Load Balancing Dispatcher
Phoenix®
v1.0.1

Deployment Guide

loadbalancer.org
1. About this Guide
This guide details the steps required to configure a load balanced Konica Minolta Dispatcher Phoenix environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any Konica Minolta Dispatcher Phoenix configuration changes that are required to enable load balancing.

For more information about initial appliance deployment, network configuration and using the Web User Interface (WebUI), please also refer to the Administration Manual.

2. Loadbalancer.org Appliances Supported
All our products can be used with Konica Minolta Dispatcher Phoenix. For full specifications of available models please refer to: https://www.loadbalancer.org/products.

Some features may not be supported in all cloud platforms due to platform specific limitations, please check with Loadbalancer.org support for further details.

3. Loadbalancer.org Software Versions Supported
   • V8.3.8 and later

4. Konica Minolta Dispatcher Phoenix Software Versions Supported
   • Konica Minolta Dispatcher Phoenix – all versions

5. Konica Minolta Dispatcher Phoenix
Konica Minolta's Dispatcher Phoenix is a powerful application that can help any business save time by automating document image processing, printing, and routing tasks via customisable workflows. With a large variety of processing features, virtually everything is possible – from cleaning up images, applying watermarks and annotations, and renaming files to routing documents to folders, FTP servers, MFPs, or e-mail recipients – and it's all fully automatic! Unique LiveFlo technology provides a real-time view of documents as they are being processed – a great way to identify bottlenecks and making sure files will reach their correct destinations. Dispatcher Phoenix provides busy offices with the convenience and flexibility they need.

The application is highly scalable up to the largest enterprise environments. Dispatcher Phoenix includes a web user interface for access to important enterprise tools – such as apps for setting up server clusters for redundancy/load balancing, failover, offloading, sharing workflows with specific users, and more. Administrators can manage their workflows (run, stop, pause) from the web as well as edit user variables and view important analytics about work being done, including the number of documents being scanned, files collected, and users scanning.

6. Load Balancing Konica Minolta Dispatcher Phoenix
For Konica Minolta Dispatcher Phoenix, the preferred load balancing method is Layer 4 DR Mode (Direct Routing, aka DSR / Direct Server Return). This is a very high performance solution that requires little change to your existing infrastructure. It is necessary to solve “the ARP problem” on the real print servers. This is a straightforward process, and is detailed on page 22 in the appendix.

Where it's not feasible to use layer 4 DR mode, layer 7 SNAT mode should be used. Whist this mode does not have the raw throughput of layer 4 methods, it still enables high performance load balancing and requires no changes to the print
7. Load Balancer Deployment Methods

As mentioned above, Layer 4 DR mode and Layer 7 SNAT mode can be used. Both methods are described below.

Layer 4 DR Mode

One-arm direct routing (DR) mode is a very high performance solution that requires little change to your existing infrastructure.

- DR mode works by changing the destination MAC address of the incoming packet to match the selected Real Server on the fly which is very fast.
- When the packet reaches the Real Server it expects the Real Server to own the Virtual Services IP address (VIP). This means that you need to ensure that the Real Server (and the load balanced application) respond to both the Real Servers own IP address and the VIP.
- The Real Server should not respond to ARP requests for the VIP. Only the load balancer should do this. Configuring the Real Servers in this way is referred to as *Solving the ARP Problem*. Please refer to page 22 for more information.
- 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.
- The load balancer must have an Interface in the same subnet as the Real Servers to ensure layer 2 connectivity required for DR mode to work.
- The VIP can be brought up on the same subnet as the Real Servers, or on a different subnet provided that the load balancer has an interface in that subnet.
- 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.
Layer 7 SNAT Mode

Layer 7 SNAT mode uses a proxy (HAProxy) at the application layer. Inbound requests are terminated on the load balancer, and HAProxy generates a new request to the chosen Real Server. As a result, Layer 7 is a slower technique than DR or NAT mode at Layer 4. Layer 7 is typically chosen when either enhanced options such as SSL termination, cookie based persistence, URL rewriting, header insertion/deletion etc. are required, or when the network topology prohibits the use of the layer 4 methods.

