



OpenDNS Solution Guide for the Cisco Integrated Services Router G2

Introduction to this Guide

As the administrator of an Integrated Services Router (ISR) G2, you are able to connect to the free and fast OpenDNS recursive DNS service which will offer you visibility into all Internet traffic originating from your ISR, and result in a faster Internet experience for your users. If you then want to add an additional layer of DNS security to your ISR, the easy-to-establish connection to OpenDNS enables you to access our free trial – which you can setup (by yourself) in less than five minutes.

Using OpenDNS

OpenDNS is a leading provider of network security and DNS services, enabling the world to connect to the Internet with confidence on any device, anywhere, anytime. The Umbrella cloud-delivered network security service blocks command & control callbacks, malware, and phishing from compromising systems and exfiltrating data over any port, protocol, or app. We apply statistical models to real-time and historical DNS data to predict domains that are likely malicious and could be used in future attacks. OpenDNS protects all devices globally without hardware to install or software to maintain. OpenDNS has data centers across all regions of the world to ensure that the first hop to the service is as fast as possible.

This document covers how to configure the Cisco Integrated Services Router G2 (ISR G2) to use the OpenDNS IP addresses of 208.67.222.222 and 208.67.220.220.

Additionally, if you are using a DNS forwarder as the primary DNS server for your network, this document covers how to update Windows 2003 Server, Windows 2008 Server, Windows 2012 Server or BIND Server to use OpenDNS.

Once you've configured your Cisco infrastructure to point to OpenDNS, then you can sign up for either a free premium DNS account or a free 14-day trial of OpenDNS Umbrella.

Free Premium DNS:

We offer a *free*, fast recursive DNS service which gives you visibility into all of your Internet traffic originating from your ISR device.

https://store.opendns.com/premiumdns/?utm_source=isr&utm_medium=cisco-partner&utm_campaign=isr-guide-free-trial-home

Free OpenDNS Umbrella 14-Day Trial at:

If you want to add an additional layer of DNS security to your ISR device, try our free trial – which you can set up by yourself in less than five minutes.

https://signup.opendns.com/freetrial/?utm_source=isr&utm_medium=cisco-partner&utm_campaign=isr-guide-free-trial#company

Setting up OpenDNS for a Cisco network

Traditionally there are several places where a network administrator might change public recursive DNS settings to use OpenDNS, but exactly where the change is made depends on the network configuration.

Note: If you're not certain whether you have a DNS forwarder on your ISR G2 or DNS server, the best way to determine what needs to be changed is to see what device is being used as the DNS server for client workstations that are receiving DHCP from the network. This information is typically in the DNS section of the network adapter settings on the client workstation.

In smaller networks, such a home or guest network, there are no internal resources that require a DNS server be configured for the network. In that case, changing the DNS Server settings on the gateway appliance (an ISR G2 in this case) from another DNS server to OpenDNS is all that is required. The OpenDNS IPs may be distributed via DHCP to the endpoint clients to use to resolve web addresses directly, or the gateway router or access point can act as a forwarder and the IP of the router is then the DNS server address for the clients. In a network like this, the instructions for *How to configure DNS servers for the Integrated Services Router G2 DHCP server* are applicable.

Most mid-to-large size networks use a DNS forwarder on a DNS server. Typically this is a server running Windows Server with DNS services installed, or a server running BIND. The DNS server resolves requests to internal resources, such as file shares or printers. The DNS forwarder forwards any requests for zones not hosted on the DNS server to OpenDNS. OpenDNS resolves the domain to an IP and returns that information to the DNS forwarder.

Instructions to update your DNS forwarder to use OpenDNS for Windows Server 2003, 2008, 2012 and BIND can be found in the *Configuring your DNS Forwarder for OpenDNS* section of this document.

How to configure DNS client services on the Integrated Services Router G2

Example Configuration

```
hostname(config)# ip name-server 208.67.222.222 208.67.220.220  
  
hostname(config)# ip domain lookup
```

Note: If the ISR G2 needs to resolve internal DNS then it must use internal DNS servers. In this scenario the internal DNS servers are configured to use OpenDNS as their DNS forwarders.

For more information on DNS configuration, see: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dns/configuration/15-mt/dns-15-mt-book/dns-config-dns.html#GUID-5C6DC8F0-15ED-45DB-8D16-88E0198A01E4

How to configure DNS servers for the Integrated Services Router G2 DHCP server

Example Configuration

```
hostname(config)# ip dhcp pool <pool_number>  
  
hostname(dhcp-config)# dns server 208.67.222.222 208.67.220.220
```

For more information on DHCP configuration, see: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/12-4t/dhcp-12-4t-book/config-dhcp-server.html

Configuring your DNS forwarder for OpenDNS

Even with a Cisco device in place at the gateway or egress, DNS for networks is often handled by DNS forwarders installed on DNS servers within the network environment. A DNS forwarder is a DNS server on a network that forwards DNS queries for external domain names to the OpenDNS servers. A DNS server on a network is designated as a forwarder when the other DNS servers in the network are configured to forward the queries that they cannot resolve locally to that DNS server.

