Akative™

RocketFailover®
Say Goodbye to Internet Downtime

DNS
Configuration Guide

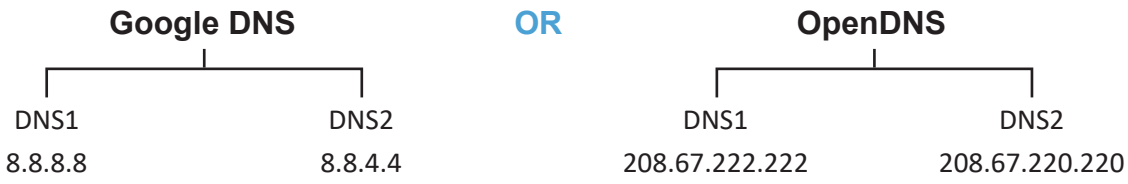
Table of Contents

Introduction

In order to utilize RocketFailover, you need to verify that your network configuration uses DNS servers from a public service such as Google, or OpenDNS. This is important because most ISP's only allow DNS requests from within their network. So your current configuration is likely using DNS servers from your ISP. As you implement RocketFailover you will want to make sure that you switch your DNS servers to either Google or OpenDNS to ensure that DNS requests work no matter which connection is active.

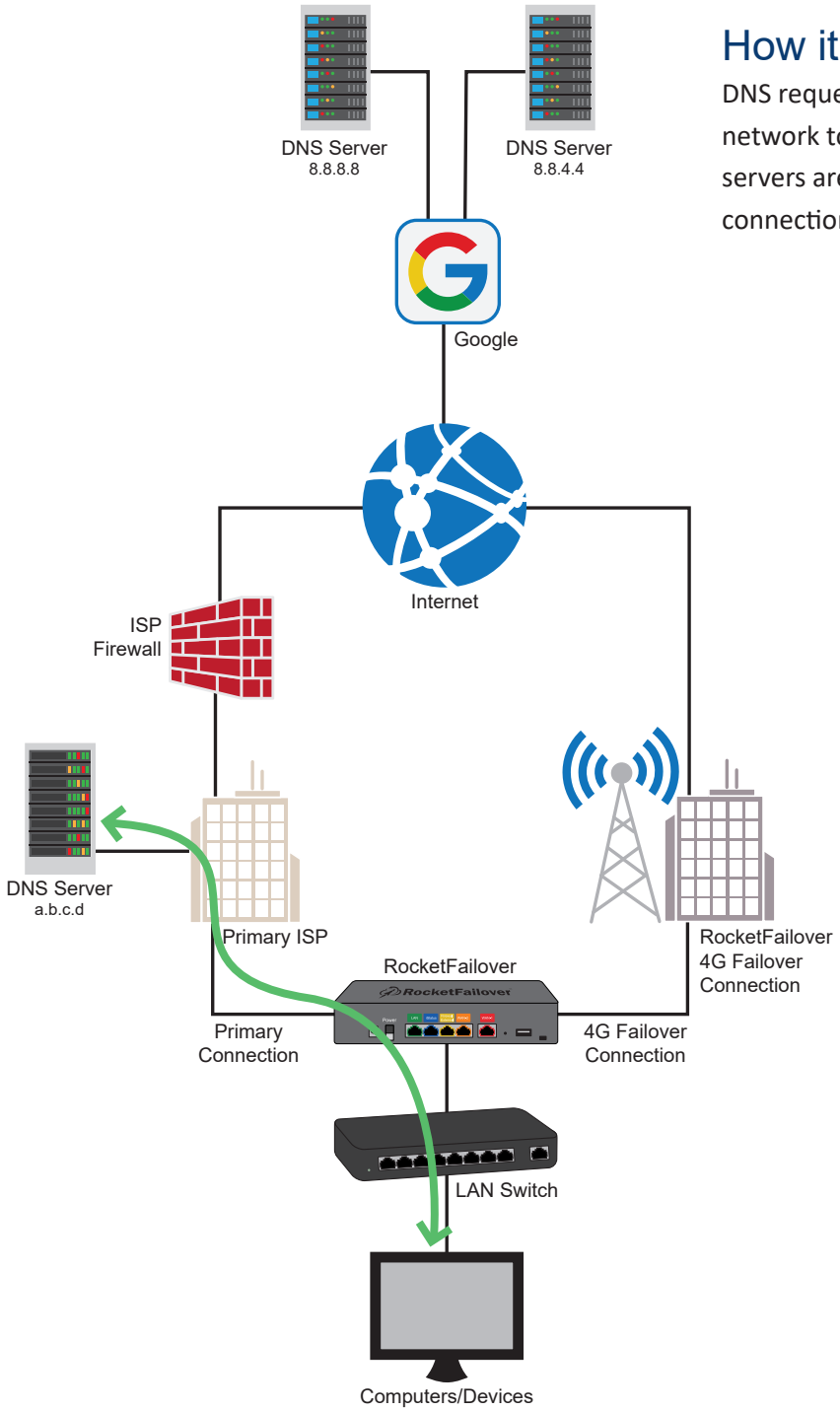
Change your router/firewall to use public DNS servers from either Google or OpenDNS. This process is explained in detail in the following pages.