This mode can be deployed in a one-arm or two-arm configuration and does not require any changes to the Real Servers. However, since the load balancer is acting as a full proxy it doesn't have the same raw throughput as the layer 4 methods.

The load balancer proxies the application traffic to the servers so that the source of all traffic becomes the load balancer.

- SNAT mode is a full proxy and therefore load balanced Real Servers do not need to be changed in any way
- Because SNAT mode is a full proxy any server in the cluster can be on any accessible subnet including across the Internet or WAN
- SNAT mode 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 own IP address by default, or any other local appliance IP address if preferred (e.g. the VIP address), this can be configured per layer 7 VIP. If required, the clients IP address can be passed through either by enabling TProxy on the load balancer, or for HTTP, using X-forwarded-For headers. Please refer to chapter 6 in the Administration Manual for more details
- SNAT mode can be deployed using either a 1-arm or 2-arm configuration
8. Dispatcher Phoenix Deployment Concept

VIPs = Virtual IP Addresses

9. Load Balancing Konica Minolta Dispatcher Phoenix

Note: It's highly recommended that you have a working Konica Minolta Dispatcher Phoenix environment first before implementing the load balancer.

Load Balancing & HA Requirements
In order to be successfully load balanced, a Konica Minolta Dispatcher Phoenix deployment must include the following components:

- Wide Area Network (WAN)
- Local Area Network (LAN)
- Firewall
- SQL Server
- Web Server
- Active Directory
- File Share

It is likely that a fully functional Dispatcher Phoenix deployment will already feature all of these components.
Persistence (aka Server Affinity)
Source IP address persistence is used for Dispatcher Phoenix servers. This ensures that a particular client will connect to the same Dispatcher Phoenix server for the duration of the session.

Virtual Service (VIP) Requirements
To provide load balancing and HA for Dispatcher Phoenix, 2 VIPs are used. The first VIP is for the underlying Microsoft print services and the second VIP is for the particular Konica Minolta service being load balanced.

Port Requirements
The following tables show the ports that are load balanced for the various Konica Minolta services:

KMBS BEST Server

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocols</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>50808</td>
<td>HTTP</td>
<td>KMBS BEST Server</td>
</tr>
<tr>
<td>50809</td>
<td>HTTPS</td>
<td>Secure BEST Server</td>
</tr>
</tbody>
</table>

KMBS LPR Service

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocols</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>515</td>
<td>TCP</td>
<td>LPR Service (LPD)</td>
</tr>
</tbody>
</table>

KMBS SMTP Service

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocols</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>TCP</td>
<td>Default, but configurable within SMTP Manager</td>
</tr>
</tbody>
</table>

KMBS SEC Workflow Worker Process

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocols</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>TCP</td>
<td>Output Port</td>
</tr>
<tr>
<td>53</td>
<td>TCP</td>
<td>Output Port</td>
</tr>
<tr>
<td>80</td>
<td>TCP</td>
<td>Output Port</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>Output Port</td>
</tr>
<tr>
<td>445</td>
<td>TCP</td>
<td>Output Port</td>
</tr>
<tr>
<td>465</td>
<td>TCP</td>
<td>Output Port</td>
</tr>
<tr>
<td>587</td>
<td>TCP</td>
<td>Output Port</td>
</tr>
</tbody>
</table>
Virtual Appliance Download & Deployment
A fully featured, fully supported 30 day trial is available if you are conducting a PoC (Proof of Concept) deployment. The VA is currently available for VMware, Virtual Box, Hyper-V, KVM and XEN and has been optimized for each Hypervisor. By default, the VA is allocated 1 CPU, 2GB of RAM and has an 8GB virtual disk. The Virtual Appliance can be downloaded here.

Note: The same download is used for the licensed product, the only difference is that a license key file (supplied by our sales team when the product is purchased) must be applied using the appliance's WebUI.

Note: Please refer to the Administration Manual and the ReadMe.txt text file included in the VA download for more detailed information on deploying the VA using various Hypervisors.

