1. About this Guide

This guide details the steps required to configure a load balanced Konica Minolta Dispatcher Paragon environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any Konica Minolta Dispatcher Paragon 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 relevant Administration Manual:

- v7 Administration Manual
- v8 Administration Manual

2. Loadbalancer.org Appliances Supported

All our products can be used for load balancing Konica Minolta Dispatcher Paragon. The complete list of models is shown below:

<table>
<thead>
<tr>
<th>Discontinued Models</th>
<th>Current Models *</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise R16</td>
<td>Enterprise R20</td>
</tr>
<tr>
<td>Enterprise VA R16</td>
<td>Enterprise MAX</td>
</tr>
<tr>
<td>Enterprise VA</td>
<td>Enterprise 10G</td>
</tr>
<tr>
<td>Enterprise R320</td>
<td>Enterprise 40G</td>
</tr>
<tr>
<td></td>
<td>Enterprise Ultra</td>
</tr>
<tr>
<td></td>
<td>Enterprise VA R20</td>
</tr>
<tr>
<td></td>
<td>Enterprise VA MAX</td>
</tr>
<tr>
<td></td>
<td>Enterprise AWS **</td>
</tr>
<tr>
<td></td>
<td>Enterprise AZURE **</td>
</tr>
<tr>
<td></td>
<td>Enterprise GCP **</td>
</tr>
</tbody>
</table>

* For full specifications of these models please refer to: http://www.loadbalancer.org/products/hardware
** Some features may not be supported, please check with Loadbalancer.org support

3. Loadbalancer.org Software Versions Supported

- V7.6.4 and later

4. Konica Minolta Dispatcher Paragon Software Versions Supported

- Dispatcher Paragon – all versions
5. Konica Minolta Dispatcher Paragon

The core of Dispatcher Paragon's functionality is the central accounting of all print, copy, and scan operations. Providing comprehensive information with details like job name, first page preview, date, number of pages, and toner coverage, the application greatly facilitates and streamlines administrator tasks. What's more, print administrators can activate pull printing, and create effective print governance policies. Enterprises thus take advantage of a range of tools that allow them to improve print, copy, and scan workflows, and increase employee productivity – all of which ultimately helps lower print-related costs while at the same time maximising document security.

6. Load Balancing Konica Minolta Dispatcher Paragon

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

Introduction and Overview of Load Balancing Methods

For a Dispatcher Paragon deployment, the preferred and default load balancer configuration uses 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 in section 2 of the appendix, Solving the ARP Problem, on page 20.

It is also possible to load balance a Dispatcher Paragon deployment using Layer 7 SNAT Mode. This mode might be preferable if making changes to the real print servers is not possible, although some Windows Registry keys need to be added. Due to the increased amount of information at layer 7, performance is not as fast as at layer 4. Also note that load balanced connections at layer 7 are not source IP transparent, which is not usually an issue when load balancing print servers but should still be considered.

Load Balancing & HA Requirements

A load balanced Konica Minolta Dispatcher Paragon environment requires the following:

- Microsoft Windows Server environment
- Installation of Dispatcher Paragon

Overview of Steps Required

Setting up a load balanced Dispatcher Paragon environment can be summarised as follows:

- Create a virtual service (VIP) on the load balancer that listens on the required ports
- Associate the print servers to the virtual service, i.e. define them as ‘real servers’ (RIPs) for the VIP
- Install and configure the Konica Minolta Windows print servers
- Configure registry settings on the print servers to enable them to be accessed via a shared name
• Configure name resolution related settings on the print servers
• Point users at the VIP to access the print server and the printer shares

7. Deployment Concept

VIPs = Virtual IP Addresses

Note: The load balancer can be deployed as a single unit, although Loadbalancer.org recommends a clustered pair for resilience & high availability. Please refer to section 3 in the appendix on page 25 for more details on configuring a clustered pair.

Virtual Service (VIP) Requirements
A single virtual service is required which load balances Dispatcher Paragon traffic on the required ports.