You may use either Google or OpenDNS for DNS service:



Primary ISP for DNS

DNS Service translates the name of a website into the IP address actually used by your browser. Whenever a user on your network types an address like www.Apple.com, behind the scenes your PC uses the DNS servers that are specified on your network to resolve this name into an IP address.

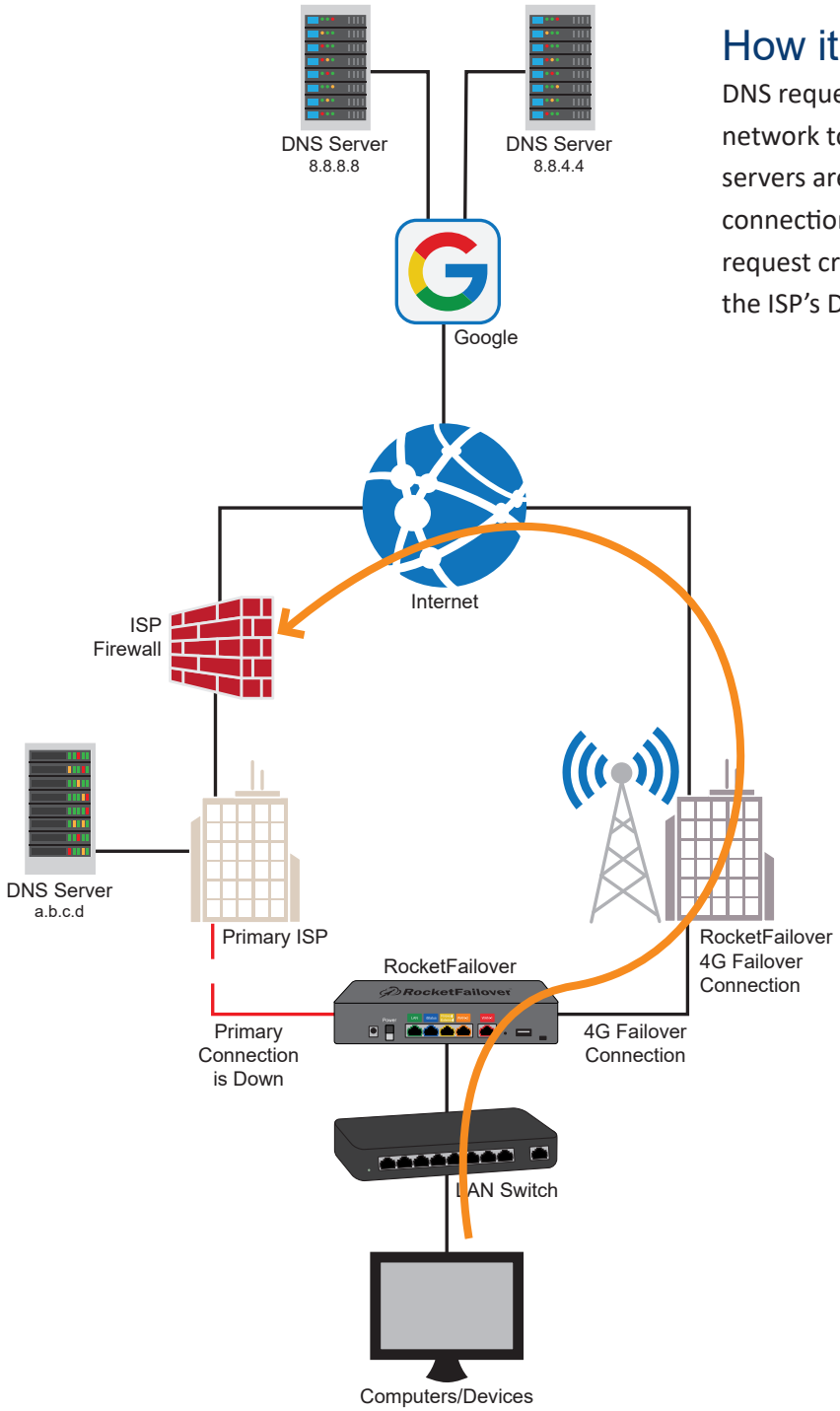


How it Works

DNS requests made from a PC on your network to your primary ISP's DNS servers are allowed when the primary connection is up.

Failover & Primary ISP's DNS

Hackers can abuse ISP's DNS servers, so most ISP's block DNS requests which do not originate from within their network. This means if your PC or network is using your ISP for DNS, that when your connection fails and you failover to RocketFailover, the DNS requests may be blocked because they will be coming to your ISP from outside their network.

