Load Balancing Konica Minolta Dispatcher Paragon

Version 1.1.0
# Table of Contents

1. About this Guide ................................................................. 3
2. Loadbalancer.org Appliances Supported .................................. 3
3. Loadbalancer.org Software Versions Supported ......................... 3
4. Konica Minolta Dispatcher Paragon Software Versions Supported .... 3
5. Konica Minolta Dispatcher Paragon ........................................ 3
6. Load Balancing Konica Minolta Dispatcher Paragon .................... 3
   Introduction and Overview of Load Balancing Methods .................. 3
   Load Balancing & HA Requirements ...................................... 4
   Overview of Steps Required .............................................. 4
7. Deployment Concept ........................................................ 4
   Virtual Service (VIP) Requirements ..................................... 4
8. Load Balancer Deployment Methods ...................................... 5
   Layer 4 DR Mode .................................................................. 5
   Layer 7 SNAT Mode ........................................................... 6
   Our Recommendation ......................................................... 7
9. Configuring Print Servers for Load Balancing ......................... 7
   Registry Modifications ....................................................... 7
      Microsoft Windows Server 2008 Specific Registry Change .......... 8
   Configuring Name Resolution ............................................. 8
      DNS Name Resolution (Windows 2000 & later) ...................... 8
      NetBIOS Name Resolution (legacy Environments) .................. 9
   Finalising the Server Configuration ...................................... 9
   Installing and Configuring Konica Minolta Dispatcher Paragon ........ 9
10. Loadbalancer.org Appliance – the Basics ............................... 9
    Virtual Appliance .......................................................... 9
    Initial Network Configuration ........................................... 10
    Accessing the WebUI ...................................................... 10
       Main Menu Options .................................................... 11
    HA Clustered Pair Configuration ....................................... 12
11. Appliance Configuration for Dispatcher Paragon – Using Layer 4 DR Mode 12
    Configuring the Virtual Service (VIP) ................................ 12
    Defining the Real Servers (RIPs) ........................................ 13
    Configuring the Virtual Service (VIP) ................................ 13
    Defining the Real Servers (RIPs) ........................................ 14
    Finalizing the Layer 7 Configuration .................................... 14
13. Testing & Verification ........................................................ 15
14. Technical Support ............................................................ 15
15. Further Documentation ...................................................... 15
16. Conclusion ....................................................................... 15
17. Appendix ....................................................................... 16
   Vendor and Application Specific Lists of Ports to Load Balance ........ 16
   Solving the ARP Problem ................................................ 16
      Windows Server 2012, 2016 & 2019 ................................ 16
   Configuring HA - Adding a Secondary Appliance .................... 21
18. Document Revision History ............................................ 24
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 Administration Manual.

2. Loadbalancer.org Appliances Supported

All our products can be used with Konica Minolta Dispatcher Paragon. 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 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 Solving the ARP Problem.

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:

1. Microsoft Windows Server environment.
2. Installation of Dispatcher Paragon.

Overview of Steps Required
Setting up a load balanced Dispatcher Paragon environment can be summarised as follows:

1. Create a virtual service (VIP) on the load balancer that listens on the required ports.
2. Associate the print servers to the virtual service, i.e. define them as 'real servers' (RIPs) for the VIP.
3. Install and configure the Konica Minolta Windows print servers.
4. Configure registry settings on the print servers to enable them to be accessed via a shared name.
5. Configure name resolution related settings on the print servers.
6. 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 Configuring HA - Adding a Secondary Appliance 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 Appliance Configuration for Dispatcher Paragon – Using Layer 4 DR Mode, and for configuring using a combination of layer 4 NAT mode and layer 7 SNAT mode refer to Appliance Configuration for Dispatcher Paragon - Using Layer 7 SNAT Mode.

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 Server’s own IP address and the VIP.

- The Real Servers 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*. For more information please refer to DR Mode Considerations.

- 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 with DR mode, e.g. VIP:80 → RIP:8080 is not supported.
- 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 corresponding request to the chosen Real Server. As a result, Layer 7 is typically not as fast as the Layer 4 methods. 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.