8. Load Balancer Deployment Methods

The load balancer can be deployed in 4 fundamental ways: Layer 4 DR mode, Layer 4 NAT mode, Layer 4 SNAT mode, and Layer 7 SNAT mode.

For Dispatcher Paragon, using layer 4 DR mode or layer 7 SNAT mode is recommended. These modes are described below and are used for the configurations presented in this guide. For configuring using DR mode please refer to the section starting on page 15, and for configuring using a combination of layer 4 NAT mode and layer 7 SNAT mode refer to the section starting on page 16.
**Layer 4 DR Mode**

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

Note: Kemp, Brocade, Barracuda & A10 Networks call this Direct Server Return and F5 call it N-Path.

- 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 section Solving the ARP Problem on page 20 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

Our Recommendation
Where possible, we recommend that Layer 4 Direct Routing (DR) mode is used. This mode offers the best possible performance since replies go directly from the Real Servers to the client, not via the load balancer. It's also relatively simple to implement. Ultimately, the final choice does depend on your specific requirements and infrastructure.

If DR mode cannot be used, for example if the real servers are located in remote routed networks, then Layer 7 SNAT
mode is recommended. If the load balancer is deployed in AWS, Azure, or GCP, layer 7 SNAT mode must be used as layer 4 direct routing is not currently possible on these platforms.

9. Configuring Print Servers for Load Balancing

The following steps should be carried out on each print server defined in the virtual service:

1. Join the server to the same domain as the client PCs
2. Install the Print and Document Service role / Print Server service
3. Install and share the printers (use exactly the same share names and permissions across all servers)
4. If DR mode is used, solve the “ARP problem” on each print server, to that DR mode will work. For detailed steps on solving the ARP problem for the various versions of Windows, please refer to section 2 of the appendix on page 20 for more information.

Note: Important: When configuring the Loopback Adapter to solve the ARP Problem, the following options must also be checked (ticked):

Client for Microsoft Networks and File & Printer Sharing for Microsoft Networks

Registry Modifications

To enable the print servers to be accessed via a shared name (Dispatcher in the example virtual service 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 as explained in the section below.

**Microsoft Windows Server 2008 Specific Registry Change**

If Microsoft Windows Server 2008 is used as the operating system for the printer servers, an additional registry entry change is required. The following registry entry should be changed from a DWORD to a QWORD:

- **Key:** HKLM\SYSTEM\CurrentControlSet\Control\Print\DNSOneWire
- **Value:** DnsOnWire
- **Type:** REG_QWORD
- **Data:** 1

**Configuring Name Resolution**

For printer load balancing to work, **either** DNS or NetBIOS name resolution should be configured as detailed below.

**DNS Name Resolution (Windows 2000 & Later)**

To configure DNS name resolution, the following steps should be completed:

1. NetBIOS over TCP/IP should be disabled on **all** interfaces of **each** print server, like shown

2. A host name and corresponding “Host (A)” record for the virtual Dispatcher service that matches the virtual IP (VIP) address for the load balancer should be created
NetBIOS Name Resolution (legacy Environments)

To configure NetBIOS name resolution, the following steps should be completed:

1. NetBIOS over TCP/IP should be **disabled on the main NIC** and **left enabled on the Loopback adapter** on each print server
2. Either a WINS server should be set up and all clients configured to use this, or pre-loaded entries in the LMHosts file of each client should be set up

Note: As shown in the flow chart in [this TechNet article](#), for a default H-node client, NetBIOS name resolution occurs in the following order:

1. Local NetBIOS cache
2. WINS server
3. NetBIOS broadcast
4. Local LMHosts file

Therefore, to avoid broadcast, LMHost entries must be declared as pre-loaded to ensure they are available in the local NetBIOS cache.

**Configuring the LMHosts file**

This is done by creating an entry like so:

**Dispatcher 10.10.10.150 #PRE**

Entries with the #PRE directive are loaded into the cache on reboot, or can be forced using the command:

```
nbtstat -R
```

The following command can be used to view the cache and verify that the entry has been added:

```
nbtstat -c
```

**Finalising the Server Configuration**

To finalise the print server configuration changes, **each print server must be rebooted**.