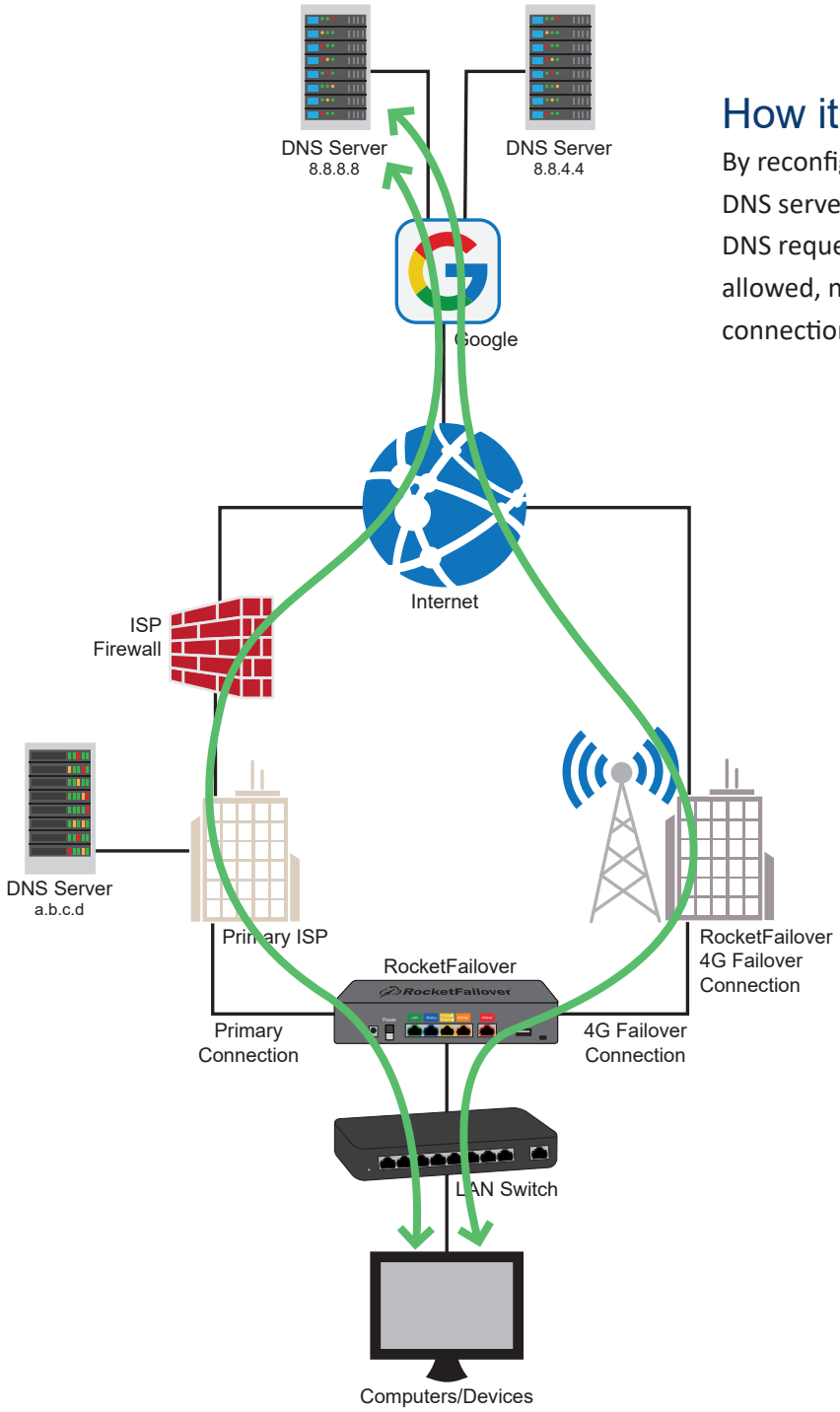


How it Works

DNS requests made from a PC on your network to your primary ISP's DNS servers are blocked when the primary connection is down because the request crosses the Internet to get to the ISP's DNS servers.

Public DNS

The solution to this problem is simple, switch your DHCP server and devices on your network to use Public DNS servers such as the ones listed on page 3.



How it Works

By reconfiguring your network to use DNS servers from Google (or OpenDNS), DNS requests made from a PC are always allowed, no matter which Internet connection is active.

Basic Setup

Have a member of your IT staff check to see if you are already using a public DNS. If you aren't have your IT staff member proceed with the following steps.

1. If you have a firewall on your network which provides DHCP service to PCs on your network. Log into your firewall.
2. Make a note of your current DNS servers.
3. Change your DHCP configuration to specify DNS servers from either Google or OpenDNS.

Google DNS		**OpenDNS**	
DNS1	8.8.8.8	DNS1	208.67.222.222
DNS2	8.8.4.4	DNS2	208.67.220.220

4. Save your configuration.
5. PCs on your network will naturally get updated DNS information as the DHCP leases expire (which may take a day or two), or you can reboot PCs on your network to see that they receive the updated DNS servers immediately.

For specific directions regarding an Operating System or Router listed below, please turn to the designated page.

Mac OS X

1. Go to System Preferences.
2. Click on Network.
3. Select the first connection in your list and click Advanced.
4. Select the DNS tab and add 208.67.222.222 and 208.67.220.220 to the list of DNS servers.
5. Click OK

Windows 7

1. Click the Start Orb, then select Control Panel.
2. Click on Network and Sharing Center.