Initial Network Configuration
The IP address, subnet mask, default gateway and DNS settings can be configured as detailed below:

Using the Network Setup Wizard at the console
After boot up, follow the instructions on the console to configure the IP address, subnet mask, default gateway and DNS settings.

Important: be sure to set a secure password for the load balancer, when prompted during the setup routine.

Accessing the Web User Interface (WebUI)
The WebUI can be accessed via HTTPS at the following URL: https://192.168.2.21:9443/lbadmin

* Note the port number → 9443

(replace 192.168.2.21 with the IP address of your load balancer if it's been changed from the default)

Login using the following credentials:

Username: loadbalancer
Password: loadbalancer

Note: To change the password, use the WebUI menu option: Maintenance > Passwords.
Once logged in, the WebUI will be displayed as shown below:

HA Clustered Pair Configuration
Loadbalancer.org recommend that load balancer appliances are deployed in pairs for high availability. In this guide a single unit is deployed first, adding a secondary slave unit is covered in section 2 of the appendix on page 27.
11. Load Balancing Konica Minolta Dispatcher Phoenix – Using DR Mode

Part 1 – Prepare the Konica Minolta Servers for Load Balancing

Step 1 – Prerequisites
For a load balanced Konica Minolta Dispatcher Phoenix environment, each print server must comply with the following requirements:

- Be a member of a Microsoft Windows Domain
- Have the Print and Document Service role / Print Server service installed
- Have all required printers installed and shared – the share names and permissions must be the same across all servers
- Have Konica Minolta Dispatcher Phoenix installed

Step 2 – Solve The ARP Problem On Each Server
When using layer 4 DR mode, the “ARP problem" must be solved on each print server for DR mode to work. For detailed steps on solving the ARP problem for Windows, please refer to section 1 of the appendix on page 22 for more information.

For a detailed explanation of DR mode and the nature of the ARP problem, please refer to the section that covers layer 4 DR mode on page 5.

Step 3 – Configure Registry Entries
For the load balanced print servers, to enable them to be accessed via a shared name (Dispatcher is the example used in this guide), add the following registry entries to each print server:

Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
Value: DisableLoopbackCheck
Type: REG_DWORD
Data: 1

Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters
Value: DisableStrictNameChecking
Type: REG_DWORD
Data: 1

Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters
Value: OptionalNames
Type: REG_MULTI_SZ
Data: Dispatcher
Note: In the example presented here, **Dispatcher** is the name that will be used to access the load balanced print servers via the virtual service (VIP) created on the load balancer. This can be set to any appropriate name. Whatever name is used, it must resolve to the IP address of the VIP.

**Step 4 – Configure Name Resolution**

For printer load balancing to work, DNS name resolution should be configured. A DNS Host (A) record for the printer share name (**Dispatcher** in this example) that points at the Phoenix Dispatcher VIP (**192.168.81.10** in this example) is required.

In addition, NetBIOS over TCPIIP should be disabled on all interfaces on each print server as shown below:

![Advanced TCP/IP Settings](image)

When configuring printers to connect back to the highly available Dispatcher Phoenix, the Dispatcher Phoenix hostname / IP address should be the VIP address and not the individual Dispatcher Phoenix host name or IP address.

**Step 5 – Reboot Each Print Server**

To apply all settings, reboot each print server.
Part 2 – Configure Load Balancing for Microsoft Print Server

Configure The Virtual Service (VIP)

1. Using the web user interface, navigate to Cluster Configuration > Layer 4 – Virtual Services and click on Add a new Virtual Service

   ![Virtual Service Configuration](image)

   2. Define the Label for the virtual service as required, e.g. PrintServers
   3. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.81.10
   4. Set the Ports to 445
   5. Leave Protocol set to TCP
   6. Leave Forwarding Method set to Direct Routing
   7. Click Update

Define The Real Servers (RIPs)

1. Using the web user interface, navigate to Cluster Configuration > Layer 4 – Real Servers and click on Add a new Real Server next to the newly created VIP

   ![Real Server Configuration](image)
2. Define the *Label* for the Real Server as required, e.g. **PS1**
3. Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.81.184**
4. Click *Update*
5. Repeat these steps to add additional print servers as required

**Part 3 – Configure Load Balancing for Konica Minolta Dispatcher Phoenix**

**Configure The Virtual Service (VIP)**

1. Using the web user interface, navigate to *Cluster Configuration > Layer 4 – Virtual Services* and click on **Add a new Virtual Service**

![Virtual Service Configuration](image)

2. Define the *Label* for the virtual service as required, e.g. **Dispatcher**
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.81.10**
4. Set the *Ports* field according to the load balanced service – please refer to page 8

Note: If you are load balancing “KMBS SEC Workflow Worker Process”, exclude port 445 from the list of ports since this port is load balanced by the Microsoft Print Server VIP configured previously.

