Load Balancing PaperCut

Version 1.1.0
Table of Contents

1. About this Guide ................................................................. 4
2. Loadbalancer.org Appliances Supported .......................... 4
3. Loadbalancer.org Software Versions Supported ............... 4
4. PaperCut NG, MF and Mobility Print Software Versions Supported ................................. 4
5. PaperCut Print Server Components ................................ 4
   Application Server ......................................................... 4
   Secondary Server (Print Provider, Mobility Print) ........... 5
   Site Server .................................................................... 5
6. Load Balancing PaperCut ................................................. 5
   Load Balancing & HA Requirements ................................. 5
   Persistence (aka Server Affinity) ..................................... 6
   Virtual Service (VIP) Requirements ................................. 6
   Load Balanced Ports ...................................................... 6
7. Deployment Concept ......................................................... 6
8. Load Balancer Deployment Methods ............................... 7
   Layer 4 DR Mode ............................................................ 8
   Layer 4 SNAT Mode ....................................................... 8
   Layer 7 SNAT Mode ........................................................ 9
   Our Recommendation ..................................................... 10
9. Configuring Microsoft Print Servers using PaperCut for Load Balancing ......................... 11
   Registry Modifications ..................................................... 11
   Configuring Name Resolution .......................................... 11
   Layer 4 DR Mode – Solving the ARP Problem .................. 11
10. Loadbalancer.org Appliance – the Basics ......................... 11
    Virtual Appliance .......................................................... 11
    Initial Network Configuration .......................................... 11
    Accessing the WebUI ...................................................... 12
    Main Menu Options ....................................................... 13
    HA Clustered Pair Configuration ..................................... 14
11. Appliance Configuration for PaperCut Print Servers – Using Layer 4 DR Mode ........... 14
    Configuring VIP 1 – PaperCut Application Servers ........ 14
    Configuring The Virtual Service (VIP) ............................ 14
    Define the Real (Active Application Server) Server ....... 15
    Configuring VIP 2 – PaperCut Secondary Server (PaperCut Print Provider) ............... 16
    Configuring The Virtual Service (VIP) ............................ 16
    Define the Real (Print Server) Servers ............................ 16
    Configuring VIP 3 – PaperCut Mobility Print ................. 17
    Configuring The Virtual Service (VIP) ............................ 17
    Finalizing the Layer 4 DR mode Configuration ................. 18
    The ARP Problem .......................................................... 18
    Configuring the Print Servers .......................................... 19
12. Appliance Configuration for PaperCut Print Servers – Using Layer 4 SNAT Mode ...... 19
    Configuring VIP 1 – PaperCut Application Servers ........ 19
    Configuring The Virtual Service (VIP) ............................ 19
    Define the Real (Active Application Server) Server ....... 20
    Configuring VIP 2 – PaperCut Secondary Server (PaperCut Print Provider) ............... 20
    Configuring The Virtual Service (VIP) ............................ 20
    Define The Real (Print Server) Servers ........................... 21
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>13. Appliance Configuration for PaperCut Print Servers – Using Layer 7 SNAT Mode</td>
<td>23</td>
</tr>
<tr>
<td>Configuring VIP 3 – PaperCut Mobility Print</td>
<td>22</td>
</tr>
<tr>
<td>Configuring The Virtual Service (VIP)</td>
<td>22</td>
</tr>
<tr>
<td>Configuring the Print Servers</td>
<td>23</td>
</tr>
<tr>
<td>14. PaperCut Microsoft Print Server Configuration</td>
<td>27</td>
</tr>
<tr>
<td>Step 1 - Initial Configuration</td>
<td>27</td>
</tr>
<tr>
<td>Step 2 – Registry Modifications</td>
<td>27</td>
</tr>
<tr>
<td>Step 3 – Configure Name Resolution</td>
<td>28</td>
</tr>
<tr>
<td>Step 4 – Server Reboot</td>
<td>28</td>
</tr>
<tr>
<td>Deploying Printers via Group Policy</td>
<td>28</td>
</tr>
<tr>
<td>15. Testing &amp; Verification</td>
<td>29</td>
</tr>
<tr>
<td>Using System Overview</td>
<td>29</td>
</tr>
<tr>
<td>Client Connection Tests</td>
<td>30</td>
</tr>
<tr>
<td>Testing PaperCut Application Server failover</td>
<td>30</td>
</tr>
<tr>
<td>16. Technical Support</td>
<td>31</td>
</tr>
<tr>
<td>17. Additional Documentation</td>
<td>31</td>
</tr>
<tr>
<td>18. Conclusion</td>
<td>31</td>
</tr>
<tr>
<td>19. Appendix</td>
<td>32</td>
</tr>
<tr>
<td>Configuring HA - Adding a Secondary Appliance</td>
<td>32</td>
</tr>
<tr>
<td>DR Mode Server Configuration</td>
<td>34</td>
</tr>
<tr>
<td>The ARP Problem - Detecting It and Solving It</td>
<td>34</td>
</tr>
<tr>
<td>Detecting the ARP Problem</td>
<td>34</td>
</tr>
<tr>
<td>Solving the ARP Problem for Linux</td>
<td>34</td>
</tr>
<tr>
<td>Solving the ARP Problem for Mac OS X/BSD</td>
<td>37</td>
</tr>
<tr>
<td>Windows Server 2012, 2016 &amp; 2019</td>
<td>37</td>
</tr>
<tr>
<td>Fallback Server Settings</td>
<td>41</td>
</tr>
<tr>
<td>Local Fallback Server</td>
<td>42</td>
</tr>
<tr>
<td>Using a Separate Dedicated Server</td>
<td>42</td>
</tr>
<tr>
<td>Using a Layer 7 VIP</td>
<td>42</td>
</tr>
<tr>
<td>Configuring A real Server as the Fallback Server</td>
<td>43</td>
</tr>
<tr>
<td>Configuring Primary / Secondary Real Servers</td>
<td>43</td>
</tr>
<tr>
<td>Document Revision History</td>
<td>44</td>
</tr>
</tbody>
</table>
1. About this Guide