3. Click on your primary connection or Local Area Connection under Active Networks.
4. Click the Properties button.

   Windows 7 may prompt you for permission to make network setting changes.
5. Highlight 'Internet Protocol Version 4' and click Properties.
6. Click the radio button 'Use the following DNS server addresses:' and type 208.67.222.222 and 208.67.220.220 in the Preferred DNS server and Alternate DNS server fields.
7. Click OK button, then the Close button, then Close again. Finally, close the Network and Sharing Center window.

   At this point, we highly suggest that you flush your DNS resolver cache and web browser caches to ensure that your new configuration settings take effect.

Windows 10

1. Click the Start button.
2. Click the Gear icon OR type Settings and press enter to search. Click on Settings.
3. Click on Network & Internet.
4. Under "Change Your Network Settings," click on "Change Adapter Options."
5. Click on your primary connection or Local Area Connection under Active Networks.
6. Click the Properties button.

   Windows 7 may prompt you for permission to make network setting changes.
7. Highlight 'Internet Protocol Version 4' and click Properties.
8. Click the radio button 'Use the following DNS server addresses:' and type 208.67.222.222 and 208.67.220.220 in the Preferred DNS server and Alternate DNS server fields.
9. Click OK button, then the Close button, then Close again. Finally, close the Network and Sharing Center window.

   At this point, we highly suggest that you flush your DNS resolver cache and web browser caches to ensure that your new configuration settings take effect.

Generic Router

1. Open the preferences for your router.

   Often, the preferences are set in your web browser, via a URL with numbers (example: http://192.168.0.1). You may need a password.