5. Leave *Protocol* set to **TCP**
6. Leave the *Forwarding Method* set to **Direct Routing**
7. Click *Update*
8. Click *Modify* next to the newly created VIP
9. Scroll down to the *Health Checks* section and set the *Check Port* to **445**
10. Click *Update*
Define The Real Servers (RIPs)

1. Using the web user interface, navigate to Cluster Configuration > Layer 4 – Real Servers and click on Add a new Real Server next to the newly created VIP.

2. Define the Label for the Real Server as required, e.g. Phoenix1.

3. Set the Real Server IP Address field to the required IP address, e.g. 192.168.81.184.

4. Click Update.

5. Repeat these steps to add additional Dispatcher Phoenix servers as required.
12. Load Balancing Konica Minolta Dispatcher Phoenix – Using SNAT Mode

Part 1 – Prepare the Konica Minolta Servers for Load Balancing

Step 1 – Prerequisites
For a load balanced Konica Minolta Dispatcher Phoenix environment, each print server must comply with the following requirements:

- Be a member of a Microsoft Windows Domain
- Have the Print and Document Service role / Print Server service installed
- Have all required printers installed and shared – the share names and permissions must be the same across all servers
- Have Konica Minolta Dispatcher Phoenix installed

Step 2 – Configure Registry Entries
For the load balanced print servers, to enable them to be accessed via a shared name (Dispatcher is the example used in this guide), add the following registry entries to each print server:

**Key:** HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa  
**Value:** DisableLoopbackCheck  
**Type:** REG_DWORD  
**Data:** 1

**Key:** HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters  
**Value:** DisableStrictNameChecking  
**Type:** REG_DWORD  
**Data:** 1

**Key:** HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters  
**Value:** OptionalNames  
**Type:** REG_MULTI_SZ  
**Data:** Dispatcher

Note: In the example presented here, Dispatcher is the name that will be used to access the load balanced print servers via the virtual service (VIP) created on the load balancer. This can be set to any appropriate name. Whatever name is used, it must resolve to the IP address of the VIP.
Step 3 – Configure Name Resolution

For printer load balancing to work, DNS name resolution should be configured. A DNS Host (A) record for the printer share name (Dispatcher in this example) that points at the Phoenix Dispatcher VIP (192.168.81.10 in this example) is required.

In addition, NetBIOS over TCP/IP should be disabled on all interfaces on each print server as shown below:

![Advanced TCP/IP Settings](image)

When configuring printers to connect back to the highly available Dispatcher Phoenix, the Dispatcher Phoenix hostname / IP address should be the VIP address and not the individual Dispatcher Phoenix host name or IP address.

Step 4 – Reboot Each Print Server

To apply all settings, reboot each print server.

Part 2 – Configure Load Balancing for Microsoft Print Server

Configure The Virtual Service (VIP)

1. Using the web user interface, navigate to Cluster Configuration > Layer 7 – Virtual Services and click on Add a new Virtual Service
2. Define the Label for the virtual service as required, e.g. PrintServers
3. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.81.10
4. Set the Ports to 445
5. Set the Layer 7 Protocol to TCP Mode
6. Click Update

Define The Real Servers (RIPs)

1. Using the web user interface, navigate to Cluster Configuration > Layer 7 – Real Servers and click on Add a new Real Server next to the newly created VIP

2. Define the Label for the Real Server as required, e.g. PS1
3. Set the Real Server IP Address field to the required IP address, e.g. 192.168.81.184
4. Leave the Real Server Port field blank
5. Click Update
6. Repeat these steps to add additional print servers as required
Part 3 – Configure Load Balancing for Konica Minolta Dispatcher Phoenix