**Installing and Configuring Konica Minolta Dispatcher Paragon**

The Dispatcher Paragon software should be set up by following the steps outlined in the *Konica Minolta Dispatcher Paragon Installation Guide*. 
10. Loadbalancer.org Appliance – the Basics

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 in several ways as detailed below:

Method 1 - 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.

Method 2 - Using the WebUI
Using a browser, connect to the WebUI on the default IP address/port: https://192.168.2.21:9443
To set the IP address & subnet mask, use: Local Configuration > Network Interface Configuration
To set the default gateway, use: Local Configuration > Routing
To configure DNS settings, use: Local Configuration > Hostname & DNS
**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 on the following page:
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 3 of the appendix on page 25.
11. Appliance Configuration for Dispatcher Paragon – Using Layer 4 DR Mode

Configuring 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
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. 10.10.10.191
4. Set the Ports field as needed, depending on your vendor or application:
   - For Konica Minolta, use ports 80,443,5014-5019,5021,5022,50001,50003
   - For HP, use ports 443,5021,5022,5025,7627,57627
   - For other vendors or applications, refer to section 1 of the appendix, Vendor and Application Specific Lists of Ports to Load Balance, on page 19
5. Leave the Protocol set to TCP
6. Leave the Forwarding Method set to Direct Routing
7. Click Update to create the virtual service

8. Click Modify next to the newly created VIP
9. Ensure that the Persistence Enable checkbox is not checked
10. Set the Health Checks Check Port to 5122
11. Click Update
Defining 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. Paragon_SRV_1
3. Set the Real Server IP Address field to the required IP address, e.g. 10.10.10.195
4. Click Update
5. Repeat these steps to add additional print servers as required

```
+-----------------+-----------------+-----------------+
| Label           | Paragon_SRV_1   |
| Real Server IP Address | 10.10.10.195   |
+-----------------+-----------------+-----------------+
```

12. Appliance Configuration for Dispatcher Paragon – Using Layer 7 SNAT Mode

Configuring 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. Dispatcher
3. Set the Virtual Service IP Address field to the required IP address, e.g. 10.10.10.150
4. Set the Ports field as needed, depending on your vendor or application:
   - For Konica Minolta, use ports 80,443,5014-5019,5021,5022,50001,50003
   - For HP, use ports 443,5021,5022,5025,762757627
   - For other vendors or applications, refer to section 1 of the appendix, Vendor and Application Specific Lists of Ports to Load Balance, on page 19
5. Set the Layer 7 Protocol to TCP Mode
6. Click Update to create the virtual service
Defining 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. Paragon_SRV_1
3. Set the Real Server IP Address field to the required IP address, e.g. 10.10.10.151
4. Click Update
5. Repeat these steps to add additional print servers as required

Finalizing the Layer 7 Configuration

To apply the new settings, HAProxy must be reloaded as follows:
1. Using the WebUI, navigate to: Maintenance > Restart Services and click **Reload HAProxy**

13. **Testing & Verification**

The load balanced print service can be tested, either by browsing to the virtual service IP address or the share name. In the example presented in this document, this would be done by going to

\10.10.10.150

or

\Dispatcher

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

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 Paragon environments.
## 17. Appendix

### 1 - Vendor and Application Specific Lists of Ports to Load Balance

The below table includes lists of ports that should be load balanced when working with equipment from different vendors or different applications.