This guide details the steps required to configure a load balanced PaperCut Application and Secondary print server utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers, Microsoft printer servers and Papercut application 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 for load balancing PaperCut print servers. 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

- V8.4.3 and later

4. Papercut NG, MF and Mobility Print Software Versions Supported

- Papercut NG/MF 20 and later

5. PaperCut

PaperCut is a print management solutions provider which delivers this via three applications:

- **PaperCut NG** for easy print management that lets you hit the ground running with full tracking, visibility. It comes with detailed print job tracking and reporting to truly rein in costly, wasteful printing. Boasting eco-friendly policies to help you use less paper, save on toner, and make sustainable habits the status quo.

- **PaperCut MF** lets you cut costs and waste in your workplace by managing print, scan, copy, and fax. It has powerful exclusive features including Secure Print Release, Integrated Scanning, Scan to Cloud and Job Ticketing.

- **PaperCut Mobility Print** keeps users printing when they’re outside your network, or on an untrusted guest network. It keeps jobs local to keep printing quick, and only uses the Internet when necessary — and cloud jobs compress and encrypt to save space and keep your data safe.

**PaperCut Print Server Components**

**Application Server**

This is the main application, where you can administer reports, printing costs and print quotas, as well as other print-related actions.

**Note**

When deploying an Application server in failover mode it is recommend to move print queues over to the PaperCut secondary servers. It is also recommended to move the Web print, print deploy service on to share storage. For details on PaperCut’s recommended deployment methods for the application servers, see their documentation for Application Server Failover.
Secondary Server (Print Provider, Mobility Print)
This reports to the application server, updating user and print information that the secondary print server has handled.

Note
Mobility Print can be installed on the secondary print servers and can be made highly available when placed behind a load balancer. Mobility Print allows users to print from their mobile devices via network print services and can be load balanced using TCP/UDP 53, 9163, and 9164.

Site Server
The PaperCut Site Server component ensures continuous availability of printing resources to support key business functions over unreliable network links or during unplanned network disruptions, in remote offices. It is ready to take over the role of a Primary Application Server in the event of a WAN outage. Key roles taken over include authentication, copy and print tracking and Find-Me printing, leaving a remote office with the ability to still be able to print.

6. Load Balancing PaperCut

Note
It's highly recommended that you have a working PaperCut version 20 or later environment first before implementing the load balancer, please see the PaperCut Help Center for further details.

Load Balancing & HA Requirements
This guide details the configuration of a load balanced Microsoft print server deployment using the PaperCut application.

For load balancing print servers, 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 covered in DR Mode Server Configuration.

It is also possible to load balance a PaperCut Secondary print server using Layer 4 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. Please note that load balanced connections using layer 4 SNAT mode are not source IP transparent, which is not usually an issue when load balancing print servers but should still be considered.
The PaperCut Application servers can only be deployed in an active-passive configuration when placed behind the load balancer. This is known as a 'failover' configuration and purely provides high availability, not load balancing.

In order to configure the Application servers in an active-passive configuration, the environment must be deployed with:

- A persistent network drive accessible by all servers
- A highly available external database (RDBMS), such as:
  - Microsoft SQL Server
  - PostgreSQL
  - MySQL
  - Oracle

Configuring the external database is beyond the scope of this guide.

**Persistence (aka Server Affinity)**

Neither Microsoft print servers or the PaperCut application require session affinity at the load balancing layer.

**Virtual Service (VIP) Requirements**

To provide load balancing and HA for PaperCut, the following VIPs are required:

- PaperCut Application Servers
- PaperCut Mobility Print
- PaperCut Print Provider

**Load Balanced Ports**

The following table shows the ports that are load balanced:

<table>
<thead>
<tr>
<th>Ports</th>
<th>Use</th>
<th>Transport Layer Protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td>445</td>
<td>Papercut Print Provider</td>
<td>TCP</td>
</tr>
<tr>
<td>53, 9163, 9164</td>
<td>Papercut Mobility Print</td>
<td>TCP/UDP</td>
</tr>
<tr>
<td>9191, 9192, 9193</td>
<td>Papercut Web User Interface</td>
<td>TCP</td>
</tr>
<tr>
<td>9173, 9175</td>
<td>Papercut Print Deploy</td>
<td>TCP</td>
</tr>
</tbody>
</table>

**Note**

A list of additional ports required to configure high availability to work with your required Multifunctional Device vendor can be found on the [PaperCut Help Center](https://www.papercut.com/support/help-center).

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.