Configure The Virtual Service (VIP)

1. Using the web user interface, navigate to Cluster Configuration > Layer 7 – Virtual Services and click on **Add a new Virtual Service**

![Virtual Service Configuration Screen](image)

2. Define the **Label** for the virtual service as required, e.g. *Dispatcher*

3. Set the **Virtual Service IP Address** field to the required IP address, e.g. *192.168.81.10*

4. Set the **Ports** field according to the load balanced service – please refer to page 8

**Note:** If you are load balancing “KMBS SEC Workflow Worker Process”, exclude port 445 from the list of ports since this port is load balanced by the Microsoft Print Server VIP configured previously.

5. Set the **Layer 7 Protocol** to **TCP Mode**

6. Click **Update**

7. Click **Modify** next to the newly created VIP

8. Scroll down to the **Health Checks** section and set the **Check Port** to **445**

9. Click **Update**

Define The Real Servers (RIPs)

1. Using the web user interface, navigate to Cluster Configuration > Layer 7 – Real Servers and click on **Add a new Real Server** next to the newly created VIP
2. Define the *Label* for the Real Server as required, e.g. *Phoenix1*
3. Set the *Real Server IP Address* field to the required IP address, e.g. *192.168.81.184*
4. Leave the *Real Server Port* field blank
5. Click *Update*
6. Repeat these steps to add additional print servers as required

**Finalize Settings – Reload HAProxy**

To apply settings and activate the new VIPs, click the **Reload** button in the blue box at the top of the screen.

---

### 13. Testing & Verification

**Testing the Load Balanced Servers**

The load balanced servers can be tested either by browsing to the virtual service IP address or to the printer share name. For example:

Using the Virtual IP address (VIP):

\192.168.81.10

or

Using the printer share name:

\Dispatcher

Any shared printers and shared folders that have been configured on the real print servers should be visible.

**Using System Overview**

The **System Overview** can be viewed in the WebUI. It shows a graphical view of all VIPs & RIPs (i.e. the Dispatcher Phoenix servers) and shows the state/health of each server as well as the state of the each cluster as a whole.

The example below shows that all Real Servers are healthy and available to accept connections.
Note: This example shows layer 4 VIPs. A layer 7 configuration will look very similar.

If a particular server fails its health check, that server will be displayed red rather than green.

14. Technical Support
For more details about configuring the appliance and assistance with designing your deployment please don't hesitate to contact the support team using the following email address: support@loadbalancer.org.

15. Further Documentation

16. Conclusion
Loadbalancer.org appliances provide a very cost effective solution for highly available load balanced Konica Minolta Dispatcher Phoenix environments.
1 - Solving the ARP Problem

When using Layer 4 DR mode, the ARP problem must be solved. This involves configuring each Real Server to be able to receive traffic destined for the VIP, and ensuring that each Real Server does not respond to ARP requests for the VIP address – only the load balancer should do this.

The steps below are for Windows 2012/2016, for other versions of Windows please refer to chapter 6 in the Administration Manual.

**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

![Add Hardware](image)

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**
4. Un-check all items except **Internet Protocol Version 4 (TCP/IPv4)** and **Internet Protocol Version 6 (TCP/IPv6)** as shown below:

![Loopback Properties](image)

Note: Leaving both checked ensures that both IPv4 and IPv6 are supported. Select one if preferred. **Important:** When configuring the Loopback Adapter to solve the ARP Problem, the following options **must** also be checked (ticked):
- Client for Microsoft Networks
- File & Printer Sharing for Microsoft Networks

5. If configuring IPv4 addresses select **Internet Protocol Version (TCP/IPv4)**, click **Properties** and configure the IP address to be the same as the Virtual Service (VIP) with a subnet mask of 255.255.255.255, e.g. 192.168.2.20/255.255.255.255 as shown below:
6. If configuring IPv6 addresses select **Internet Protocol Version (TCP/IPv6)**, click **Properties** and configure the IP address to be the same as the Virtual Service (VIP) and set the **Subnet Prefix Length** to be the same as your network setting, e.g. 2001:470:1f09:e72::15/64 as shown below:

