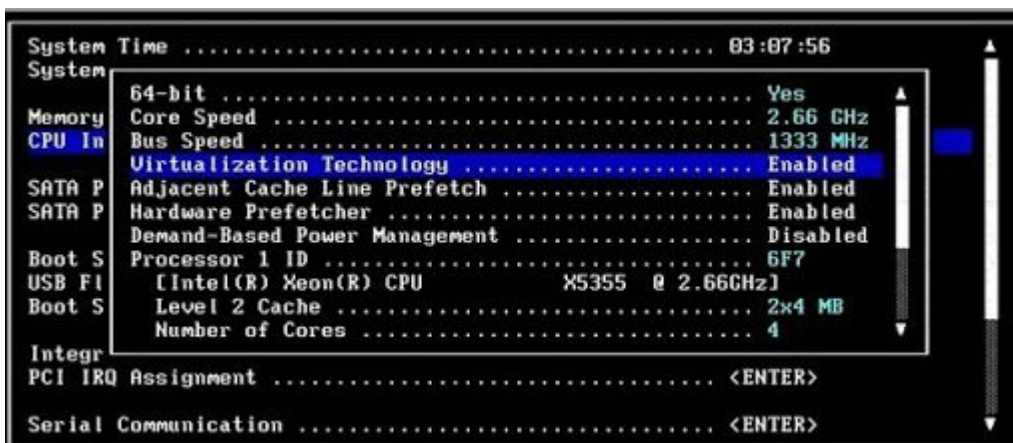
- VMware (Player/Workstation/Server & vSphere ESX/ESXi)
- Microsoft Hyper-V

## Host Requirements

To run the Loadbalancer.org Enterprise VA (whatever Hypervisor is being used) the following basic server specifications must be met:

- A compatible 64bit CPU
- Virtual Technology hardware support – either Intel-VT or AMD-V compliant CPU's

For an Intel based server, VT must be enabled in the BIOS as shown in the example below:



If your server is unable to support 64bit guests, an error message will be displayed when attempting to start the VA.

## Downloading the Appliance

All downloads are accessible from the following location:

<http://www.loadbalancer.org/downloads.php>

*N.B. To access the downloads you'll need to enter your name & email address, select the Hypervisor type (VMware or Hyper-V) and specify the application that you'll be load balancing. Once the required details are entered, click **Submit**, we'll then send you an email that includes the various links.*

*Any information provided is 100% confidential. We may follow up with an email to see how you are getting on with the trial and offer assistance but under no circumstances will Loadbalancer.org send you other promotional material or share your information with a third party.*

## VMware Hypervisors

Three downloads are available as listed below:

### 1) VMware Player, Server & Workstation

- Download **LBVMv7.zip** (virtualHW.version = 4)
- For VMware server v2.x you can highlight the VA after import and select Upgrade to Hardware v7, for VMware Player, Workstation & Server v1.x no further steps are required

### 2) vSphere 4.x & ESX 4.x / ESXi 4.x and vSphere 5.x & ESXi 5.x

- Download **LBVMESXv7.zip** (ovf v1.0, hardware v7)

### 3) Virtual Infrastructure Client 2.5.x & ESX 3.x / ESXi 3.x

In this case you have two choices:

- Download **LBVMESXv7\_ovf0.9.zip** (ovf v0.9, hardware v4)  
or
- Download **LBVMv7.zip** and use the converter for your environment to convert to a compatible VA



NOTE: Due to Vmxnet3 driver compatibility limitations with the various versions of ESX & ESXi only the LBVMESXv7.zip download uses the Vmxnet3 network drivers. The other downloads use E1000 drivers.

### Deploying the Virtual Appliance

1. Download & extract the appropriate file (see previous section)
2. deploy the VA -
  - For VMware Server use: **Virtual Machine > Add VM to Inventory**
  - For vSphere use: **File > Deploy ovf Template**
  - For Virtual Infrastructure use: **File > Virtual Appliance > Import**
3. Start the Virtual Appliance, allow a minute for booting
4. Now refer to page 22 onwards for details on setting up the network

### VMware Tools

The latest versions of all drivers that are installed when VMware tools are deployed are included by default in the Appliances kernel. Therefore, VMware tools do not need to be installed.

These drivers are kept up to date through periodic updates that are made available for the appliance via Loadbalancer.org's online software update feature.

## Microsoft Hyper-V

One download is available as listed below, this can be used for all versions of Hyper-V.

### 1) Windows 2008 R2 & Windows 2012

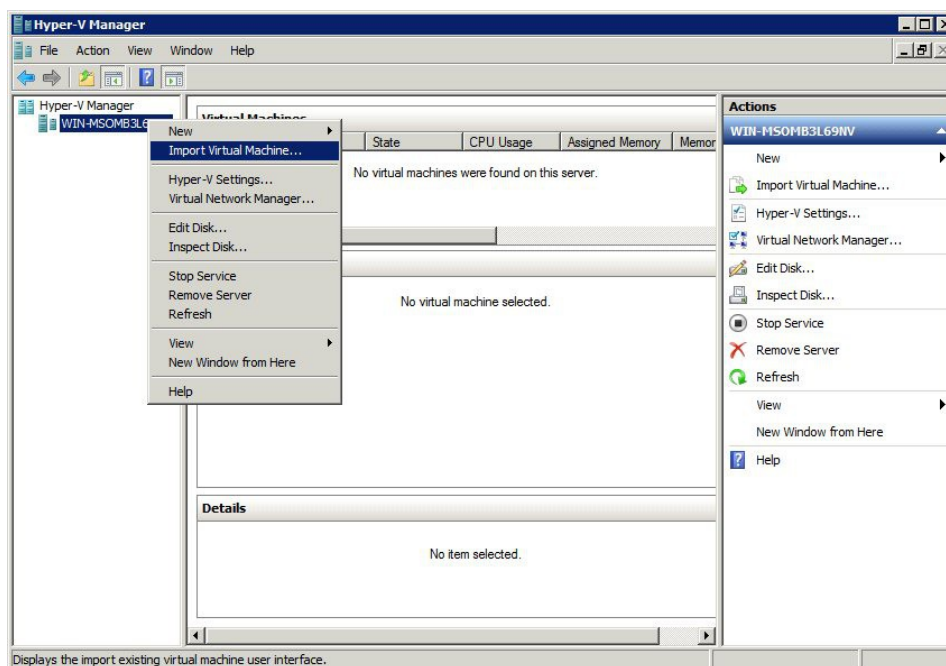
- Download **LBVMHYPER-Vv7.zip**

### Deploying the Virtual Appliance

The following two sections explain how the appliance is deployed under Windows 2008 and Windows 2012.

#### Windows 2008 R2

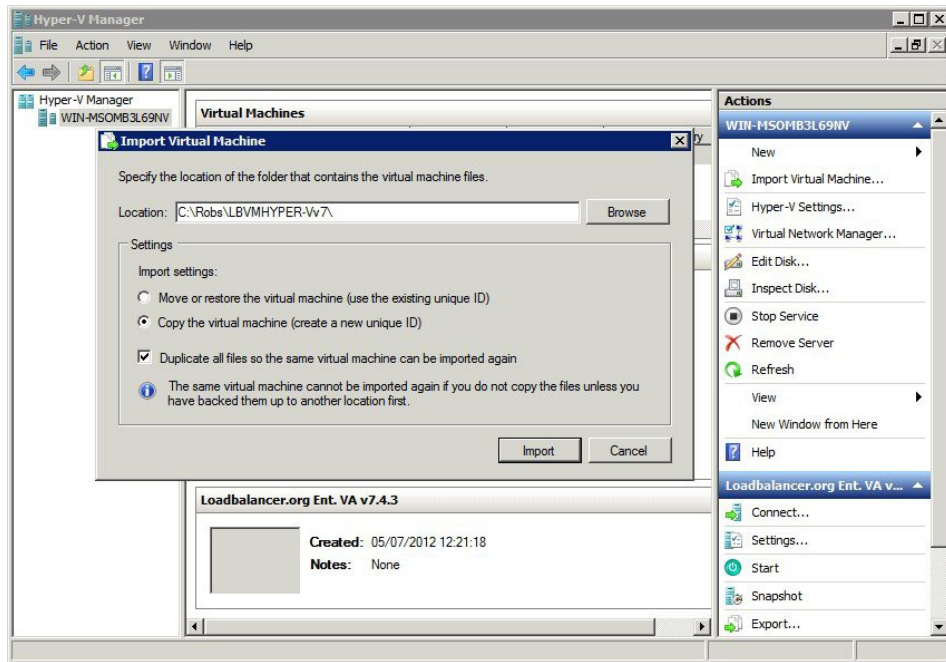
1. Download & extract the compressed archive
2. Start Hyper-V Manager, then using the right-click menu or the Actions pane select **Import Virtual Machine** as shown below:



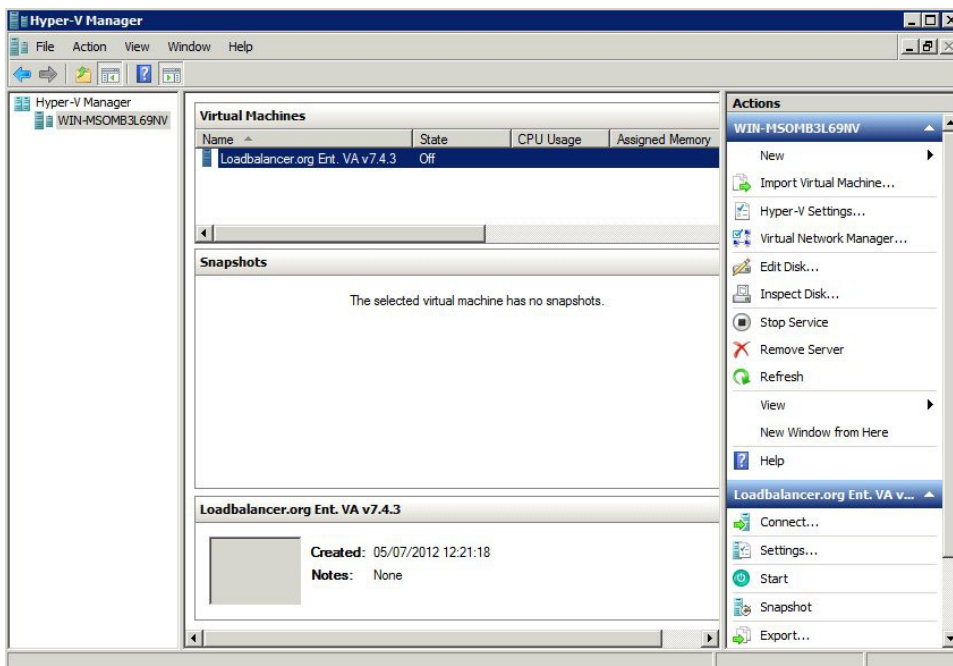
3. Click **Next**



- Browse to the location of the extracted download and select the folder LBVMHYPER-Vv7 as shown below:



- Select the option "Copy the virtual machine (create a new unique ID)" and also select the "Duplicate all files so the same virtual machine can be imported again" check-box, click **Import**
- The import will now start, once complete the new appliance will appear in the Virtual Machine list as shown below:



- The appliance has 4 NIC cards, to connect these right-click the appliance and select **Settings** then for each Network Adapter select the required network
- Right-click and select **Start** to power up the appliance, allow a minute to boot
- Now refer to page 22 onwards for details on setting up the network

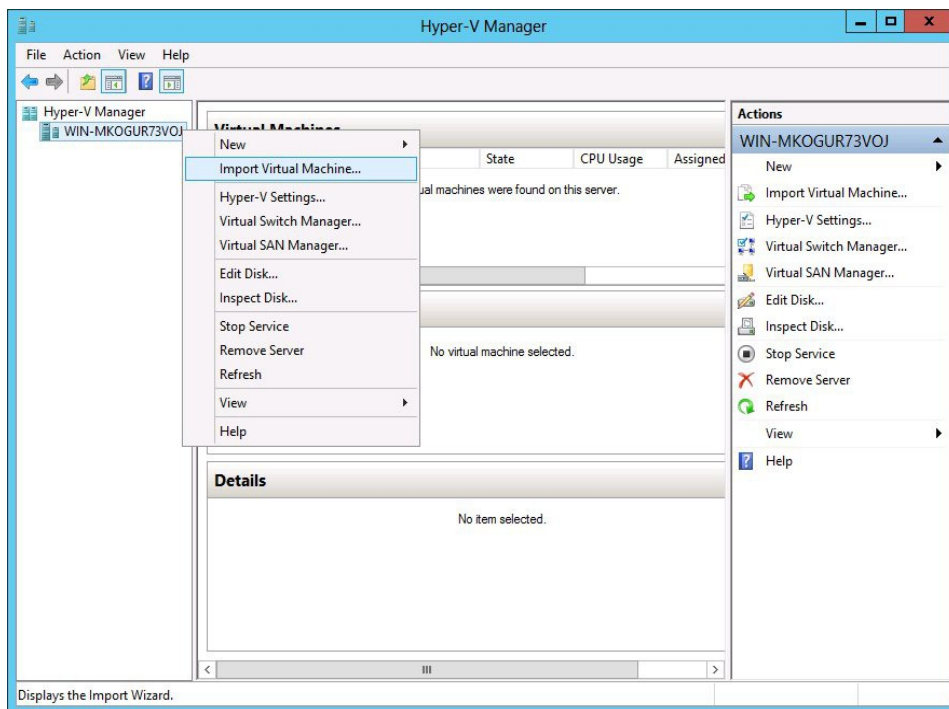
If you're deploying a clustered pair, you'll first need to do one of the following steps before importing the second virtual machine. If this is not done, the second virtual machine cannot be deployed because the disk from the first import already exists, and there will therefore be a conflict:

- Shutdown the first VM and modify the name of the disk  
*or*
- Change the default file location using the Hyper-V *Settings* option in the Actions pane

Once one of the above steps is done, repeat steps 2-9 above to create the second virtual machine.