- Layer 7 SNAT mode is a full proxy and therefore load balanced Real Servers do not need to be changed in any way.
- Because layer 7 SNAT mode is a full proxy, any server in the cluster can be on any accessible subnet including across the Internet or WAN.
- Layer 7 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 balancer’s 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 load balancer can be configured to provide the actual client IP address to the Real Servers in 2 ways. Either by inserting a header that contains the client’s source IP address, or by modifying the Source Address field of the IP packets and replacing the IP address of the load balancer with the IP address of the client. For more information on these methods please refer to Transparency at Layer 7.

- Layer 7 SNAT mode can be deployed using either a one-arm or two-arm configuration.
- Port translation is possible with Layer 7 SNAT mode, e.g. VIP:80 → RIP:8080 is supported.
- You should not use the same RIP:PORT combination for layer 7 SNAT mode VIPs and layer 4 SNAT mode VIPs because the required firewall rules conflict.
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 Solving the ARP Problem for more information.

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
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 as shown below:

   ![Advanced TCP/IP Settings](image)

   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.

As shown in the flow chart in this Technet article, for a default H-node client, NetBIOS name resolution occurs in the following order:

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**

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, XEN and Nutanix AHV and has been optimized for each Hypervisor. By default, the VA is allocated 2 vCPUs, 4GB of RAM and has a 20GB 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.
Please refer to The Virtual Appliance - Hypervisor Deployment and the ReadMe.txt text file included in the VA download for more detailed information on deploying the VA using various Hypervisors.

For the VA, 4 NICs are included but only eth0 is connected by default at power up. If the other NICs are required, these should be connected using the network configuration screen within the Hypervisor.

Initial Network Configuration
After boot up, follow the instructions on the console to configure the IP address, subnet mask, default gateway, DNS and other network settings.

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

Accessing the WebUI
The WebUI is accessed using a web browser. By default, user authentication is based on local Apache .htaccess files. User administration tasks such as adding users and changing passwords can be performed using the WebUI menu option: Maintenance > Passwords.

Note
A number of compatibility issues have been found with various versions of Internet Explorer and Edge. The WebUI has been tested and verified using both Chrome & Firefox.

Note
If required, users can also be authenticated against LDAP, LDAPS, Active Directory or Radius. For more information please refer to External Authentication.

1. Using a browser, access the WebUI using the following URL:


2. Log in to the WebUI:

   Username: loadbalancer
   Password: <configured-during-network-setup-wizard>

   Note
   To change the password, use the WebUI menu option: Maintenance > Passwords.

Once logged in, the WebUI will be displayed as shown below:
The WebUI for the VA is shown, the hardware and cloud appliances are very similar. The yellow licensing related message is platform & model dependent.

3. You'll be asked if you want to run the Setup Wizard. If you click Accept the Layer 7 Virtual Service configuration wizard will start. If you want to configure the appliance manually, simple click Dismiss.

**Main Menu Options**

**System Overview** - Displays a graphical summary of all VIPs, RIPs and key appliance statistics

**Local Configuration** - Configure local host settings such as IP address, DNS, system time etc.

**Cluster Configuration** - Configure load balanced services such as VIPs & RIPs

**Maintenance** - Perform maintenance tasks such as service restarts and taking backups

**View Configuration** - Display the saved appliance configuration settings

**Reports** - View various appliance reports & graphs
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 unit is covered in Configuring HA - Adding a Secondary Appliance.

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 Vendor and Application Specific Lists of Ports to Load Balance.

5. Leave the Protocol set to TCP.


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.

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, 7627, 57627.
   - For other vendors or applications, refer to Vendor and Application Specific Lists of Ports to Load Balance.

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

**Note** For additional general guidance please also refer to *Testing Load Balanced Services*.

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

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

The table below 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, 57627</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>

### Solving the ARP Problem

#### Windows Server 2012, 2016 & 2019

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 of 3: 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 of 3: 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. Uncheck all items except **Internet Protocol Version 4 (TCP/IPv4)** and **Internet Protocol Version 6 (TCP/IPv6)** as shown below:
Note | Leaving both checked ensures that both IPv4 and IPv6 are supported. Select one if preferred.

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.

Note For Windows 2012/2016/2019, it’s not necessary to modify the interface metric on the advanced tab and should be left set to Automatic.

Step 3 of 3: Configure the strong/weak host behavior

To configure the correct strong/weak host behavior for Windows 2012/2016/2019, the following commands must be run on each Real Server:

For IPv4 addresses:

```plaintext
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:

```plaintext
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.