8. Load Balancer Deployment Methods

The load balancer can be deployed in 4 fundamental ways:

1. Layer 4 DR mode
2. Layer 4 NAT mode
3. Layer 4 SNAT mode
4. Layer 7 SNAT mode

For Microsoft Print Servers using PaperCut, layer 4 DR mode and layer 4 & 7 SNAT modes are recommended. These modes are described below and are used for the configurations presented in this guide. For configuring using DR mode refer to Appliance Configuration for PaperCut Print Servers – Using Layer 4 DR Mode and for configuring using layer 4 SNAT mode refer to Appliance Configuration for PaperCut Print Servers – Using Layer 4 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 4 SNAT Mode

Layer 4 SNAT mode is a high performance solution, although not as fast as Layer 4 NAT mode or Layer 4 DR mode.
The load balancer translates all requests from the external Virtual Service to the internal Real Servers in the same way as NAT mode - please refer to Layer 4 NAT Mode for more information.

Layer 4 SNAT mode is not transparent, an iptables SNAT rule translates the source IP address to be the load balancer rather than the original client IP address.

Layer 4 SNAT mode can be deployed using either a one-arm or two-arm configuration.

For two-arm deployments, eth0 is normally used for the internal network and eth1 is used for the external network although this is not mandatory. If the Real Servers require Internet access, Autonat should be enabled using the WebUI option: Cluster Configuration > Layer 4 - Advanced Configuration, the external interface should be selected.

Port translation is not possible with Layer 4 SNAT mode, e.g. VIP:80 → RIP:8080 is not supported.

You should not use the same RIP:PORT combination for layer 4 SNAT mode VIPs and layer 7 SNAT mode VIPs because the required firewall rules conflict.

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 → R1P: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 it is not possible to make changes to the real servers, or if the real servers are located in remote routed networks, then layer 4 SNAT mode is recommended.
9. Configuring Microsoft Print Servers using PaperCut for Load Balancing

To configure Microsoft print servers for load balancing the following settings need to be applied:

**Registry Modifications**

For the print servers that are going to be load balanced, to enable them to be accessed via a shared name.

**Configuring Name Resolution**

For printer load balancing to work, DNS name resolution should be configured. A host name and corresponding "Host (A)" record for the virtual service should be created, and should match the virtual IP (VIP) address defined on the load balancer.

**Note** For details of the required changes for registry modifications and configuring name resolution please refer to PaperCut Microsoft Print Server Configuration.

**Layer 4 DR Mode – Solving the ARP Problem**

If using layer 4 DR mode, the 'ARP problem' must be solved on each real server for DR mode to work. For detailed steps on solving the ARP problem, please refer to The ARP Problem - Detecting It and Solving It 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.

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.

**Note** 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.

**Note** 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. Appliance authentication is based on Apache .htaccess files. User admin 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:
Note: 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 PaperCut Print Servers – Using Layer 4 DR Mode

When deploying PaperCut, three virtual services must be configured: a virtual service for the PaperCut Application Server, the Print Provider, and a virtual service for the PaperCut Mobility Print.

Configuring VIP 1 – PaperCut Application Servers

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 required Label (name) for the VIP, e.g. Papercut_WUI.
3. Set the Virtual Service IP address field to the required IP address, e.g. 172.24.11.38.
4. Set the Virtual Service Ports field to 9191,9192,9193.
5. Leave the Protocol set to TCP.
7. Click Update to create the virtual service.

8. Now click Modify next to the newly created Virtual Service.
9. Disable Persistence by unchecking the Enable check box.
10. Under Health Checks set the Check Type to Negotiate.
11. Leave the Check Port field empty.
12. In the Request to send field put the application server health monitoring authorization key which can be found in the HTTP header:

```
/api/health/application-server/status?disk-threshold-mb=1&Authorization=<AUTHORIZATION KEY>
```

The HTTP header can be found in the Application server under Web user interface > Options > Advanced

--

13. Click Update.

**Note**

In some cases other ports may need to be forwarded such as port 9192, 9193 and additional ports depending on a customers multifunctional devices. For a list of PaperCut ports please refer to the PaperCut Help Centre.

### Define the Real (Active Application Server) Server

1. Using the WebUI, navigate to: Cluster Configuration > Layer 4 – Real Servers and click Add a new Real Server next to the newly created VIP.
2. Enter the following details:

   ![Layer 4 Add a new Real Server - Papercut_WUI](Image)

3. Enter an appropriate label for the Real Server, e.g. App_Svr1.
4. Change the Real Server IP Address field to the required address, e.g. 172.24.11.36.
5. Click Update.
6. Repeat the above steps for the remaining application server.

Configuring VIP 2 – PaperCut Secondary Server (PaperCut Print Provider)

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 required Label (name) for the VIP, e.g. Print_Provider.
3. Set the Virtual Service IP address field to the required IP address, e.g. 172.24.11.38.
4. Set the Virtual Service Ports field to 445.
5. Leave the Protocol set to TCP.
7. Click Update to create the virtual service.
8. Now click Modify next to the newly created Virtual Service.
9. Disable Persistence by unchecking the Enable check box.
10. Click Update.