## Windows 2012

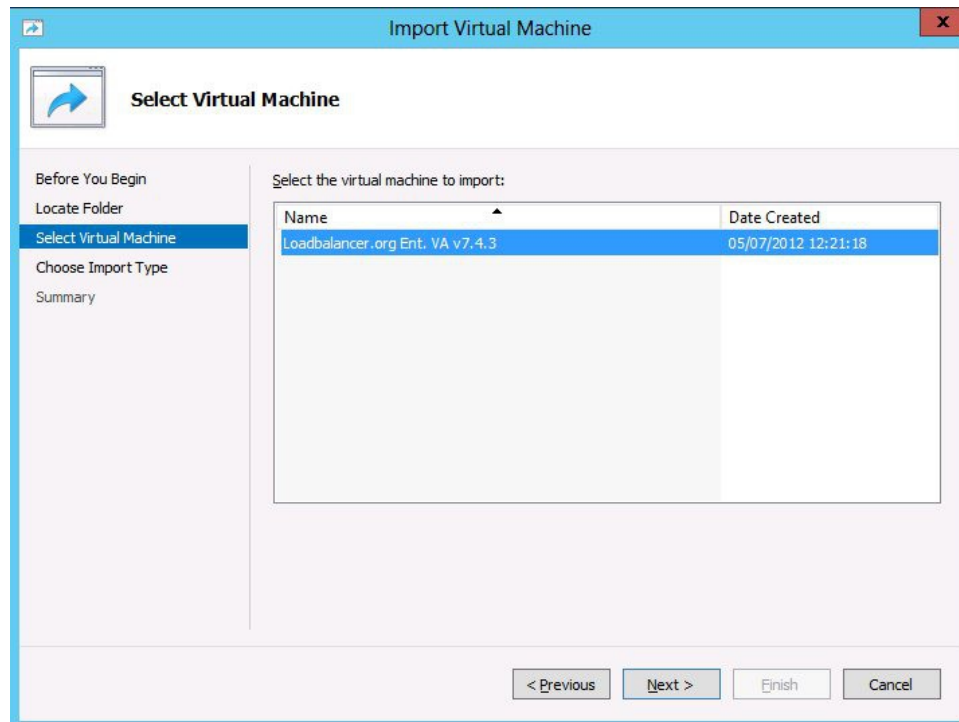
1. Download & extract the compressed archive
2. Start Hyper-V Manager, then using the right-click menu or the Actions pane select **Import Virtual Machine** as shown below:



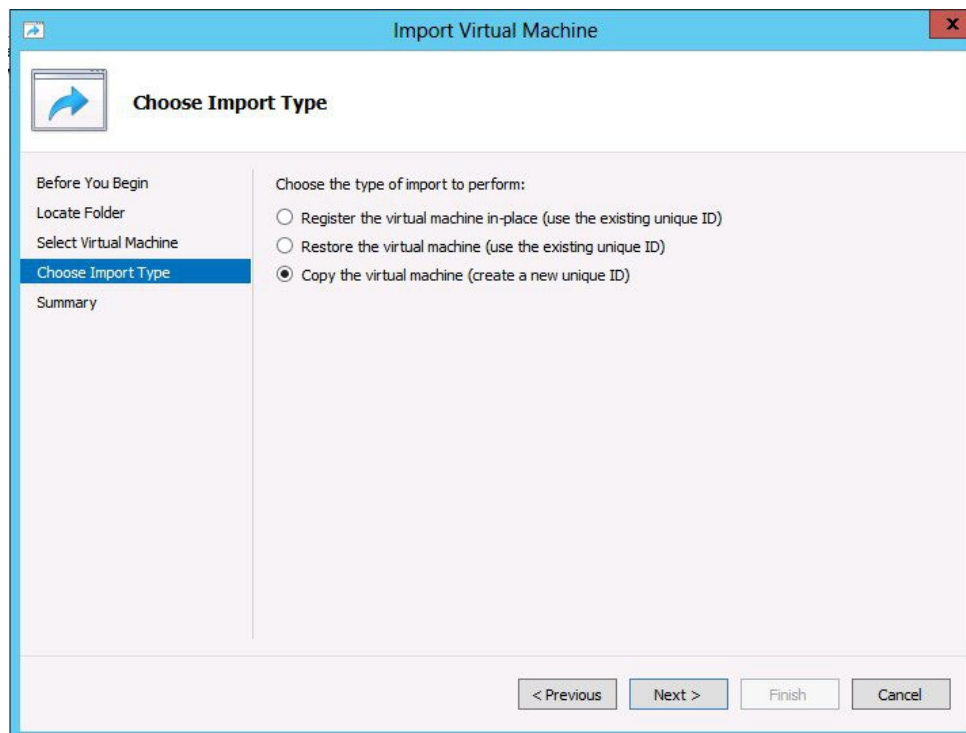
3. Click **Next**
4. Now browse to the location of the extracted download and select the folder LBVMHYPER-Vv7



5. Click **Next**, the following screen will be displayed:



6. Click **Next**, the following screen will be displayed:



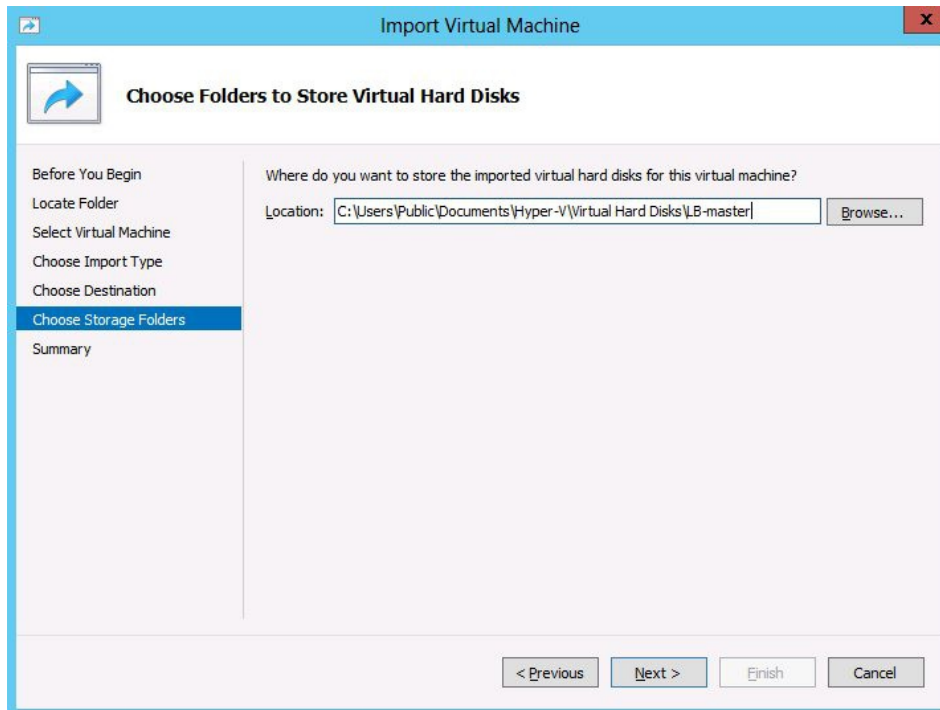
7. Make sure that 'Copy the virtual machine (create a new unique ID)' is selected and click **Next**, the following screen will be displayed:

The screenshot shows the 'Import Virtual Machine' wizard window. The title bar is 'Import Virtual Machine'. The main window has a blue header with a blue arrow icon and the text 'Choose Folders for Virtual Machine Files'. On the left, there is a vertical list of steps: 'Before You Begin', 'Locate Folder', 'Select Virtual Machine', 'Choose Import Type', 'Choose Destination' (highlighted with a blue bar), 'Choose Storage Folders', and 'Summary'. The main area contains the following text: 'You can specify new or existing folders to store the virtual machine files. Otherwise, the wizard imports the files to default Hyper-V folders on this computer, or to folders specified in the virtual machine configuration.' Below this text is a checkbox labeled 'Store the virtual machine in a different location' which is currently unchecked. There are three text input fields with 'Browse...' buttons: 'Virtual machine configuration folder:' (C:\ProgramData\Microsoft\Windows\Hyper-V\), 'Snapshot store:' (C:\ProgramData\Microsoft\Windows\Hyper-V\), and 'Smart Paging folder:' (C:\ProgramData\Microsoft\Windows\Hyper-V\). At the bottom, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

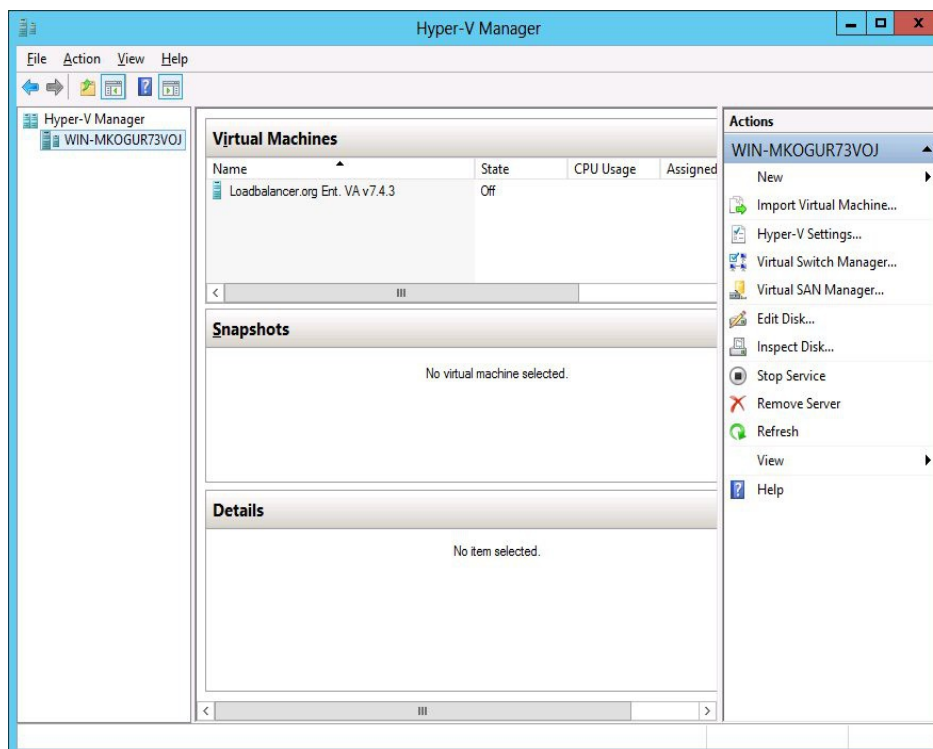
8. Tick the check-box 'Store the Virtual Machine in different location', then define a suitable location for the virtual machines files, e.g. :

This screenshot is similar to the previous one, but the checkbox 'Store the virtual machine in a different location' is now checked. The text input fields for the folders are also updated to a custom path: 'C:\ProgramData\Microsoft\Windows\Hyper-V\LB-master'. The 'Virtual machine configuration folder:' field has a 'Browse...' button. The 'Snapshot store:' field has a 'Browse...' button. The 'Smart Paging folder:' field has a 'Browse...' button. The 'Next >' button is now enabled and highlighted in blue.