7. Click **OK** on TCP/IP Properties, then click **Close** on Ethernet Properties to save and apply the new settings

8. Now repeat the above process on the other Windows 2012/2016 Real Servers
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 Windows 2012/2016 is running in the correct mode to be able to respond to the VIP, the following commands must be run on each Real Server:

For IPv4 addresses:

```
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
```

For IPv6 addresses:

```
netsh interface ipv6 set interface "net" weakhostreceive=enabled
netsh interface ipv6 set interface "loopback" weakhostreceive=enabled
netsh interface ipv6 set interface "loopback" weakhostsend=enabled
netsh interface ipv6 set interface "loopback" dadtransmits=0
```

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 ipv6 set interface "LAN" weakhostreceive=enabled
netsh interface ipv6 set interface "LOOPBACK" weakhostreceive=enabled
netsh interface ipv6 set interface "LOOPBACK" weakhostsend=enabled
netsh interface ipv6 set interface "LOOPBACK" dadtransmits=0
```
Note: 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 appropriate netsh commands as shown in the example below:

```
netsh interface ipv6 set interface "net" weakhostreceive-enabled
netsh interface ipv6 set interface "loopback" weakhostreceive-enabled
netsh interface ipv6 set interface "loopback" weakhostsend-enabled
netsh interface ipv6 set interface "loopback" datatransmits-0
```

Note: This shows an IPv6 example, use the IPv4 commands if you’re using IPv4 addresses.

2. Now repeat these 4 commands on the other Windows 2012/2016 Real Servers

Note: Solving the ARP problem for other version of Windows is similar. For full details, please refer to the Administration Manual.
2 – Clustered Pair Configuration – Adding a Slave Unit
If you initially configured just the master unit and now need to add a slave - our recommended procedure, please refer to the relevant section below for more details:

Note: A number of settings are not replicated as part of the master/slave pairing process and therefore must be manually configured on the slave appliance. These are listed below:

- Hostname & DNS settings
- Network settings including IP addresses, bonding configuration and VLANs
- Routing configuration including default gateways and static routes
- Date & time settings
- Physical – Advanced Configuration settings including Internet Proxy IP address & port, Firewall table size, SMTP relay and Syslog server
- SNMP settings
- Graphing settings
- Firewall Script & Firewall Lockdown Script settings
- Software updates

To add a slave node – i.e. create a highly available clustered pair:

- Deploy a second appliance that will be the slave and configure initial network settings
- Using the WebUI, navigate to: Cluster Configuration > High-Availability Configuration

- Specify the IP address and the loadbalancer users password (the default is 'loadbalancer') for the slave (peer) appliance as shown above
- Click Add new node
• The pairing process now commences as shown below:

![Create a Clustered Pair](image)

• Once complete, the following will be displayed:

![High Availability Configuration - Master](image)

• To finalize the configuration, restart heartbeat and any other services as prompted in the blue message box at the top of the screen

Note: Clicking the Restart Heartbeat button on the master appliance will also automatically restart heartbeat on the slave appliance.

Note: Please refer to chapter 9 – Appliance Clustering for HA in the Administration Manual for more detailed information on configuring HA with 2 appliances.
## 18. Document Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Change</th>
<th>Reason for Change</th>
<th>Changed By</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.0</td>
<td>21st October 2020</td>
<td>Initial version</td>
<td></td>
<td>NH / RJC</td>
</tr>
<tr>
<td>1.0.1</td>
<td>25th March 2021</td>
<td>Added section &quot;Loadbalancer.org Appliance – the Basics&quot;</td>
<td>Not included in the initial version</td>
<td>RJC</td>
</tr>
</tbody>
</table>
About Loadbalancer.org

Loadbalancer.org’s mission is to ensure that its clients’ businesses are never interrupted. The load balancer experts ask the right questions to get to the heart of what matters, bringing a depth of understanding to each deployment. Experience enables Loadbalancer.org engineers to design less complex, unbreakable solutions - and to provide exceptional personalized support.