Define the Real (Print Server) Servers
1. Using the WebUI, navigate to: Cluster Configuration > Layer 4 – Real Servers and click Add a new Real Server next to the newly created VIP.
2. Enter the following details:
3. Enter an appropriate label for the Real Server, e.g. **PS1**.
4. Change the **Real Server IP Address** field to the required address, e.g. **172.24.11.39**.
5. Click **Update**.
6. Repeat the above steps to add your other Print Server(s).

**Note**

In the next section, "Configuring VIP 3 – PaperCut Mobility Print" we will make use of the **Duplicate Service** button to retain the configuration including the added real servers. We will then need to amend the configuration with a new label and IP address accordingly, while other configuration items, such as added real servers, will be retained.

---

**Configuring VIP 3 – PaperCut Mobility Print**

**Configuring The Virtual Service (VIP)**

1. Using the web user interface, navigate to **Cluster Configuration > Layer 4 – Virtual Services** and click on **Modify** on the **PrintProviderVIP** virtual service.
2. Click the **Duplicate Service** located in the top right of the menu.
3. Define the required **Label** (name) for the VIP, e.g. **MobilityPrint**.
4. Set the **Virtual Service Ports** field to **53,9163,9164**.
5. Leave the **Protocol** set to **TCP/UDP**.
6. Leave the **Forwarding Method** set to **Direct Routing**.
7. Under the **Health Checks** set the **Check Port** to **9163**.
8. Click **Update**.
Please be aware that Mobility Print will need to be installed on the same Secondary print servers within the cluster. However it is recommended that you segregate these services at a VIP level as this allows for the more granular control and health checking of those services. For example if you create a singular VIP with multiple services being load balanced by that VIP, should one of those services were to fail the VIP and corresponding real server will also be marked as down. Having a singular multi service VIP is fine during testing but not recommended for production.

Finalizing the Layer 4 DR mode Configuration

When using a layer 4 DR mode configuration, all real servers need to be configured to solve the "ARP problem."

The ARP Problem

DR mode works by changing the MAC address of the inbound packets to match the Real Server selected by the load balancing algorithm. To enable DR mode to operate:

- Each Real Server must be configured to accept packets destined for both the VIP address and the Real Server’s IP address (RIP). This is because in DR mode the destination address of load balanced packets is the VIP address, whilst for other traffic such as health checks, administration traffic etc. it’s the Real Server’s own IP address (the RIP). The service/process (e.g. IIS) must also respond to both addresses.

- Each Real Server must be configured so that it does not respond to ARP requests for the VIP address – only
the load balancer should do this.

Configuring the Real Servers in this way is referred to as "Solving the ARP problem". The steps required depend on the OS used as detailed in The ARP Problem - Detecting It and Solving It.

Configuring the Print Servers

Now follow the steps in PaperCut Microsoft Print Server Configuration.

12. Appliance Configuration for PaperCut Print Servers – Using Layer 4 SNAT Mode

When deploying PaperCut, three virtual services must be configured: a virtual service for the PaperCut Application Server, the Print Provider, and a virtual service for the PaperCut Mobility Print.

Configuring VIP 1 – PaperCut Application Servers

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 required Label (name) for the VIP, e.g. Papercut_WUI.

3. Set the Virtual Service IP address field to the required IP address, e.g. 172.24.11.38.

4. Set the Virtual Service Ports field to 9191,9192,9193.

5. Leave the Protocol set to TCP.

6. Leave the Forwarding Method set to SNAT.

7. Click Update to create the virtual service.

8. Now click Modify next to the newly created Virtual Service.

9. Disable Persistence by unchecking the Enable check box.
10. Under Health Checks set the Check Type to **Negotiate**.

11. Leave the Check Port field empty.

12. In the Request to send field, input the application server health monitoring authorization key which can be found in the HTTP header:

   ```
   /api/health/application-server/status?disk-threshold-mb=1&Authorization=<AUTHORIZATION KEY>
   ```

   The HTTP header can be found in the Application server under **Web user interface > Options > Advanced**.

13. Click **Update**.

**Define the Real (Active Application Server) Server**

1. Using the WebUI, navigate to: **Cluster Configuration > Layer 4 – Real Servers** and click **Add a new Real Server** next to the newly created VIP.

2. Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>App_Svr1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>172.24.11.36</td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
<tr>
<td>Minimum Connections</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Connections</td>
<td>0</td>
</tr>
</tbody>
</table>

3. Enter an appropriate **Label** for the Real Server, e.g. **App_Svr1**.

4. Change the **Real Server IP Address** field to the required address, e.g. **172.24.11.36**.

5. Click **Update**.

6. Repeat the above steps for the remaining application server.

**Configuring VIP 2 – PaperCut Secondary Server (PaperCut Print Provider)**

**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 required Label (name) for the VIP, e.g. Print_Provider.

3. Set the Virtual Service IP address field to the required IP address, e.g. 172.24.11.38.

4. Set the Virtual Service Ports field to 445.

5. Leave the Protocol set to TCP.

6. Leave the Forwarding Method set to SNAT.

7. Click Update to create the virtual service.

8. Now click Modify next to the newly created Virtual Service.

9. Disable Persistence by unchecking the Enable check box.

10. Click Update.

---

**Layer 4 - Add a new Virtual Service**

<table>
<thead>
<tr>
<th>Virtual Service</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Label</strong></td>
<td>Print_Provider</td>
<td></td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>172.24.11.38</td>
<td></td>
</tr>
<tr>
<td><strong>Ports</strong></td>
<td>445</td>
<td></td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
<td>TCP</td>
<td></td>
</tr>
<tr>
<td><strong>Forwarding</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Forwarding Method</strong></td>
<td>SNAT</td>
<td></td>
</tr>
</tbody>
</table>