9. Click **Next**, then define a location for the hard disk files, e.g. :



10. click **Next**, then click **Finish** to complete the import process. Once complete, the load balancer will appear in the Virtual Machines list as shown below:



11. The appliance has 4 NIC cards, to connect these right-click the appliance and select Settings then for each Network Adapter select the required network
12. Highlight the new load balancer and start it either by using the right-click menu or the Actions pane

13. Now refer to page 22 onwards for details on setting up the network

If you're deploying a clustered pair, repeat steps 2-13 for the slave unit, making sure that a different folder location is selected in steps 8 & 9.

#### Linux Integration Services

The latest versions of all required drivers that are installed when Linux Integration Services are deployed are included by default in the Appliances kernel. Therefore, the installation of Linux Integration Services on the VA is not required.

These drivers are kept up to date through periodic updates that are made available for the appliance via Loadbalancer.org's online software update feature.

## Physical Appliance (for reference)

- Remove all packaging
- Rack mount the appliance if required
- The power supply is an auto sensing unit (100v to 240v)
- Connect the power lead from the power socket to the mains or UPS
- Connect your network cable from your switch or hub to the internal network port (*eth0*)
- If using a two-armed configuration connect a second network cable to the external port (*eth1*)

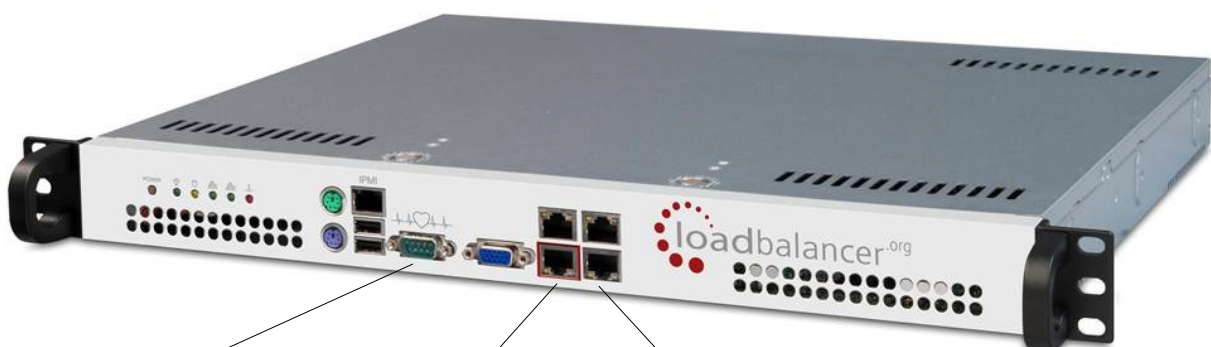


If two load balancers (recommended) are being used, connect a null modem cable (one cable is supplied with each appliance) between the two serial ports, then configure the slave first.

- Attach a monitor to the VGA port and keyboard to the USB or PS/2 port
- Check mains power is on and press the power switch to start the appliance (the fans should start & front panel LEDs should light)
- Allow a minute for booting

The next few pages of this document cover the following steps:

- Initial Network Interface Configuration
- Accessing the WUI
- Configuring the appliance using the web based wizard
- Appliance configuration using the WUI
- Testing the load balancer configuration



Serial connection  
for the fail-over  
(heartbeat) cable

eth0 is usually the  
internal network

eth1 is usually the  
external network

## Initial Network Interface Configuration

By default the load balancer is pre-configured with the following IP address & mask:

**192.168.2.21 / 255.255.255.0**

This default address can be changed in two ways:

- Using the built-in Network Setup Wizard
- Using traditional Linux commands

### *Using the Network Setup Wizard*

To run the wizard, login to the console of the appliance as the 'setup' user. This is explained in the initial console start-up message as shown below:

```
Welcome to the Loadbalancer.org appliance.

To perform initial network configuration, log in to the console as
Username: setup
Password: setup

To access the web interface and wizard, point your browser at
http://192.168.2.21:9080/
or
https://192.168.2.21:9443/

lbmaster login: _
```

- login to the console:  
**Username:** setup  
**Password:** setup
- Once logged in, enter the IP address, mask and default gateway at the prompts as shown below:

```
Loadbalancer.org basic network set up

Static IP address (eg. 192.168.0.26)      : 192.168.70.175
Interface netmask (eg. 24)                : 18
Default gateway (eg. 192.168.0.1)        : 192.168.64.1
```

After the required settings have been entered, a summary will be presented along with details of how to access the WUI as shown below:

#### Summary of settings

Static IP address: 192.168.70.175/18

Default gateway: 192.168.64.1

You may now connect the eth0 network interface to your switch, and continue configuration through the web interface on:

`http://192.168.70.175:9080/lbadmin/`

Press any key... \_

The IP address is now configured for interface eth0.

IP addresses for the other interfaces can now be configured via the WUI or using the Linux commands covered in the next section.

### *Using Linux Commands*

To set the IP address, login to the console or an SSH session as root:

**Username:** root

**Password:** loadbalancer

Now set the IP address using the following command:

```
ip addr add <IP address>/<mask> dev eth0
```

e.g.

```
ip addr add 192.168.1.100/24 dev eth0
```

***NB. Setting the IP address in this way is temporary, the IP address MUST be set via the WUI to make this permanent***

## Accessing the Web User Interface (WUI)

- Using a web browser, access the WUI using the following URL:

***http://192.168.2.21:9080/lbadmin/***

*(replace 192.168.2.21 with your IP address if its been changed)*

*NB. If you prefer you can use the HTTPS administration address:*

***https://192.168.2.21:9443/lbadmin/***

*(replace 192.168.2.21 with your IP address if its been changed)*

- Login to the WUI:

***Username:*** loadbalancer

***Password:*** loadbalancer

- Once logged in, you'll be asked if you want to run the web based setup wizard. The wizard asks a series of questions in order to setup the appliance with an initial basic configuration. If you prefer to configure the appliance manually, simple select 'no' to the question.

### **EDIT CONFIGURATION > SETUP WIZARD**

The Loadbalancer.org Setup Wizard has not been run yet. You can run it now or anytime later with Edit Configuration > Setup Wizard

Do you want to run it now?

☐ yes ☐ no

## Configuring the Loadbalancer.org Appliance Using the Web Based Wizard

The wizard can be used to setup a single layer 4 DR mode or NAT mode Virtual Server with a single real server. The wizard can be used for both single unit deployments and clustered pair deployments.

### ***Outline steps – Single unit deployments:***

- Set the IP address using the methods described earlier
- Now start the WUI and run the wizard (*Edit Configuration > Setup Wizard*)

### ***Outline steps – Clustered pair deployments:***

- Set the IP address on both units as described earlier
- Connect the serial cable (*NB. it's also possible to use the network for heartbeat comms if preferred*)
- Start the WUI on the slave unit and run the wizard (*Edit Configuration > Setup Wizard*)
- Now run the wizard on the master unit to complete the process



## Example Answers Using the Wizard for a Two-Arm NAT Configuration (Single Unit)

The following example covers setting up a layer 4 NAT mode virtual server with one real server. Additional Virtual Servers (VIPs) and Real Servers (RIPs) can then be added using the WUI.

### EDIT CONFIGURATION > SETUP WIZARD

Is this unit part of an HA-pair?

☐ yes ☒ no

Will the load balancer form part of a one armed set-up (i.e. same subnet as servers)?

☐ yes ☒ no

Then the load balancer will form part of a two-armed set-up. (See Quickstart guide for further explanation.)

We will now configure the load balancer's network interfaces:

Enter the IP address for the INTERNAL interface eth0 (CIDR format):

192.168.2.120/24

Enter the IP address for the EXTERNAL interface eth1 (CIDR format):

10.0.0.120/16

Now we will configure the DNS and gateway settings for the load balancer.

Enter the IP address of the default gateway IP v4:

10.0.0.1

Enter the IP address of the default gateway IP v6:

Enter the IP address of the nameserver:

10.0.0.1

Enter the IP address of the second nameserver:

Now we will configure the first Virtual Service.

Enter the port number for the Virtual Service:

80

Enter the IP address of the first Real Server (backend):

192.168.2.60

Please check that all your settings are correct!

Submit

Check that your settings are correct and click **Submit**. Once the wizard is complete the load balancer is configured and ready to use.

For NAT mode – as used in this example, you must also configure the real server to ensure that it uses the internal IP address of the load balancer as its default gateway. Once this is done you can test the virtual server from the external network. By default, the wizard uses the IP address of the external interface for the first virtual server, 10.0.0.120 in this example.

You can now use the *Edit Configuration* menu in the WUI to easily add more virtual or real servers to your configuration.

To restore manufacturer's settings – at the console use the command **lbrestore** or in the WUI goto *Maintenance > Backup & Restore > Restore Manufacturer's Defaults*. This will reset the address to 192.168.2.21.

25

## Appliance Configuration Using the Web User Interface



When using a Clustered Pair, all configuration must be done via the master unit, the slave unit will then be synchronized automatically.

If you have already used the web based wizard, then you will already be using the WUI. From here all administration tasks can be carried out. If not, access the WUI as follows:

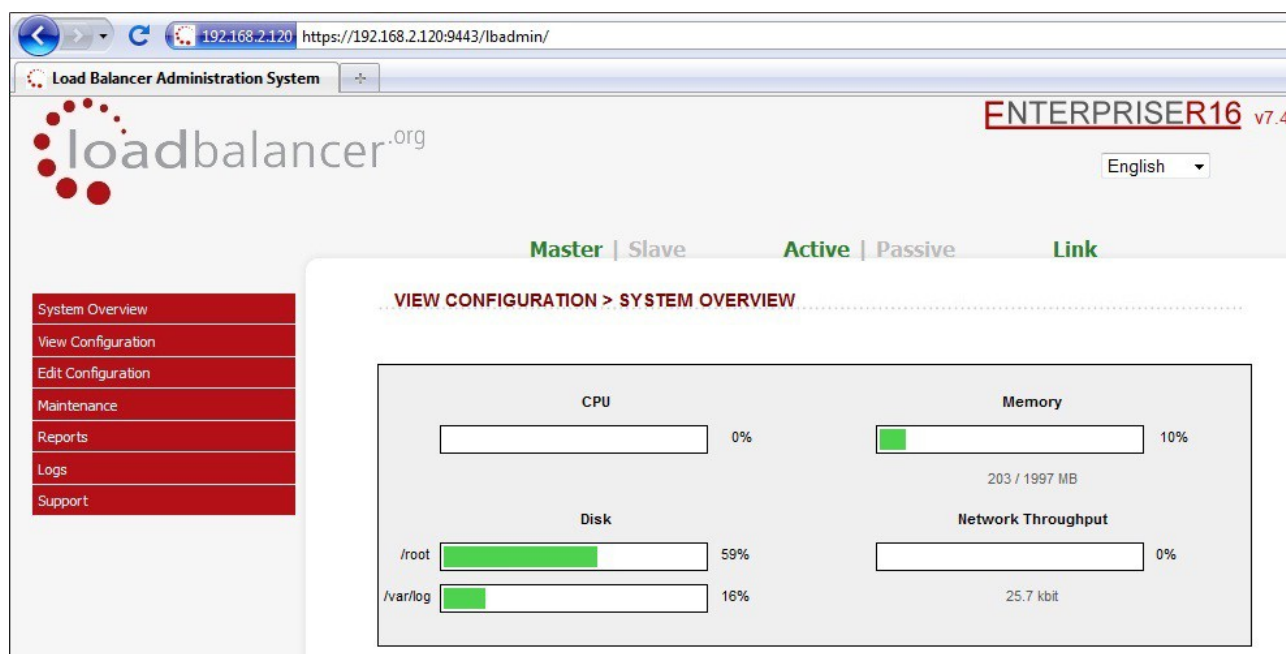
With a web browser access the web interface: ***http://192.168.2.21:9080/lbadmin/***

*(replace 192.168.2.21 with the correct IP address)*

log in to the WUI: ***Username:*** loadbalancer

***Password:*** loadbalancer

*NB. If you prefer you can use the HTTPS administration address: ***https://192.168.2.21:9443/lbadmin/****



All administration tasks can be carried out through the web interface. If root access to the appliance is required for any reason via the console or a ssh session, the following default credentials should be used:

root credentials: ***Username:*** root  
***Password:*** loadbalancer

## Adding Virtual Servers

If used, the wizard sets up a single Virtual Server (VIP). Extra VIPs can be added using the WUI.