• Start PowerShell or use a command window to run the appropriate netsh commands as shown in the example below:

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

Repeat steps 1 - 3 on all remaining Windows 2012/2016/2019 Real Server(s).

For Windows 2012/2016/2019 you can also use the following PowerShell Cmdlets:

The following example configures both IPv4 and IPv6 at the same time:

Set-NetIpInterface -InterfaceAlias loopback -WeakHostReceive enabled -WeakHostSend enabled -DadTransmits 0
Set-NetIpInterface -InterfaceAlias net -WeakHostReceive enabled

To configure just IPv4:

Set-NetIpInterface -InterfaceAlias loopback -WeakHostReceive enabled -WeakHostSend enabled -DadTransmits 0 -AddressFamily IPv4

Set-NetIpInterface -InterfaceAlias net -WeakHostReceive enabled -AddressFamily IPv4

To configure just IPv6:

Set-NetIpInterface -InterfaceAlias loopback -WeakHostReceive enabled -WeakHostSend enabled -DadTransmits 0 -AddressFamily IPv6

Set-NetIpInterface -InterfaceAlias net -WeakHostReceive enabled -AddressFamily IPv6

**Configuring HA - Adding a Secondary Appliance**

Our recommended configuration is to use a clustered HA pair of load balancers to provide a highly available and resilient load balancing solution.

We recommend that the Primary appliance should be configured first, then the Secondary should be added. Once the Primary and Secondary are paired, all load balanced services configured on the Primary are automatically replicated to the Secondary over the network using SSH/SCP.

**Note**

For Enterprise Azure, the HA pair should be configured first. In Azure, when creating a VIP using an HA pair, 2 private IPs must be specified – one for the VIP when it’s active on the Primary and one for the VIP when it’s active on the Secondary. Configuring the HA pair first, enables both IPs to be specified when the VIP is created.

The clustered HA pair uses Heartbeat to determine the state of the other appliance. Should the active device (normally the Primary) suffer a failure, the passive device (normally the Secondary) will take over.

**Note**

A number of settings are not replicated as part of the Primary/Secondary pairing process and therefore must be manually configured on the Secondary appliance. These are listed by WebUI menu option in the table below:

<table>
<thead>
<tr>
<th>WebUI Main Menu Option</th>
<th>Sub Menu Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Configuration</td>
<td>Hostname &amp; DNS</td>
<td>Hostname and DNS settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Network Interface</td>
<td>All network settings including IP address(es), bonding configuration and VLANs</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Routing</td>
<td>Routing configuration including default gateways and static routes</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>System Date &amp; time</td>
<td>All time and date related settings</td>
</tr>
<tr>
<td>WebUI Main Menu Option</td>
<td>Sub Menu Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Physical – Advanced</td>
<td>Various settings including Internet Proxy, Management Gateway, Firewall connection tracking table size, NIC offloading, SMTP relay, logging and Syslog Server</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Security</td>
<td>Appliance security settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>SNMP Configuration</td>
<td>Appliance SNMP settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Graphing</td>
<td>Appliance graphing settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>License Key</td>
<td>Appliance licensing</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Software Updates</td>
<td>Appliance software update management</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Firewall Script</td>
<td>Appliance firewall (iptables) configuration</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Firewall Lockdown Wizard</td>
<td>Appliance management lockdown settings</td>
</tr>
</tbody>
</table>

To add a Secondary node - i.e. create a highly available clustered pair:

1. Deploy a second appliance that will be the Secondary and configure initial network settings.
2. Using the WebUI on the Primary appliance, navigate to: Cluster Configuration > High-Availability Configuration.

![CREATE A CLUSTERED PAIR](image)

3. Specify the IP address and the loadbalancer user’s password for the Secondary (peer) appliance as shown above.
4. Click **Add new node**.
5. The pairing process now commences as shown below:
6. Once complete, the following will be displayed on the Primary appliance:

**High Availability Configuration - primary**

![Configuration Screen]

7. 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 Primary appliance will also automatically restart heartbeat on the Secondary appliance.

**Note**  
For more details on configuring HA with 2 appliances, please refer to Appliance Clustering for HA.
## 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>
<tr>
<td>1.1.0</td>
<td>1 October 2021</td>
<td>Converted the document to AsciiDoc</td>
<td>Move to new documentation system</td>
<td>AH, RJC, ZAC</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.

© Copyright Loadbalancer.org • www.loadbalancer.org