**Define The Real (Print Server) Servers**

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

2. Enter the following details:
3. Enter an appropriate Label for the Real Server, e.g. PS1.

4. Change the Real Server IP Address field to the required address, e.g. 172.24.11.39.

5. Click Update.

6. Repeat the above steps for the remaining application server.

Note

In the next section, "Configuring VIP 3 – PaperCut Mobility Print", we will make use of the Duplicate Service button to retain the configuration including the added real servers. We will then need to amend the configuration with a new label and IP address accordingly, while other configuration items, such as added real servers, will be retained.

Configuring VIP 3 – PaperCut Mobility Print

Configuring The Virtual Service (VIP)

1. Using the web user interface, navigate to Cluster Configuration > Layer 4 – Virtual Services and click on Modify on the PrintProviderVIP virtual service.

2. Click the Duplicate Service located in the top right of the menu.

3. Define the required Label (name) for the VIP, e.g. MobilityPrint.

4. Set the Virtual Service Ports field to 53,9163,9164.

5. Leave the Protocol set to TCP/UDP.

6. Leave the Forwarding Method set to SNAT.

7. Under Health Checks set the Check Port to 9163.

8. Click Update.
Configuring the Print Servers

Now follow the steps in PaperCut Microsoft Print Server Configuration.

13. Appliance Configuration for PaperCut Print Servers – Using Layer 7 SNAT Mode

When deploying PaperCut, three virtual services must be configured: a virtual service for the PaperCut Application Server, the Print Provider, and a virtual service for the PaperCut Mobility Print.

Configuring VIP 1 – PaperCut Application Servers

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 required Label (name) for the VIP, e.g. Papercut_WUI.
3. Set the Virtual Service IP address field to the required IP address, e.g. 172.24.11.38.
4. Set the Virtual Service Ports field to 9191,9192,9193.
5. Set the Protocol to TCP Mode.
6. Click **Update** to create the virtual service.

7. Click **Modify** next to the newly created Virtual Service.

8. Under *Persistence* select **None**.

9. Under *Health Checks* set the *Check Type* to **Negotiate**.

10. Leave the *Check Port* field empty.

11. In the *Request to send* field put the application server health monitoring authorization key which can be found in the HTTP header:

   ```
   /api/health/application-server/status?disk-threshold-mb=1&Authorization=<AUTHORIZATION KEY>
   ```

   The HTTP header can be found in the Application server under *Web user interface > Options > Advanced*.

12. Click **Update**.

**Define the Real (Active Application Server) Server**

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 4 – Real Servers* and click **Add a new Real Server** next to the newly created VIP.

2. Enter the following details:
3. Enter an appropriate Label for the Real Server, e.g. App_Svr1.

4. Change the Real Server IP Address field to the required address, e.g. 172.24.11.36.

5. Click Update.

6. Repeat the above steps for the remaining application server.

Configuring VIP 2 – PaperCut Secondary Server (PaperCut Print Provider)

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 required Label (name) for the VIP, e.g. Print_Provider.

3. Set the Virtual Service IP address field to the required IP address, e.g. 172.24.11.38.

4. Set the Virtual Service Ports field to 445.

5. Set the Protocol to TCP Mode.

6. Click Update to create the virtual service.
7. Now click **Modify** next to the newly created Virtual Service.
8. Under **Persistence** select **None**.
9. Click **Update**.

**Define the Real (Print Server) Servers**

1. Using the WebUI, navigate to: **Cluster Configuration > Layer 7 – Real Servers** and click **Add a new Real Server** next to the newly created VIP.

2. Enter the following details:

   ![Layer 7 Add a new Real Server - Print Provider](image)

   - **Label**: PS1
   - **Real Server IP Address**: 172.24.11.39
   - **Real Server Port**: 
   - **Re-Encrypt to Backend**: 
   - **Weight**: 100

   - **Duplicate Service** button to retain the configuration including the added real servers. We will then need to amend the configuration with a new label and IP address accordingly, while other configuration items, such as added real servers, will be retained.

**Configuring VIP 3 – PaperCut Mobility Print**

**Configuring The Virtual Service (VIP)**

1. Using the web user interface, navigate to **Cluster Configuration > Layer 7 – Virtual Services** and click on **Modify** on the **PrintProviderVIP** virtual service.

2. Click **Duplicate Service**, located in the top right of the menu.

3. Define the required **Label** (name) for the VIP, e.g. **MobilityPrint**.

4. Set the **Virtual Service Ports** field to **53,9163,9164**.

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

6. Under **Health Checks** click **Advanced** and set **Check Port** to **9163**.

7. Click **Update**.
8. Click Reload Haproxy to commit the configuration.

**WARNING:** Label Print_Local already exists. A temporary label of Print_Local-1 has been assigned.

**Layer 7 - Modify Virtual Service**

<table>
<thead>
<tr>
<th>Virtual Service</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual Configuration</td>
<td></td>
</tr>
<tr>
<td>Label</td>
<td>Mobility_Print</td>
</tr>
<tr>
<td>IP Address</td>
<td>172.24.11.38</td>
</tr>
<tr>
<td>Ports</td>
<td>53,8163,9164</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Protocol</th>
<th>[Advanced]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 7 Protocol</td>
<td>TCP Mode</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Connection Distribution Method</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Balance Mode</td>
<td>Weighted Least Connections</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Persistence</th>
<th>[Advanced]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Persistence Mode</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Health Checks</th>
<th>[Advanced]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health Checks</td>
<td>Connect to port</td>
</tr>
<tr>
<td>Check Port</td>
<td>9163</td>
</tr>
</tbody>
</table>

**Configuring the Print Servers**

Now follow the steps in PaperCut Microsoft Print Server Configuration.