- Select *Edit Configuration > Layer 4 Configuration > Virtual Servers*

*NB. If the wizard was used, you'll see the VIP that was created by the wizard*

### EDIT CONFIGURATION > VIRTUAL SERVERS

[ Add a new Virtual Server ]

VIP1	192.168.69.35	Port 80 - tcp	Direct Routing	[ Modify ]	[ Delete ]
------	---------------	---------------	----------------	------------	------------

- Click [Add a new Virtual Server]

### EDIT CONFIGURATION > ADD A NEW VIRTUAL SERVER

Label	<input type="text" value="VIP Name"/>	?
Virtual Server IP address	<input type="text" value="10.0.0.20"/>	?
Virtual Server Ports	<input type="text" value="80"/>	?
Forwarding Method	<input type="text" value="Direct Routing"/>	?
Persistent	<input type="text" value="no"/>	?
Protocol	<input type="text" value="TCP"/>	?
<input type="button" value="Update"/>		

- Define the required settings for the new VIP:
  - Enter the Label, IP address and port(s) for the VIP
  - Select the required forwarding method
  - Enable persistence if required
  - Set the protocol (normally TCP)

## Adding Real Servers

If used, the wizard sets up a single Real Server (RIP). Extra RIPs can be added using the WUI.

- Select *Edit Configuration > Layer 4 Configuration > Real Servers*

*NB. If the wizard was used, you'll see the RIP that was created by the wizard*

### EDIT CONFIGURATION > REAL SERVERS

VIP1	192.168.69.35	Port 80	Direct Routing	[ Add a new Real Server ]
RIP1	192.168.68.41		Weight 1	[ Modify ] [ Delete ]

- Click [Add a new Real Server]

### EDIT CONFIGURATION > ADD A NEW REAL SERVER

Label	<input type="text" value="RIP Name"/>	?
Real Server IP Address	<input type="text" value="IPAddress"/>	?
Weight	<input type="text" value="1"/>	?
Minimum Connections	<input type="text" value="0"/>	?
Maximum Connections	<input type="text" value="0"/>	?
<input type="button" value="Update"/>		

- Define the required settings for the new RIP:
  - Enter the Label, IP address and port for the RIP
  - Set the weight – this defaults to 1. If real servers have different performance specifications, then the weight can be adjusted – a higher number means more traffic is sent to that server
  - Leave the Minimum & Maximum Connections set to 0 for unrestricted

## Configuring the Real Servers

Depending on the deployment method (DR, NAT or SNAT) used, the actual physical servers may need additional configuration to allow the load balancer to operate correctly. The following sections define what is needed for the various modes.

### Configuring the Real Servers for Layer 4 NAT Mode

If you are using a two-arm NAT load balancing method, the real server configuration is a simple case of configuring the load balancer as the default gateway. Normally, a floating IP address is added using *Edit Configuration > Floating IPs*. This is important when a master / slave configuration is used to allow failover & failback of the default gateway address.



Failure to correctly configure the real servers default gateway is the most common mistake when using NAT mode.

### Configuring the Real Servers for Layer 4 DR Mode (Linux)

If you are using the one-arm DR load balancing method, each real server requires the ARP problem to be solved. All real servers must be configured to respond to the VIP address as well as the RIP address. This is because in DR mode load balanced traffic arrives on the VIP address, whilst other traffic such as health-checks, administration traffic etc. use the real server's IP address.

#### Detecting the ARP Problem

You can use *Reports > Layer 4 Current Connections* to check whether the ARP problem has been solved. If not, the connection state will be SYN\_RECV as shown below when a client connection to the VIP is attempted:

#### REPORTS > LAYER 4 CURRENT CONNECTIONS

```
IPVS connection entries
pro expire state      source          virtual         destination
TCP 00:51  SYN_RECV  192.168.2.7:64763  192.168.2.109:80  192.168.2.99:80
```

#### Solving for Linux – Method 1 (using iptables)

You can use iptables (netfilter) on each real server to re-direct incoming packets destined for the virtual server IP address. To make this permanent, simply add the command to an appropriate start-up script such as /etc/rc.local. If the real server is serving multiple VIPs, add additional iptables rules for each VIP.

```
iptables -t nat -A PREROUTING -p tcp -d <VIP> -j REDIRECT
```

e.g.

```
iptables -t nat -A PREROUTING -p tcp -d 10.0.0.21 -j REDIRECT
```

this means redirect any incoming packets destined for 10.0.0.21 (the virtual server) locally.



Method 1 does not work with IPv6 Virtual Servers, use method 2 below instead.

#### Solving for Linux – Method 2 (using arp\_ignore sysctl values)

This is the preferred method as it supports both IPv4 and IPv6. Each real server needs the loopback adapter to be configured with the Virtual Servers IP address. This address must not respond to ARP requests and the web server also needs to be configured to respond to this address. To set this up follow steps 1-3 below.

#### Step 1 : re-configure ARP on the real servers (this step can be skipped for IPv6 virtual servers)

To do this add the following lines to /etc/sysctl.conf:

```
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
```

#### Step 2 : apply these settings

Either reboot the real server or run the following command to apply these settings:

```
/sbin/sysctl -p
```

#### Step 3 : add the virtual servers' IP address to the loopback adapter

run the following command for each VIP. To make this permanent, simply add the command to an appropriate startup script such as /etc/rc.local.

```
ip addr add dev lo <IPv4-VIP>/32
```

*for IPv6 addresses use:*

```
ip addr add dev lo <IPv6-VIP>/128
```

Alternatively, modify the appropriate interface script to add the additional IP address(es).



Failure to correctly configure the real servers to handle the ARP problem is the most common mistake in DR mode configurations.

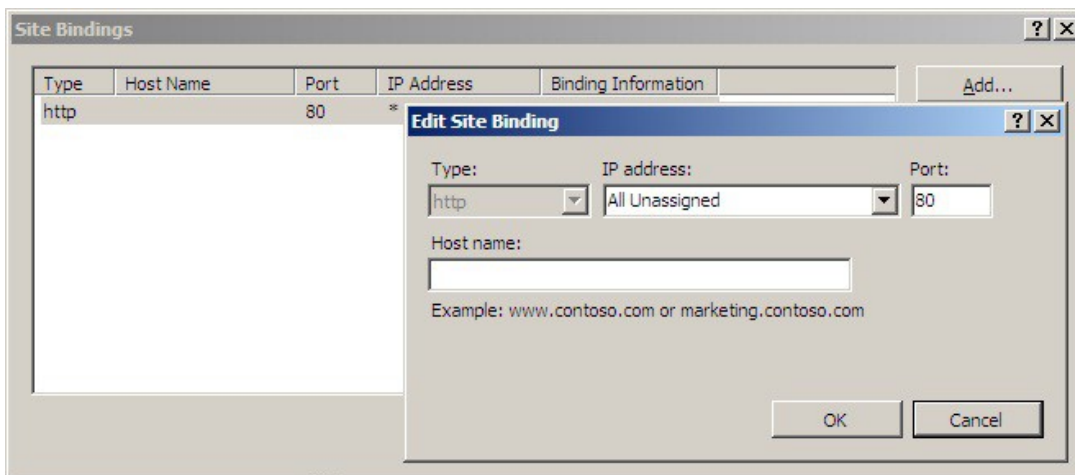
## Configuring the Real Servers for Layer 4 DR Mode (Windows)

If you're using a one-arm DR mode load balancing method, each web server requires the ARP problem to be handled:

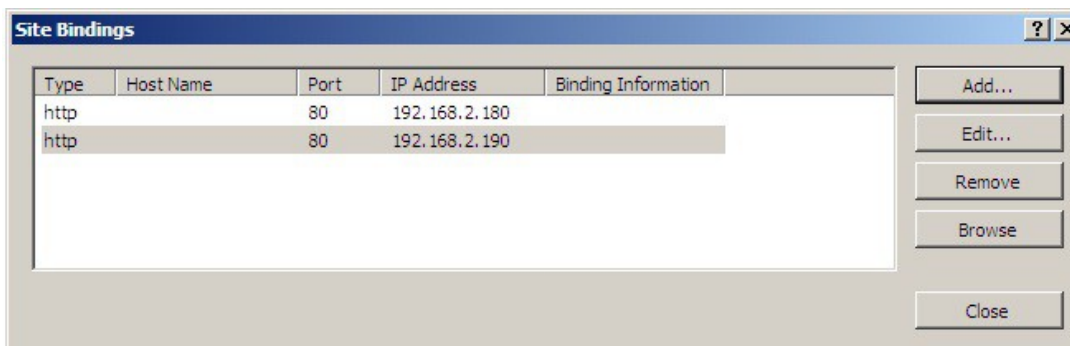
- For all real servers in Direct Routing mode the load balanced application must respond to both the Virtual IP as well as the servers Real IP. With Windows IIS the IP address must either be set to 'All Unassigned' or use the Advanced tab to add a second IP address as shown below
- Each real server must have the Microsoft loopback adapter installed and configured
- The Microsoft loopback adapter must be configured to deal with the ARP problem
- For Windows 2008 / 2012 a series of three netsh commands must also be run on each server to configure the weak / strong host behavior

### Configuring IIS to Respond to Both the RIP and VIP

By default, IIS listens on all configured IP addresses, this is shown in the example below. As can be seen the IP address field is set to 'All Unassigned'.



If the default configuration is left, no further IIS configuration is required. If you do change the IP address in the bindings from 'All Unassigned' to a specific IP address, then you need to make sure that you also add a binding for the Virtual Server IP address (VIP) as shown below:



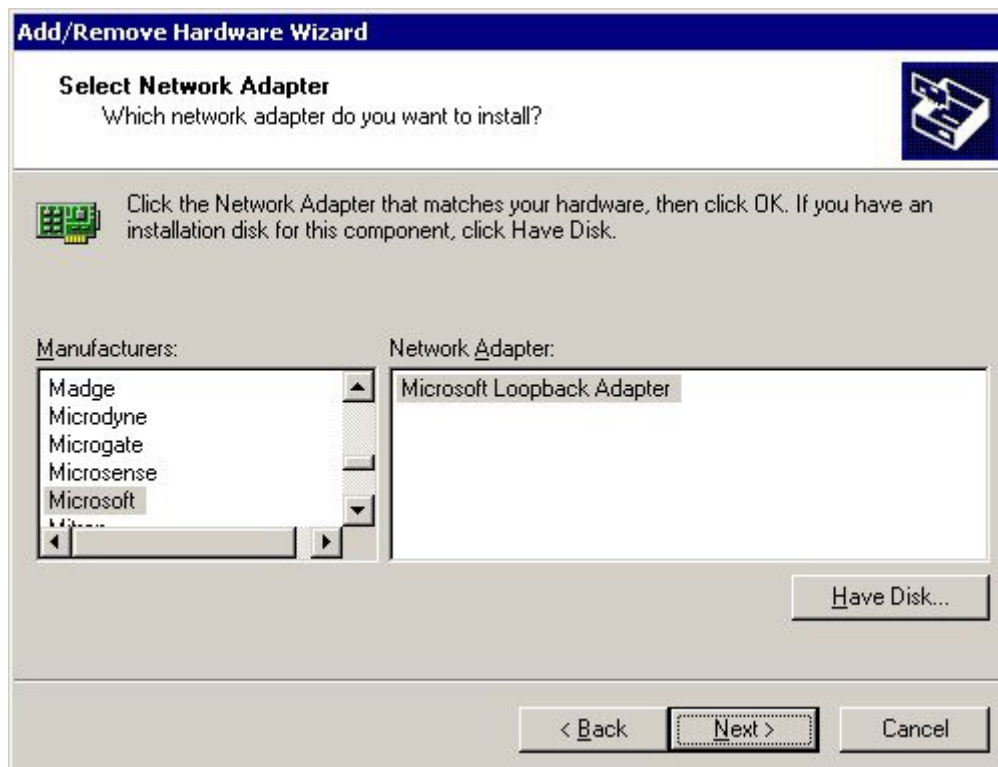


### Resolving ARP issues for Windows server 2000 (applies to DR mode only)

Windows 2000 Server supports the direct routing (DR) method through the use of the MS loopback adapter to handle the traffic. The IP address on the loopback adapter must be set to be the same as the Virtual Servers IP address (VIP). If the real server is included in multiple VIPs, you can add additional IP addresses to the loopback adapter that correspond to each VIP.