   If you're like us, and you set the router password long ago and cannot remember it now, you can often reset the password to the manufacturer default by pressing a button on the router itself.

   Or preferences may be set via specific application for your router, which you installed on your computer when you added the router.
2. Find the DNS server settings.

   Scan for the letters DNS next to a field which allows two or three sets of numbers, each broken into four groups of one to three numbers.
3. Put in the OpenDNS server addresses, 208.67.222.222 and 208.67.220.220, as your DNS server settings and save/apply.

Linksys Router

1. Visit the router's IP address in a new browser window.

   http://192.168.1.1 is the default Linksys router IP address.
2. Enter the Network password.

   The "Enter Network Password" window will appear. Skip user name and type the router's password (admin is the default password, if you haven't changed it) and click the OK button.
3. Type in OpenDNS addresses, 208.67.222.222, 208.67.220.220, in Static DNS 1 and Static DNS 2 fields.
4. Click Save Settings button.

Netgear Router

1. Type the router's setup URL (http://www.routerlogin.net, http://192.168.0.1 or http://192.168.1.1) into a web browser address bar.

   http://192.168.1.1 is the default Netgear router IP address.
2. Enter the password.
3. Type in OpenDNS addresses, 208.67.222.222 and 208.67.220.220, in Primary DNS and Secondary DNS fields.
4. Click Apply button.
5. Wait for the settings to be updated.

D-Link Router

1. Visit the router's IP address (http://192.168.0.1) in a new browser window.
   If you are attempting to configure a D-Link router, take note of your computer's Default Gateway IP address. The Default Gateway is the IP address of the D-Link router. By default, it should be 192.168.0.1. Most D-Link devices use the 192.168.0.X range.
2. Enter the router password.
   Note: if you have not changed the original settings, the default username is admin and the password is blank (nothing).
3. Click on the Manual Internet Connection Setup button at the bottom.
4. Enter the OpenDNS addresses, 208.67.222.222 and 208.67.220.220, in Primary DNS Server and Secondary DNS Server fields.
5. Click Save Settings button at the top.

Enterprise Deployments with Internal DNS

Your DNS servers can either be configured to use forwarders where DNS requests are forwarded to upstream DNS servers (normally your ISP). If you are using forwarders, and you are using DNS servers which do not respond to public DNS requests, you will want to change your servers to use either Google or OpenDNS public DNS servers. Those servers are listed in numerous places throughout this document. Any competent network administrator who manages your DNS will be able to help you change the currently configured DNS forwarders. If you have questions, please email http://thinix.com/support for additional assistance.

OR

Your DNS servers can be configured to use root-hints where they will resolve DNS requests from root servers. If you are using your own DNS servers with root-hints you will not normally need to make changes to your DNS configuration to implement RocketFailover.

Akative™

Akative Compatible Public DNS Servers

Provider	Primary DNS	Secondary DNS	Content Filtered DNS Primary	Content Filtered DNS Secondary
Google	8.8.8.8	8.8.4.4		
OpenDNS	208.67.222.222	208.67.220.220		
Quad9	9.9.9.9	149.112.112.112		
Cloudflare	1.1.1.1	1.0.0.1		
Verisign	64.6.64.6	64.6.65.6		
Comodo	8.26.56.26	8.20.247.20		
Level3	209.244.0.3	209.244.0.4		
OpenNIC	185.121.177.177	169.239.202.202		
Dyn DNS	216.146.35.35	216.146.36.36		
DNS.Watch	216.146.35.35	216.146.36.36		
OpenDNS Family Shield			208.67.222.123	208.67.220.123
CleanBrowsing.org *(Free **Adult content filter**, blocks adult content but does not block VPN's or mixed-content sites like Reddit)*			185.228.168.10	185.228.169.11
CleanBrowsing.org *(Free **Family content filter**, blocks adult and VPN proxies, also blocks mixed sites such as Reddit)*			185.228.168.168	185.228.169.168
CleanBrowsing.org *(Free **Security content filter**, blocks malware, phishing, spam but doesn't block adult content)*			185.228.168.9	185.228.169.9
SafeDNS			195.46.39.39	195.46.39.40