14. PaperCut Microsoft Print Server Configuration

**Step 1 - Initial Configuration**

Complete the following steps on each print server:

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 & share the printers (use the same share names and permissions across all servers).

**Step 2 – Registry Modifications**

To enable the print servers to be accessed via a shared name (PapercutPrintService in this guide), add the following registry entries to each print server:
<table>
<thead>
<tr>
<th>Ref.</th>
<th>Registry Key Requirements</th>
</tr>
</thead>
</table>
| 1    | Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa  
Value: DisableLoopbackCheck  
Type: REG_DWORD  
Data: 1 |
| 2    | Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters  
Value: DisableStrictNameChecking  
Type: REG_DWORD  
Data: 1 |
| 3    | Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters  
Value: OptionalNames  
Type: REG_MULTI_SZ  
Data: PapercutPrintService |

**Step 3 – Configure Name Resolution**

To configure DNS name resolution complete the following steps:

1. Disable NetBIOS over TCP/IP on all interfaces of each print server.
2. Create a DNS record for the share name, in this example: PapercutPrintService → 172.24.11.38.

**Step 4 – Server Reboot**

To apply all the changes, reboot each print server.

**Deploying Printers via Group Policy**

- Ensure that the load balanced print server name (e.g. PapercutPrintService) is resolvable by DNS as explained in Step 3 – Configure Name Resolution.
- On your print server, open: Administrative Tools > Printer Management.
  - Right-click Print Servers and enter the name for your load balanced print server (e.g. PapercutPrintService) and click OK.
  - Expand the Printers section.
  - Right click the printer you want to deploy, and click Deploy with Group Policy.
Select the relevant GPO and configure the remaining settings according to your requirements.

Note

PaperCut NG and MF have a fantastic feature called Print Deploy which makes deployment of print queues out to end users workstations super simple. For further details please see the PaperCut Help Center.

15. Testing & Verification

You should now be able to access your printers by browsing using either the Virtual Service IP address, or the share name. In this example:

\172.24.11.38

or

\PapercutPrintService

Using System Overview

The System Overview can be viewed in the WebUI. It shows a graphical view of all VIPs & RIPs (i.e. the PaperCut secondary 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

The Papercut_WUI VIP actively health checks both application servers and will only display the active server in the pool with a green upward arrow. The passive application server will be presented with a red downward arrow until application-server failover occurs on the backend. Servers that a marked with a red arrow will not receive any connections from the load balancer until marked as healthy (green) and online.
Client Connection Tests

Ensure that clients print jobs can succeed via the load balancer to the PaperCut print servers. You’ll probably need to create new DNS records or modify your existing DNS records, replacing the IP addresses of individual servers or the cluster with the IP address of the Virtual Service on the load balancer.

Note
For more details on testing & diagnosing load balanced services please refer to Testing Load Balanced Services.

Testing PaperCut Application Server failover

<table>
<thead>
<tr>
<th>Test</th>
<th>How</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test if the active server is handling traffic.</td>
<td>Attempt to load the PaperCut NG/MF admin web interface using the IP or hostname of the server that you want to test—not the IP/hostname of the NLB. If the server is in the active state, you will see the PaperCut login page.</td>
</tr>
<tr>
<td>Test if the passive server is ready to pick up the load.</td>
<td>Attempt to load the Admin web interface using the IP or hostname of the server that you want to test—not the IP/hostname of the NLB. If the server is in the passive state, you will see a page that looks like this:</td>
</tr>
</tbody>
</table>

High availability activated
Server in passive monitoring mode
<table>
<thead>
<tr>
<th>Test</th>
<th>How</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test if a device is connected via the NLB.</td>
<td>Change the IP/hostname that the device is configured with to be the IP of the Network Load Balancer and restart the device. If the device connects, the NLB is correctly handling the traffic.</td>
</tr>
<tr>
<td>Test if secondary components (user client, secondary server, etc.) are connected to the NLB.</td>
<td>Change the configured IP and restart (same process as above).</td>
</tr>
<tr>
<td>Perform a failover</td>
<td>Trigger a failure on the active Application Server and confirm that traffic is routed to and operation continues automatically on another server in the pool. We recommend performing this multiple times for each server in the pool.</td>
</tr>
</tbody>
</table>

16. 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.

17. Additional Documentation


18. Conclusion

Loadbalancer.org appliances provide a very cost effective solution for a highly available load balanced PaperCut print server environments.
19. Appendix

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 Configuration</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>Local Configuration</td>
<td>Physical – Advanced Configuration</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, navigate to: Cluster Configuration > High-Availability Configuration.

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:
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*.