#### Step 1 – Install the Microsoft loopback adapter

1. Open the Control Panel and double-click **Add/Remove Hardware**
2. Once the Hardware Wizard opens, click **Next**
3. Select **Add/Troubleshoot a device**, click **Next**
4. Once the device list appears, select **Add a new device** at the top of the list, click **Next**
5. Select **No, I want to select the hardware from a list**, click **Next**
6. Scroll down the list and select **Network Adapters**, click **Next**
7. Select **Microsoft & Microsoft Loopback Adapter**, click **Next** as shown below

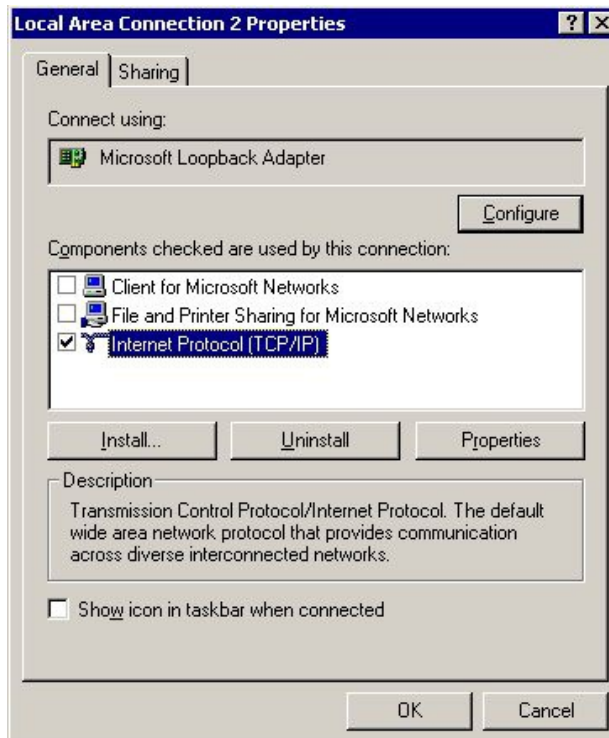


8. Click **Next** to start the installation, when complete click **Finish**

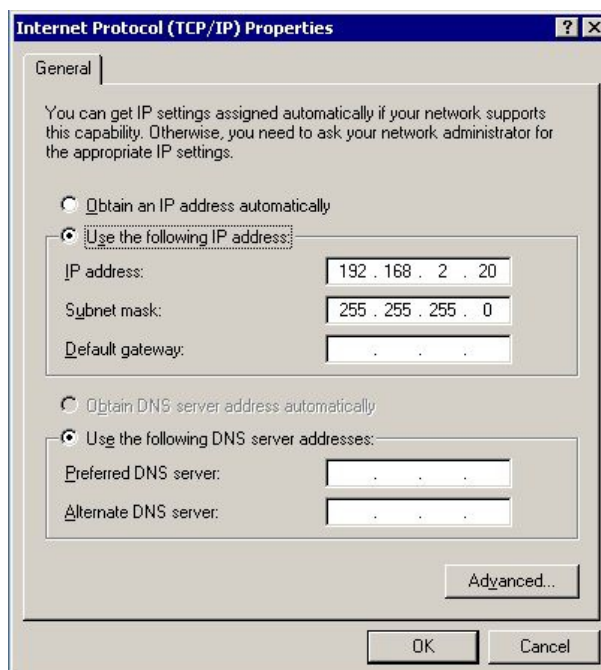


## Step 2 – Configure the loopback adapter

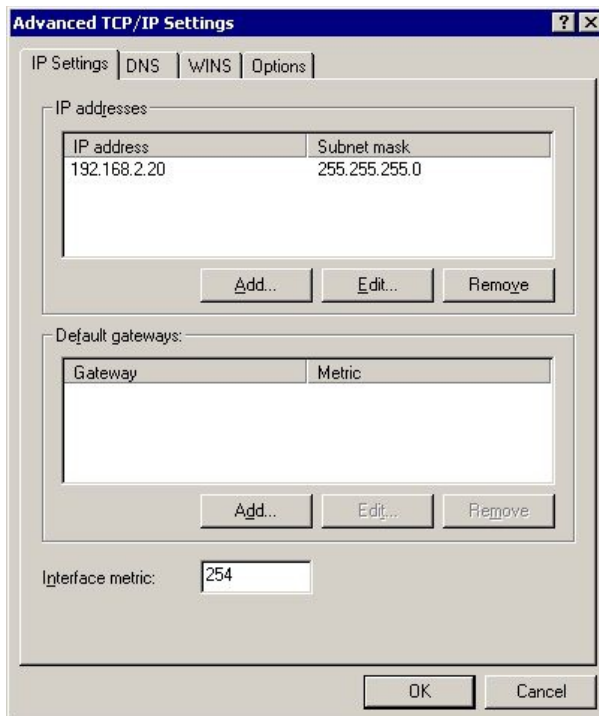
1. Open the Control Panel and double-click **Network and Dial-up Connections**
2. Right-click the new loopback adapter and select **Properties**
3. Un-check all items except **Internet Protocol (TCP/IP)** as shown below



4. Select **Internet Protocol (TCP/IP)**, click **Properties** and configure the IP address and mask to be the same as the Virtual Server IP address (VIP), e.g. 192.168.2.20/24 as shown below



5. Click **Advanced** and change the **Interface metric** to 254 as shown below, this prevents the adapter responding to ARP requests for the VIP address



6. Click **OK** on Advanced Settings, TCP/IP Properties and Connection Properties to save and apply the new settings
7. Repeat the above steps for all other Windows 2000 real servers

### Resolving ARP issues for Windows server 2003 (applies to DR mode only)

Windows server supports the direct routing (DR) method through the use of the MS loopback adapter to handle the traffic. The IP address on the loopback adapter must be set to be the same as the Virtual Servers IP address (VIP). If the real server is included in multiple VIPs, you can add additional IP addresses to the loopback adapter that correspond to each VIP.

#### Step 1 – Install the Microsoft loopback adapter

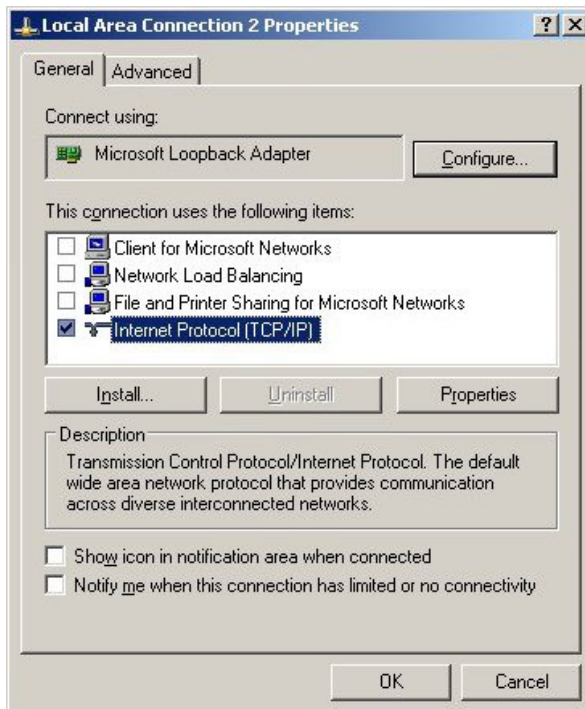
1. Open the Control Panel and double-click **Add Hardware**
2. Once the Hardware Wizard opens, click **Next**
3. Select **Yes, I have already connected the hardware**, click **Next**
4. Scroll to the bottom of the list, select **Add a new hardware device**, click **Next**
5. Select **Install the hardware that I manually select from a list (Advanced)**, click **Next**
6. Select **Network adapters**, click **Next**
7. Select **Microsoft & Microsoft Loopback Adapter**, click **Next** as shown below



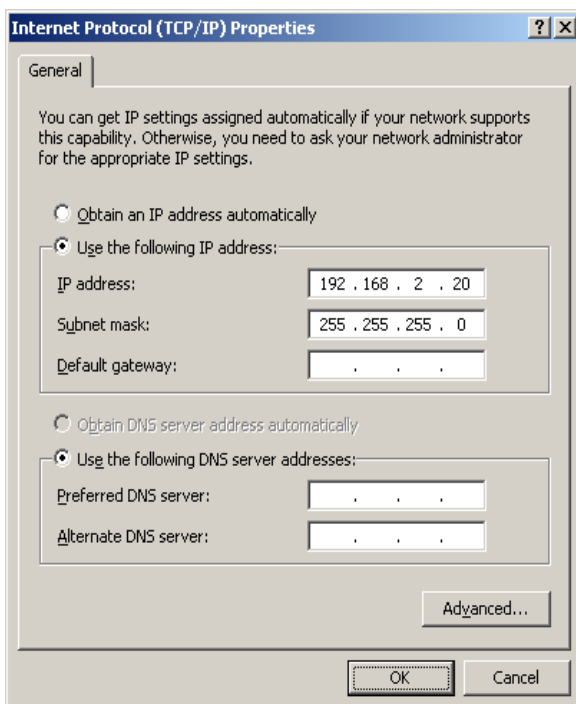
8. Click **Next** to start the installation, when complete click **Finish**

## Step 2 – Configure the loopback adapter

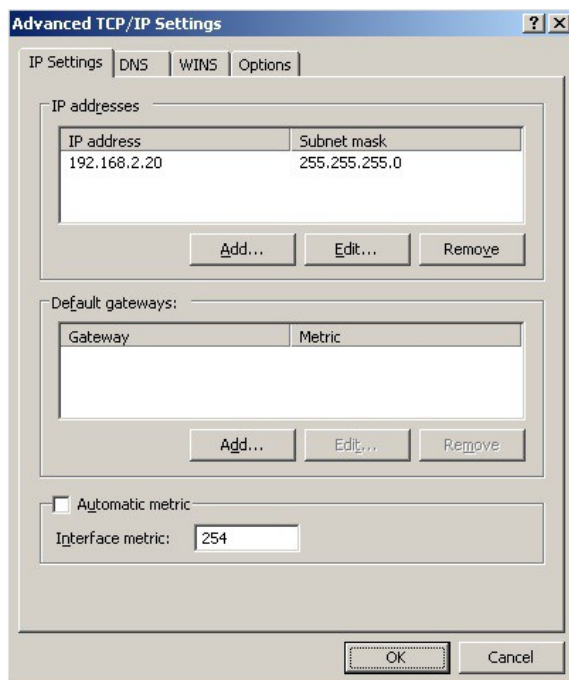
1. Open the Control Panel and double-click **Network Connections**
2. Right-click the new loopback adapter and select **Properties**
3. Un-check all items except **Internet Protocol (TCP/IP)** as shown below



4. Select **Internet Protocol (TCP/IP)**, click **Properties** and configure the IP address and mask to be the same as the Virtual Server (VIP), e.g. 192.168.2.20/24 as shown below



- Click **Advanced**, un-check **Automatic metric** and change **Interface metric** to 254 as shown below, this prevents the adapter responding to ARP requests for the VIP address