<table>
<thead>
<tr>
<th>Vendor / Application</th>
<th>List of Ports to Load Balance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brother</td>
<td>5026,5027</td>
</tr>
<tr>
<td>Desktop Interface</td>
<td>5558</td>
</tr>
<tr>
<td>Develop</td>
<td>5014-5019,5021,5022</td>
</tr>
<tr>
<td>End User Interface Payment System</td>
<td>8080,8443</td>
</tr>
<tr>
<td>Epson</td>
<td>80,443,5021-5024</td>
</tr>
<tr>
<td>FlexiSpooler server / client (non-)spooling</td>
<td>80,443,515,631,5559,9100</td>
</tr>
<tr>
<td>Fuji Xerox</td>
<td>5011-5013,5021,5022,5029</td>
</tr>
<tr>
<td>HP</td>
<td>443,5021,5022,5025,7627,757627</td>
</tr>
<tr>
<td>Konica Minolta</td>
<td>80,443,5014-5019,5021,5022,50001,50003</td>
</tr>
<tr>
<td>Lexmark</td>
<td>5021,5022</td>
</tr>
<tr>
<td>Mobile Integration Gateway</td>
<td>5559</td>
</tr>
<tr>
<td>Mobile Print Server</td>
<td>5559</td>
</tr>
<tr>
<td>Mobile terminal (Android, iPhone, Windows, generic)</td>
<td>5021,5022</td>
</tr>
<tr>
<td>OKI</td>
<td>389,636,5011,5012</td>
</tr>
<tr>
<td>Olivetti</td>
<td>5014-5019,5021,5022</td>
</tr>
<tr>
<td>Other application LPR printing, e.g. SAP</td>
<td>515</td>
</tr>
<tr>
<td>Ricoh</td>
<td>5011,5012,5021,5022,64098</td>
</tr>
<tr>
<td>SafeQ Client</td>
<td>9100</td>
</tr>
<tr>
<td>Samsung</td>
<td>80,5013</td>
</tr>
<tr>
<td>Sharp</td>
<td>5011,5012,5021,5022</td>
</tr>
<tr>
<td>SPM payment machine</td>
<td>4196-4199</td>
</tr>
<tr>
<td>Terminal Professional (TPv3.5)</td>
<td>4096,5011,5021,5022</td>
</tr>
<tr>
<td>Terminal Professional (TP4)</td>
<td>5021,5022</td>
</tr>
<tr>
<td>Terminal Ultralight</td>
<td>4096</td>
</tr>
<tr>
<td>Toshiba</td>
<td>389,636,5011,5012,5021,5022,49629,49630</td>
</tr>
<tr>
<td>User/LPD Windows Spooler</td>
<td>515</td>
</tr>
<tr>
<td>Xerox</td>
<td>80,161,443,389,636,5011,5012,5021,5022</td>
</tr>
</tbody>
</table>
2 – 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. 10.10.150/255.255.255.255 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. fe80:0:0:0:0:0:a0a:a96/128 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:

   ![Image of Network Connections]

   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

   ![Image of Windows PowerShell]

   Note: Solving the ARP problem for other version of Windows is similar. For full details, please refer to the [administration manual](http://www.loadbalancer.org).
3 – 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

Version 7:

Please refer to Chapter 8 – Appliance Clustering for HA in the v7 Administration Manual.

Version 8:

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>4 May 2020</td>
<td>Initial version</td>
<td></td>
<td>NH, AH</td>
</tr>
<tr>
<td>1.0.1</td>
<td>20 May 2020</td>
<td>Added appendix <em>Vendor and Application Specific Lists of Ports to Load Balance</em>&lt;br&gt;Added references to the new appendix in the configuration instructions</td>
<td>Adds support for a large variety of vendors and applications</td>
<td>NH, AH</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.

United Kingdom
Loadbalancer.org Ltd.
Compass House, North Harbour Business Park, Portsmouth, PO6 4PS UK:+44 (0) 330 380 1064 sales@loadbalancer.org support@loadbalancer.org

Canada
Loadbalancer.org Appliances Ltd.
300-422 Richards Street, Vancouver, BC V6B 2Z4, Canada TEL:+1 302.213.0122 sales@loadbalancer.org support@loadbalancer.org

United States
Loadbalancer.org, Inc.
4550 Linden Hill Road, Suite 201 Wilmington, DE 19808, USA TEL: +1 833.274.2566 sales@loadbalancer.org support@loadbalancer.org

Germany
Loadbalancer.org GmbH Tengstraße 2780798, München, Germany TEL: +49 (0)89 2000 2179 sales@loadbalancer.org support@loadbalancer.org