### DR Mode Server Configuration

When using Layer 4 DR mode the ARP problem must be solved. This involves configuring each Papercut Secondary Print Server to accept traffic destined for the VIP in addition to its own IP address and ensuring that each server does not respond to ARP requests for the VIP address – only the load balancer should do this.

#### The ARP Problem - Detecting It and Solving It

**Detecting the ARP Problem**

Attempt to connect to the VIP and then use *Reports > Layer 4 Current Connections* to check whether the connection state is **SYN_RECV** as shown below.

```
<table>
<thead>
<tr>
<th>PRO</th>
<th>EXPIRE</th>
<th>STATE</th>
<th>SOURCE</th>
<th>VIRTUAL</th>
<th>DESTINATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>00:26</td>
<td>SYN_RECV</td>
<td>192.168.64.7:20415</td>
<td>192.168.111.232:80</td>
<td>192.168.110.240:80</td>
</tr>
<tr>
<td>TCP</td>
<td>00:26</td>
<td>SYN_RECV</td>
<td>192.168.64.7:20414</td>
<td>192.168.111.232:80</td>
<td>192.168.110.240:80</td>
</tr>
<tr>
<td>TCP</td>
<td>04:18</td>
<td>NONE</td>
<td>192.168.64.7:0</td>
<td>192.168.111.232:80</td>
<td>192.168.110.240:80</td>
</tr>
</tbody>
</table>
```

If it is, this is normally a good indication that the ARP problem has not been correctly solved.

**Solving the ARP Problem for Linux**

**Method 1 (using iptables)**

You can use **iptables** (netfilter) on each Real Server to re-direct incoming packets destined for the Virtual Service IP address. To make this permanent, simply add the following command to an appropriate start-up script such as /etc/rc.local on each of your Real Servers. If Real Servers are serving multiple VIPs, add additional iptables rules for each VIP.

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

**e.g.**

```
iptables -t nat -A PREROUTING -d 10.0.0.21 -j REDIRECT
```
Change the IP address to be the same as your Virtual Service.

This means redirect any incoming packets destined for 10.0.0.21 (the Virtual Service) locally, i.e. to the primary address of the incoming interface on the Real Server.

Method 1 may not always be appropriate if you’re using IP-based virtual hosting on your web server. This is because the iptables rule above redirects incoming packets to the primary address of the incoming interface on the web server rather than any of the virtual hosts that are configured. Where this is an issue, use method 2 below instead.

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

Method 2 (using arp_ignore sysctl values)

This is the preferred method as it supports both IPv4 and IPv6. Each Real Server needs the loopback adapter to be configured with the Virtual Services IP address. This address must not respond to ARP requests and the web server also needs to be configured to respond to this address. To set this up follow steps 1-4 below on each Real Server.

Step 1 of 4: re-configure ARP on the Real Servers (this step can be skipped for IPv6 Virtual Services)

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

```bash
net.ipv4.conf.all.arp_ignore=1
net.ipv4.conf.eth0.arp_ignore=1
net.ipv4.conf.eth1.arp_ignore=1
net.ipv4.conf.all.arp_announce=2
net.ipv4.conf.eth0.arp_announce=2
net.ipv4.conf.eth1.arp_announce=2
```

Adjust the commands shown above to suit the network configuration of your servers.

Step 2 of 4: re-configure DAD on the Real Servers (this step can be skipped for IPv4 Virtual Services)

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

```bash
net.ipv6.conf.lo.dad_transmits=0
net.ipv6.conf.lo.accept_dad=0
```

Step 3 of 4: apply these settings

Either reboot the Real Server or run the following command to apply these settings:

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

Step 4 of 4: add the Virtual Services IP address to the loopback adapter

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

© Copyright Loadbalancer.org • Documentation • Load Balancing PaperCut
ip addr add dev lo <IPv4-VIP>/32

for IPv6 addresses use:

ip addr add dev lo <Ipv6-VIP>/128

Note You can check if this command added the VIP successfully using the command:

ip addr ls

You can remove the VIP from the loopback adapter using the command:

ip addr del dev lo <IPv4-VIP>/32

Steps 1, 2 & 3 can be replaced by writing directly to the required files using the following commands (run as root at the command line), this is temporary until the next reboot:

Note

```
echo 1 > /proc/sys/net/ipv4/conf/all/arp_ignore
echo 1 > /proc/sys/net/ipv4/conf/eth0/arp_ignore
echo 1 > /proc/sys/net/ipv4/conf/eth1/arp_ignore
echo 2 > /proc/sys/net/ipv4/conf/all/arp_announce
echo 2 > /proc/sys/net/ipv4/conf/eth0/arp_announce
echo 2 > /proc/sys/net/ipv4/conf/eth1/arp_announce
echo 0 > /proc/sys/net/ipv6/conf/lo/dad_transmits
echo 0 > /proc/sys/net/ipv6/conf/lo/accept_dad
```

Method 3 (using firewalld)

In some newer versions of Linux, iptables is being deprecated in favour of firewalld. The following command can be used on each Real Server to resolve the ARP issue using firewalld:

```
firewall-cmd --permanent --direct --add-rule ipv4 nat PREROUTING 0 -d <VIP> -j REDIRECT
```

e.g.

```
firewall-cmd --permanent --direct --add-rule ipv4 nat PREROUTING 0 -d 10.0.0.50 -j REDIRECT
```

Note Change the IP address to be the same as your Virtual Service.