- Click **OK** on Advanced Settings & TCP/IP Properties, then click **Close** on Connection Properties to save and apply the new settings
- Now repeat the above process for all other Windows 2003 real servers



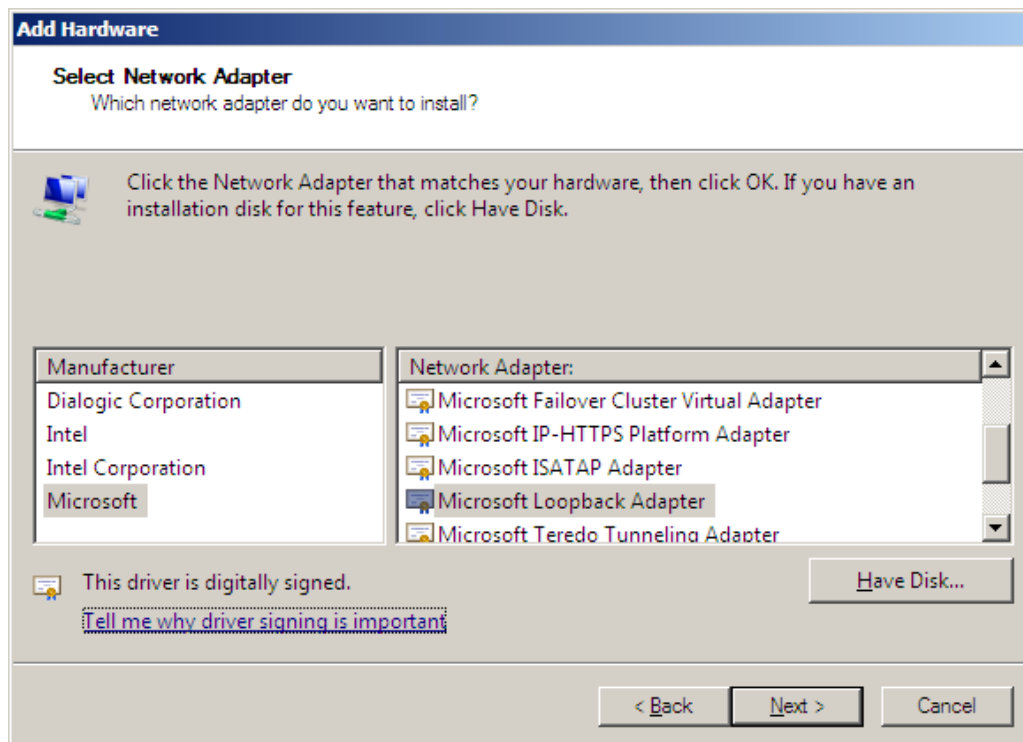
For Windows server 2003 SP1 & later, if you have enabled the built-in firewall, you will need to create an exception to enable access to the web server. This exception by default will allow traffic on both the network and loopback adapters.

### Resolving ARP issues for Windows server 2008 (applies to DR mode only)

The basic concept is the same as for Windows 2000 / 2003. However, additional steps are required to set the strong / weak host behavior. This is used to either block or allow interfaces receiving packets destined for a different interface on the same server. As with Windows 2000 / 2003, If the real server is included in multiple VIPs, you can add additional IP addresses to the loopback adapter that correspond to each VIP.

#### Step 1 – Install the Microsoft loopback adapter

1. Click **Start**, then run **hdwwiz** to start the Hardware Installation Wizard
2. When the Wizard has started, click **Next**
3. Select **Install the hardware that I manually select from a list (Advanced)**, click **Next**
4. Select **Network adapters**, click **Next**
5. Select **Microsoft & Microsoft Loopback Adapter**, click **Next**

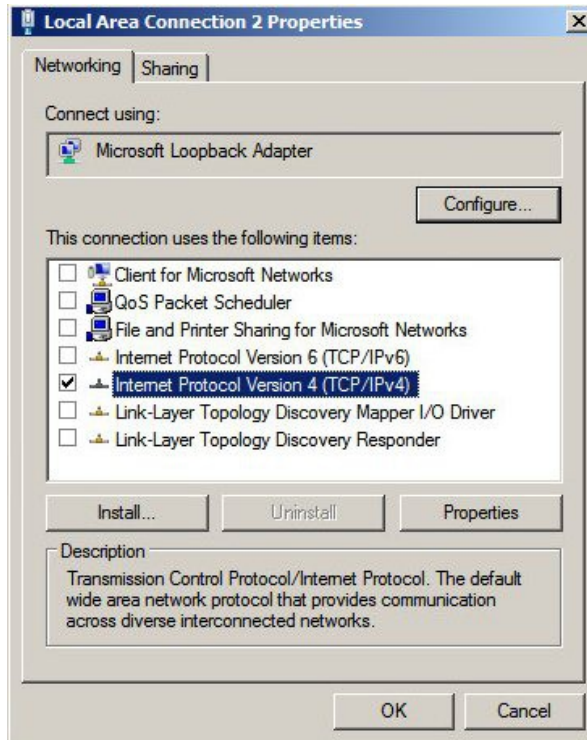


6. Click **Next** to start the installation, when complete click **Finish**

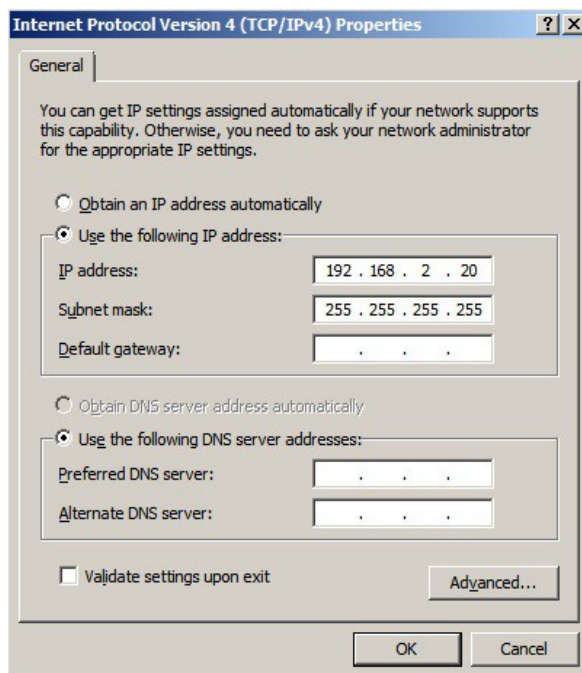
#### Step 2 – Configure the loopback adapter

1. Open Control Panel and click **View Network status and tasks** under **Network and internet**
2. Click **Change adapter settings**
3. Right-click the new Loopback adapter and select **Properties**

- Un-check all items except **Internet Protocol Version 4 (TCP/IPv4)** as shown below



- Select **Internet Protocol Version (TCP/IPv4)**, click **Properties** and configure the IP address to be the same as the Virtual Server (VIP) with a full subnet mask, e.g. 192.168.2.20/32 as shown below



- Click **OK** on TCP/IP Properties, then click **Close** on Connection Properties to save and apply the new settings
- Now repeat the above process on the other Windows 2008 real servers

*N.B. For Windows 2008, it's not necessary to modify the interface metric on the advanced tab and should be left set to Automatic*

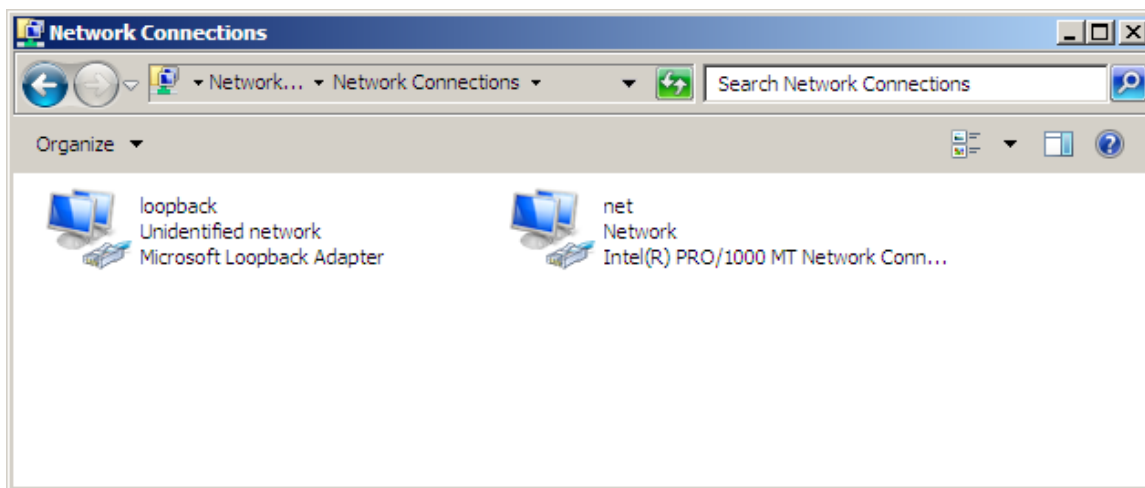
### Step 3 – Configure the strong / weak host behavior

Windows Server 2000 and Windows Server 2003 use the weak host model for sending and receiving for all IPv4 interfaces and the strong host model for sending and receiving for all IPv6 interfaces. You cannot configure this behavior. The Next Generation TCP/IP stack in Windows 2008 and later supports strong host sends and receives for both IPv4 and IPv6 by default. To ensure that the Windows 2008 is running in the correct mode to be able to respond to the VIP, the following commands must be run on each real server:

```
netsh interface ipv4 set interface "net" weakhostreceive=enabled
netsh interface ipv4 set interface "loopback" weakhostreceive=enabled
netsh interface ipv4 set interface "loopback" weakhostsend=enabled
```

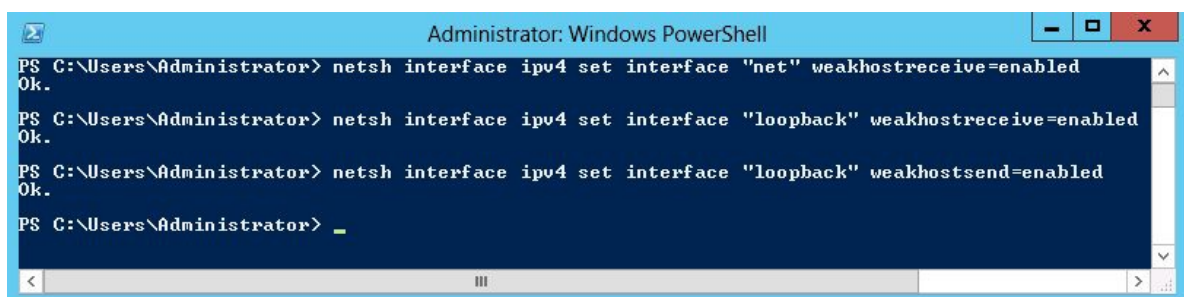
For these commands to work, the LAN connection NIC must be named “net” and the loopback NIC must be named “loopback” as shown below. If you prefer to leave your current NIC names, then the commands above must be modified accordingly. For example, if your network adapters are named “LAN” and “LOOPBACK”, the commands required would be:

```
netsh interface ipv4 set interface "LAN" weakhostreceive=enabled
netsh interface ipv4 set interface "LOOPBACK" weakhostreceive=enabled
netsh interface ipv4 set interface "LOOPBACK" weakhostsend=enabled
```



*N.B. The names for the NICs are case sensitive, so make sure that the name used for the interface and the name used in the commands match exactly.*

1. Start Powershell or use a command Window to run the 3 netsh commands as shown below



2. Now repeat these 3 commands on the other Windows 2008 real servers

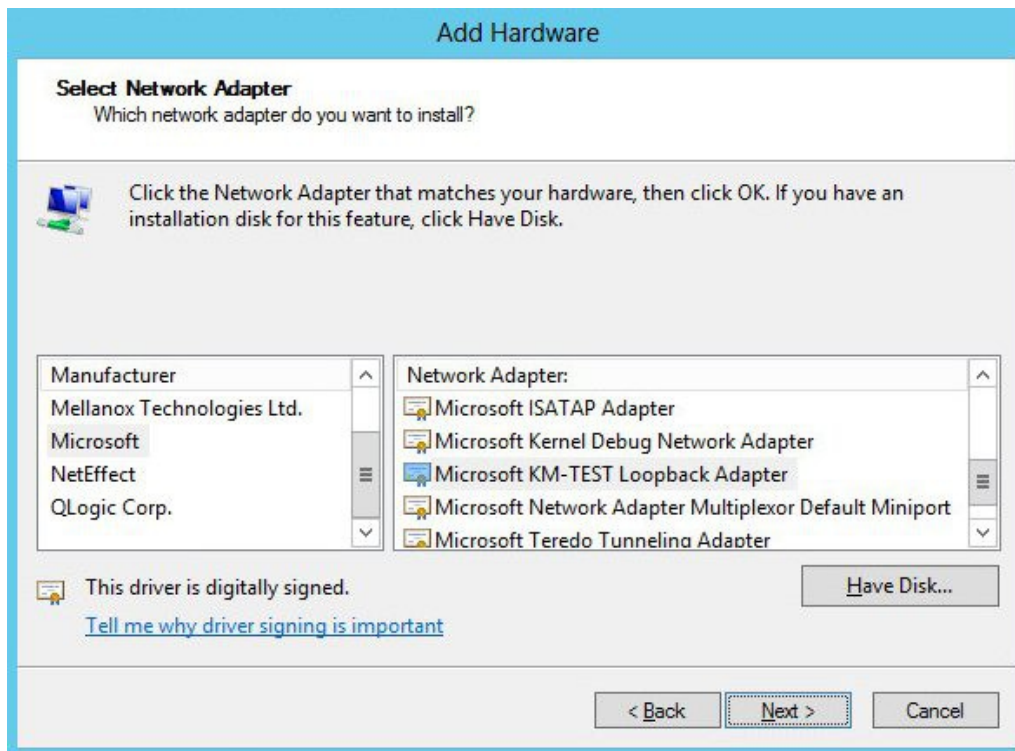


## Resolving ARP issues for Windows server 2012 (applies to DR mode only)

The basic concept is the same as for Windows 2000 / 2003. However, additional steps are required to set the strong / weak host behavior. This is used to either block or allow interfaces receiving packets destined for a different interface on the same server. As with Windows 2000 / 2003 / 2008, If the real server is included in multiple VIPs, you can add additional IP addresses to the loopback adapter that correspond to each VIP.

### Step 1 – Install the Microsoft loopback adapter

1. Click **Start**, then run **hdwwiz** to start the Hardware Installation Wizard
2. When the Wizard has started, click **Next**
3. Select **Install the hardware that I manually select from a list (Advanced)**, click **Next**
4. Select **Network adapters**, click **Next**
5. Select **Microsoft & Microsoft KM-Test Loopback Adapter**, click **Next**

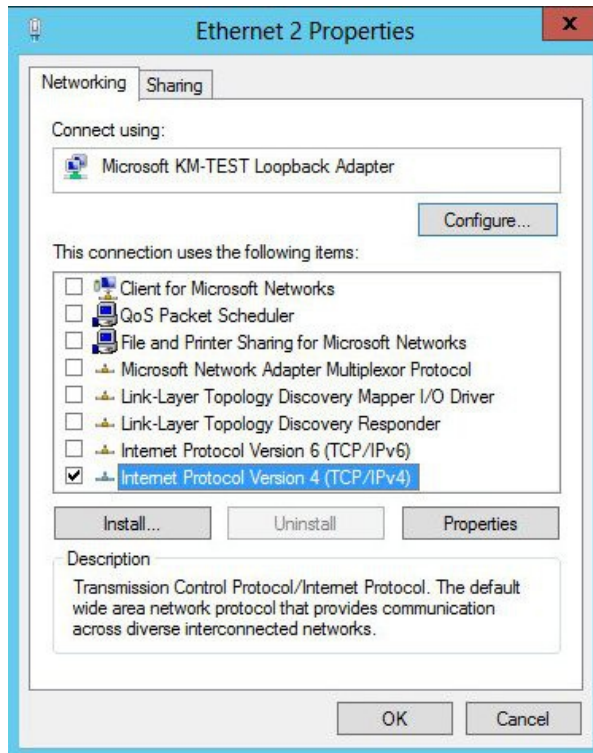


6. Click **Next** to start the installation, when complete click **Finish**

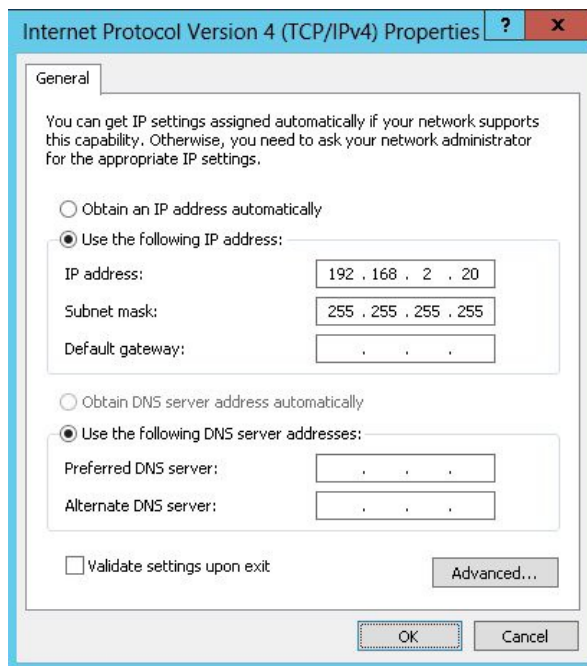
### Step 2 – Configure the loopback adapter

1. Open Control Panel and click **Network and Sharing Center**
2. Click **Change adapter settings**
3. Right-click the new Loopback adapter and select **Properties**

- Un-check all items except **Internet Protocol Version 4 (TCP/IPv4)** as shown below



- Select **Internet Protocol Version (TCP/IPv4)**, click **Properties** and configure the IP address to be the same as the Virtual Server (VIP), with a full subnet mask e.g. 192.168.2.20/32 as shown below



- Click **OK** on TCP/IP Properties, then click **Close** on Ethernet Properties to save and apply the new settings
- Now repeat the above process on the other Windows 2012 real servers

*N.B. For Windows 2012, it's not necessary to modify the interface metric on the advanced tab and should be left set to Automatic*

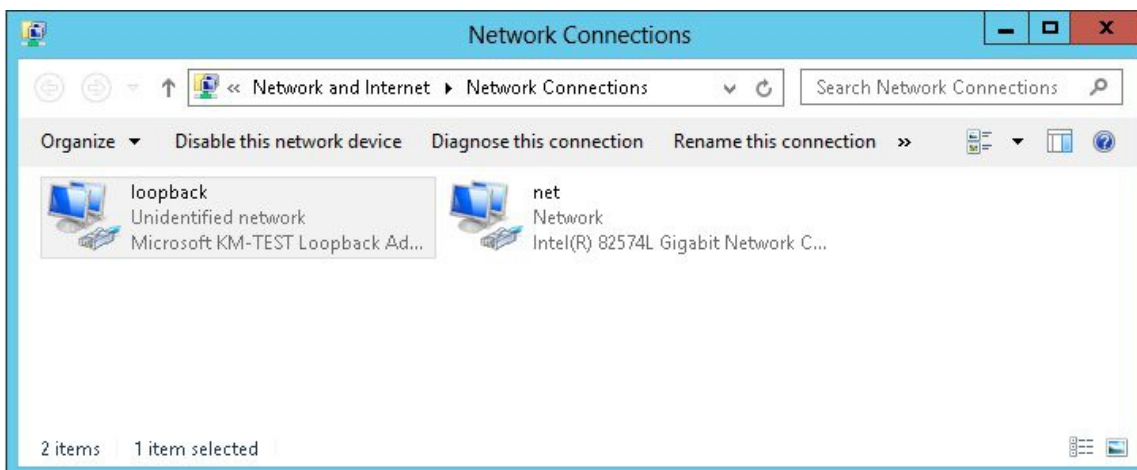
### Step 3 – Configure the strong / weak host behavior

Windows Server 2000 and Windows Server 2003 use the weak host model for sending and receiving for all IPv4 interfaces and the strong host model for sending and receiving for all IPv6 interfaces. You cannot configure this behavior. The Next Generation TCP/IP stack in Windows 2008 and later supports strong host sends and receives for both IPv4 and IPv6 by default. To ensure that the Windows 2008 is running in the correct mode to be able to respond to the VIP, the following commands must be run on each real server:

```
netsh interface ipv4 set interface "net" weakhostreceive=enabled
netsh interface ipv4 set interface "loopback" weakhostreceive=enabled
netsh interface ipv4 set interface "loopback" weakhostsend=enabled
```

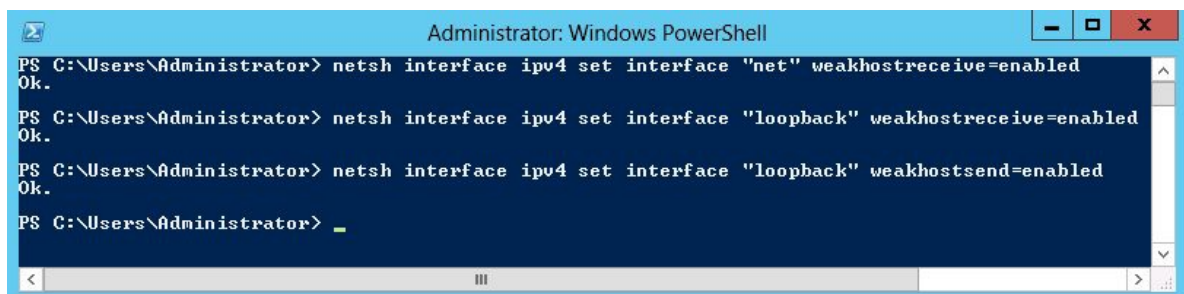
For these commands to work, the LAN connection NIC must be named “net” and the loopback NIC must be named “loopback” as shown below. If you prefer to leave your current NIC names, then the commands above must be modified accordingly. For example, if your network adapters are named “LAN” and “LOOPBACK”, the commands required would be:

```
netsh interface ipv4 set interface "LAN" weakhostreceive=enabled
netsh interface ipv4 set interface "LOOPBACK" weakhostreceive=enabled
netsh interface ipv4 set interface "LOOPBACK" weakhostsend=enabled
```



*N.B. The names for the NICs are case sensitive, so make sure that the name used for the interface and the name used in the commands match exactly.*

1. Start Powershell or use a command Window to run the 3 netsh commands as shown below



2. Now repeat these 3 commands on the other Windows 2012 real servers

## Verifying netsh Settings for Windows 2008 & 2012

To verify that settings have been configured correctly, run the following command on each real server to clearly list the settings that have been applied to the interface:

```
netsh interface ipv4 show interface <interface name>
```

i.e. for the 'loopback' adapter run: netsh interface ipv4 show interface loopback

i.e. for the 'net' adapter run: netsh interface ipv4 show interface net

e.g.

```
C:\Users\Administrator>netsh interface ipv4 show interface loopback
```

```
Interface loopback Parameters
```

```
-----
IfLuid                : ethernet_9
IfIndex               : 15
State                 : connected
Metric                : 30
Link MTU              : 1500 bytes
Reachable Time        : 28500 ms
Base Reachable Time   : 30000 ms
Retransmission Interval : 1000 ms
DAD Transmits         : 3
Site Prefix Length    : 64
Site Id               : 1
Forwarding            : disabled
Advertising           : disabled
Neighbor Discovery     : enabled
Neighbor Unreachability Detection : enabled
Router Discovery      : dhcp
Managed Address Configuration : enabled
Other Stateful Configuration : enabled
Weak Host Sends       : enabled
Weak Host Receives    : enabled
Use Automatic Metric  : enabled
Ignore Default Routes : disabled
Advertised Router Lifetime : 1800 seconds
Advertise Default Route : disabled
Current Hop Limit     : 0
Force ARPND Wake up patterns : disabled
Directed MAC Wake up patterns : disabled
```

```
C:\Users\Administrator>
```

This shows that the settings have been applied correctly.



For Windows server 2008 / 2012, if you want to leave the built-in firewall enabled, you'll either need to enable the relevant default firewall exceptions or create your own to enable access to the web server. By default these exceptions will allow traffic on both the network and loopback adapters.