To apply the new configuration, reload the firewall rules:

```
firewall-cmd --reload
```

The current permanent configuration will become the new firewalld runtime configuration as well as the configuration at the next system start.
Solving the ARP Problem for Mac OS X/BSD

OS X is BSDish, so you need to use BSDish syntax:

```bash
ifconfig lo0 alias <VIP> netmask 255.255.255.255 -arp up
```

You’ll need to add this to the startup scripts on all of your Real Servers.

**Note**

Don’t forget that the service on the Real Servers needs to listen on both the RIP address and VIP address as mentioned previously. Failure to correctly configure the Real Servers to handle the ARP problem is the most common mistake in DR mode configurations.

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**.

   ![Add Hardware](image)

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:

   ![Loopback Properties](image)

   **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:

```
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.

- 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:

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

To configure just IPv4:

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

To configure just IPv6:

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

Fallback Server Settings

The fallback server is activated under the following conditions for both Layer 4 & Layer 7 Virtual Services:

- When all associated Real Servers have failed their health check
- When all associated Real Servers have been taken offline via the WebUI

The fallback page can be provided in the following ways:
- Using the load balancer's built in NGINX fallback page
- Using a separate server to host the fallback page
- Using a Layer 7 VIP

**Local Fallback Server**

The appliance has a built in fallback server that uses NGINX. The local fallback page can be modified using the WebUI menu option: *Maintenance > Fallback Page*

```
<html>
<head>
  <meta charset="UTF-8">
  <title>The page is temporarily unavailable</title>
  <style>
    body { font-family: Tahoma, verdana, arial, sans-serif; }
  </style>
</head>
<body>
  <table width="100%" height="100%">
    <tr>
      <td align="center" valign="middle">
        The page you are looking for is temporarily unavailable.<br/>
        Please try again later.<br/>
        (NGINX port reminder 9081)
      </td>
    </tr>
  </table>
</body>
</html>
```

The local fallback server is an NGINX instance that by default listens on port 9081.

If a layer 4 VIP is added that listens on port 80, NGINX is automatically configured to listen on ports **9081 & 80**.

**Note**

You can use any valid HTML for the default page, simply copy and paste the required HTML into the Fallback Page.

If you are using the load balancer for your holding page and your Real Servers are all offline then the local NGINX server is exposed to hacking attempts. If you are concerned about this you can change the fallback server to be one of your internal servers.

**Using a Separate Dedicated Server**

For DR mode the fallback server must be listening on the same port as the VIP (port re-mapping is not possible with DR mode). Also, don’t forget to solve the ARP problem for the dedicated fallback server.

**Using a Layer 7 VIP**

It's possible to set the fallback server to be a layer 7 VIP. This is especially useful in WAN/DR site environments. It also enables an external fallback server to be easily configured for Layer 4 VIPs without having to comply with the requirements mentioned in the previous section. To do this, create a layer 7 fallback VIP and configure your fallback server as an associated RIP. Then enable the MASQ option for the Layer 4 VIP and set the fallback VIP as its fallback server. If all servers are down, requests will then be routed via the Layer 7 VIP to your fallback server. If the layer 4 VIP is multi-port, specify 0 as the port for the fallback server. Requests will then be forwarded to the correct port.
Configuring A real Server as the Fallback Server
It's possible to configure one of the Real Servers as the fallback server. This can be useful for example when all servers are very busy and health checks start to fail simply because the response is taking longer than the configuration allows. In this case, traffic will still be sent to one of the Real Servers rather than to a separate fallback page.

Configuring Primary / Secondary Real Servers
If you want to setup a VIP that sends all traffic to a primary server and only sends traffic to a secondary server if the primary server fails, configure the VIP with the primary server as a RIP, and the secondary server as the fallback server.
<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>1 June 2020</td>
<td>Initial version</td>
<td></td>
<td>IBG</td>
</tr>
<tr>
<td>1.0.1</td>
<td>15 June 2020</td>
<td>Configuration updates, Papercut hyperlink added</td>
<td>Required content updates</td>
<td>IBG</td>
</tr>
<tr>
<td>1.0.2</td>
<td>19 June 2020</td>
<td>Updated screenshots and hyperlinks</td>
<td>Required content updates</td>
<td>IBG</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added additional ports for the Papercut Web User Interface service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.0.3</td>
<td>26 June 2020</td>
<td>Removed fallback server configuration</td>
<td>Required content updates</td>
<td>IBG</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Replaced system overview image</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added note for papercut_wui vip in testing and verification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.0.4</td>
<td>29 June 2020</td>
<td>Updated Papercut product information</td>
<td>Required content updates</td>
<td>IBG, AH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Document title and filename change</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Differentiating the &quot;Version 19 and earlier&quot; document from the new &quot;Version 20&quot; PaperCut document</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.0.5</td>
<td>10 August 2020</td>
<td>Updated loopback adaptor settings</td>
<td>Incorrect loopback adaptor configuration</td>
<td>IBG</td>
</tr>
<tr>
<td>1.0.6</td>
<td>16 October 2020</td>
<td>Added Layer 7 SNAT configuration</td>
<td>Required for multi-site configuration</td>
<td>IBG</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added Fallback Server configuration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.0</td>
<td>1 January 2022</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