Failure to correctly configure the real servers to handle the ARP problem is the most common problem in DR configurations.

## Configuring the Real Server for Layer 7 SNAT Mode

When using Layer7 (HAProxy) Virtual Servers, no changes are required to the real servers.

## IPv6 Support

New to v7.x is full IPv6 support. This allows Virtual Servers to be configured using IPv6 addresses. Its also possible to mix IPv4 and IPv6 addresses on a single appliance as illustrated below:

### EDIT CONFIGURATION > NETWORK INTERFACE CONFIGURATION

Bonding

Bond eth0 & eth1 as bond0:

☐

?

Bond eth2 & eth3 as bond1:

☐

?

Bond Interfaces

VLAN

Interface:

eth0

?

VLAN ID:

1

?

Add VLAN

IP Address Assignment

eth0

192.168.2.135/24  
fde6:d14c:3089:1::382/120

eth1

10.12.1.135/24  
fde6:d14c:3089:1::384/120

eth2

eth3

Configure Interfaces

## Testing the Load Balancer Configuration

For testing, add a page to each real web servers root directory e.g. test.html and put the server name on this page for easy identification during your tests.

Now you need a couple of clients to do the testing. Open up a web browser on two different clients and enter the URL for the VIP i.e. http://192.168.1.20/.

Each client should see a different server name because of the load balancing algorithm in use i.e. they are being load balanced across the cluster.

**Why test using two clients?** If you use a single client it will most likely keep on hitting the same server for multiple requests. This is to do with the way that the load balancing algorithms are optimized.



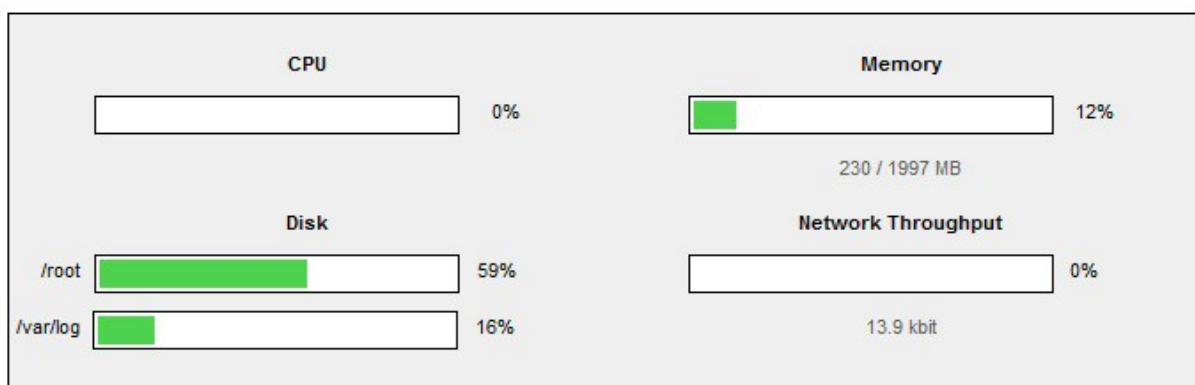
When using a two-arm NAT load balancing method the test client must be in the external subnet.

## Connection Error Diagnosis

If you get a connection error when trying to access the VIP then:

1. Check *View Configuration > Network Configuration* and make sure that the VIP is active on the load balancer, if not check *Logs > Heartbeat* for errors
2. Check *System Overview* and make sure none of your VIPs are highlighted in red. If they are, your cluster is down. Green indicates a healthy cluster, yellow indicates that your cluster may need attention (one real server may be down), and blue indicates a real server has been deliberately taken offline

### VIEW CONFIGURATION > SYSTEM OVERVIEW



Key cluster healthy cluster may need attention cluster is down real server deliberately offline

+	HTTP_Cluster - 192.168.2.182 Ports 80 Protocol TCP	Connections - Active: 0 Inactive: 0
+	FTP_Cluster - 192.168.2.184 Ports 21 Protocol TCP	Connections - Active: 0 Inactive: 0
+	SMTP_Cluster - 192.168.2.186 Ports 25 Protocol TCP	Connections - Active: 0 Inactive: 0



3. If the VIP is still not working then check *Reports > Current Connections* to see the current traffic in detail, any packets marked SYN\_RECV imply incorrect real server configuration. Check that any NAT mode servers have the correct default gateway and any DR mode servers are responding to the VIP as well as their own IP.

## Health Check Diagnosis

Go to the Maintenance > System Overview section of the web interface and check that when you use 'take offline' the connections are redirected to the rest of the cluster as expected.

Pull the network cable out of one of the web servers, wait a few seconds (for the load balancer to detect the change) and then refresh the browsers on both clients. They should now both switch to the same server (as one has been removed from the load balancing list).

Put the network cable back in to the web server, wait a few seconds and then refresh the browsers again. They should now show different web servers again.

Key cluster healthy cluster may need attention cluster is down real server deliberately offline

HTTP_Cluster - 192.168.2.182 Ports 80 Protocol TCP Connections - Active: 0 Inactive: 0								
Label	IP	Method	Weight	Active conns	Inactive conns			
alpha_server	192.168.2.178	DR	1	0	0	Drain	Halt	↑
bravo_server	192.168.2.190	DR	0	0	0	Bring Online		⚙
charlie_server	192.168.2.191	DR	0	0	0	Drain	Halt	↓

'**alpha\_server**' is green which indicates that the server is operating normally.

'**bravo\_server**' is blue, this indicates that it is deliberately in maintenance mode. You can use 'Bring Online' to make it active.

'**charlie\_server**' is down (red). This implies that the real server has failed a health check; you can investigate this using *Logs > Layer 4*. If you know the real server should be active, you may need to increase the health check time-out *Edit Configuration > Layer 4 – Advanced Settings* or *Layer 7 – Advanced Settings*.

## Appliance Log Files

The appliance has a number of log files that are very useful when diagnosing problems. These can be viewed using the WUI under the *Logs* main menu option.

Any errors that occur can prevent services being brought up, so if you're experiencing issues, reviewing the logs for any obvious issues is often a good place to start.

## Testing High-Availability for a Loadbalancer.org HA-Pair

To test fail-over of a clustered pair, once fully configured power down the master and check that the slave unit takes over all the floating IP(s). If fail-over to the slave unit does not occur correctly, check *Logs > Heartbeat* on both nodes for any errors.



It's very important to verify that master / slave failover occurs correctly before going live. This proves the resilience of the cluster and makes you aware of the failover / failback process. Please refer to the administration manual for details of the `hb_takeover` command which can be used to force a failover / failback.



When testing load balancer fail-over, don't just pull the serial cable and network cable out. This will not cause a fail-over but will cause a split brain (i.e. both units active) to occur. You can configure fail-over on network failure but this is not enabled by default. To enable this, a ping node must be configured under *Edit Configuration > Heartbeat Configuration*.

New to v7.x is the role status at the top of each screen. For a working pair, the normal view is shown below:



This shows that the master unit is active and that the heartbeat link is up between master & slave.

Other states:

Master   Slave	Active   Passive	Link	this is a master unit, it's active, no slave unit has been defined
Master   Slave	Active   Passive	Link	this is a master unit, it's active, a slave has been defined but the link to the slave is down. <b>Action:</b> <i>check &amp; verify the heartbeat configuration</i>
Master   Slave	Active   Passive	Link	this is a slave unit, it's active (a failover from the master has occurred) and the heartbeat link to the master has been established
Master   Slave	Active   Passive	Link	this is a master unit, a slave unit has been defined, but the link is down (e.g. serial cable unplugged) so the state cannot be determined. In this case the floating IP's may be active on both units. <b>Action:</b> <i>check &amp; verify the heartbeat configuration, check the serial cable (if applicable), check heartbeat logs &amp; if required restart heartbeat on both units</i>
Master   Slave	Active   Passive	Link	this is the master unit, a slave unit has been defined on the master, but the link is down (e.g. serial cable unplugged) so the state cannot be determined. In this case the heartbeat service has probably stopped on both units. <b>Action:</b> <i>check &amp; verify the heartbeat configuration, check the serial cable (if applicable), check heartbeat logs &amp; if required restart heartbeat on both units</i>

**NB. Restarting heartbeat will cause a temporary outage of all load balanced services**



## Does Your Application Cluster Correctly Handle its Own State?



Load balancers work most effectively if the application servers are completely stateless. This means that if a web server fails and is automatically taken out of the cluster; then all the current user sessions will be transferred to other servers in the cluster without the users needing to re- login to the application again. ***If your application doesn't have a persistent data store then you can't have seamless fail over for your back-end servers.***

Do your web servers store persistent information on local drives?

- Images (jpeg, png, gif etc.)
- Files (html, php, asp etc.)

If so these files either need to be on shared storage such as an NFS/CIFS mount, or they need to be replicated to all of the nodes in the cluster.

### *Replication Solutions for Shared Data*

On UNIX you can use the RSYNC command to replicate files, on Windows Server you can use RSYNC as well but you may prefer ROBOCOPY from the Windows Server Resource Kit. Usually you will upload your content to one master server and then replicate it to the other servers in the cluster.

### *Solutions for Session Data*

Standard ASP and PHP session data is stored locally by default, leaving your session data in a local store will prevent you from implementing seamless application server fail-over in your cluster. If an application server fails, all of the local session data will be lost and your user will need to re-log in and possibly lose shopping baskets etc.

This problem is easily resolvable by implementing a shared persistent data store for the cluster. This is usually either done with a shared back-end database or a shared memory solution.

### *Persistence*

Persistence is a feature that is required by many web applications. Once a user has interacted with a particular server all subsequent requests are sent to the same server thus persisting to that particular server. It is normally required when the session state is stored locally to the web server as opposed to a database.

## *What do You do if Your Application is Not Stateless?*

Some applications require state to be maintained such as:

- Terminal Services
- SSH
- FTP (upload)
- SMTP (incoming)

You may also find that you are unable to modify your HTTP/HTTPS based application to handle shared session data.

For these cases, you can use persistence based on source IP address. You lose the ability to have transparent fail-over, but you do still get increased capacity and manageability. This persistence problem occurs with all load balancers and all vendors use standard methods and technologies to mitigate the issue.

## *Loadbalancer.org Persistence Methods*

- Source IP (subnet)
- Cookie (Active or Passive)

The standard Layer 4 persistence method is source IP persistence, you can handle millions of persistent connections at Layer 4. Just modify your virtual server to be persistent if you require source IP persistence.

Cookies are a Layer 7 based persistence method that can offer more even traffic distribution and also handle any clients where the source IP address may change during the session (e.g. mega proxies).

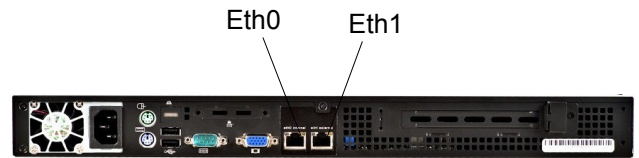
## Loadbalancer.org Technical Support

If you have any questions regarding the appliance don't hesitate to contact the support team [support@loadbalancer.org](mailto:support@loadbalancer.org) or your local reseller.

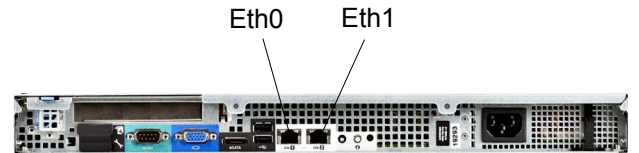
For more details please refer to our full administration manual which is available at:  
<http://www.loadbalancer.org/pdffiles/loadbalanceradministrationv7.pdf>

## Appendix A – Physical Appliance Front & Rear Panel Layouts (for reference)

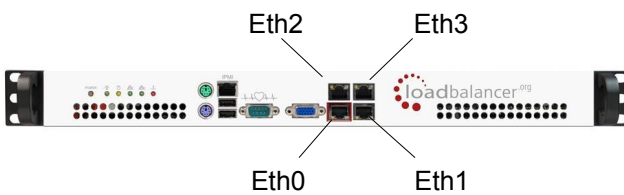
### Enterprise / Enterprise R16 – Supermicro



### Enterprise – Dell



### Enterprise Max – Supermicro



### Enterprise Max / 10G – Dell