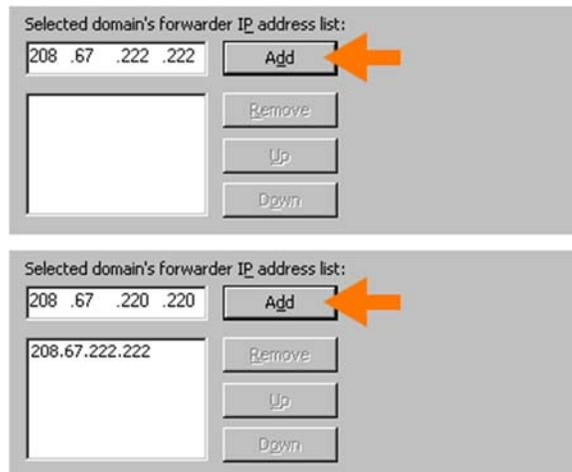
The following instructions cover how to configure your DNS forwarder to use the OpenDNS public DNS servers for BIND and Windows Server 2003, 2008 and 2012.

Windows Server 2003 and 2003 R2

1. From the Start menu, navigate to **Administrative Tools > DNS**.
2. Choose the DNS server you want to edit.
3. Select **Forwarders**.
4. Select **All Other DNS domains** in the DNS domain list
5. Add OpenDNS addresses to the selected server's forwarder IP address list.

Please write down your current DNS settings before switching to OpenDNS, in case you want to return to your old settings for any reason.

OpenDNS' addresses are 208.67.222.222 and 208.67.220.220.



6. Click **OK** to confirm the changes.

We recommend that you flush the DNS resolver cache of the server and the DNS caches of the clients/users using the DNS server to ensure that your new DNS configuration settings take immediate effect.

For more information, read here: <https://support.opendns.com/entries/26336865>

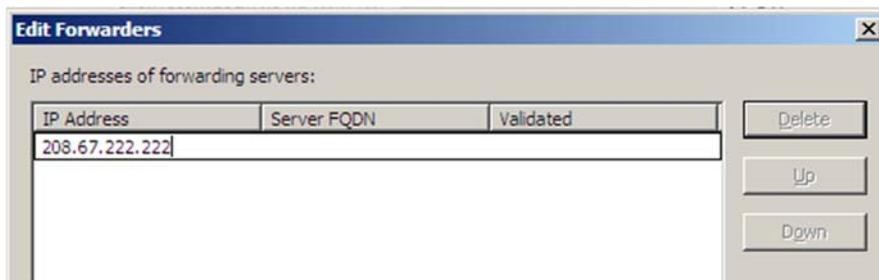
Windows Server 2008 and 2008 R2

1. From the Start menu, navigate to **Administrative Tools > DNS**.
2. Choose the DNS server you want to edit.

3. Select **Forwarders**.
4. Click **Edit**.
5. Add OpenDNS addresses in the selected server's forwarder IP address list.

Please write down your current DNS settings before switching to OpenDNS, in case you want to return to your old settings for any reason.

OpenDNS' addresses are 208.67.222.222 and 208.67.220.220.



6. Click **OK**.
7. Click **OK** again to confirm the changes.

We recommend that you flush the DNS resolver cache of the server and the DNS caches of the clients/users using the DNS server to ensure that your new DNS configuration settings take immediate effect.

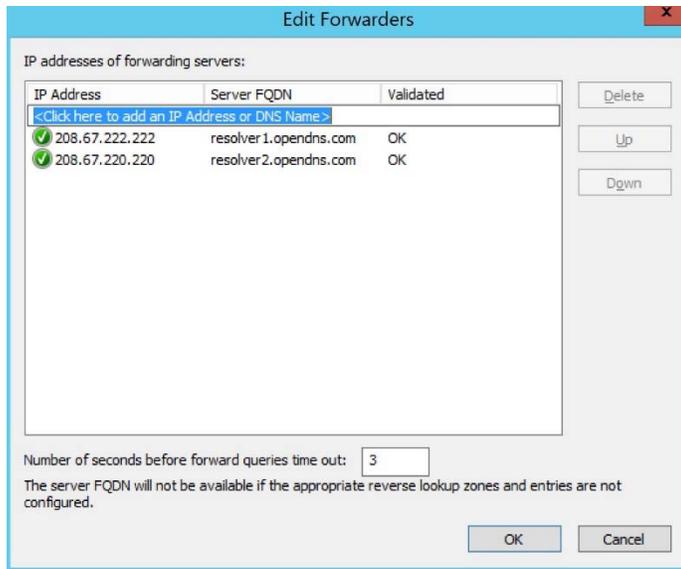
For more information, see: <https://support.opendns.com/entries/26336865>

Windows Server 2012 and 2012 R2

1. In the Start menu, type **DNS** into Search.
2. Select **DNS** from the search results.
3. Choose the DNS server you want to edit.
4. Select **Forwarders**.
5. Click **Edit**.
6. Add OpenDNS addresses in the selected server's forwarder IP address list.

Please write down your current DNS settings before switching to OpenDNS, in case you want to return to your old settings for any reason.

OpenDNS' addresses are 208.67.222.222 and 208.67.220.220.



7. Click **OK**.
8. Click **OK** again to confirm the changes.

BIND based DNS server: Configure BIND to use Open DNS via the shell and Webmin

To point your BIND-based DNS server to use OpenDNS resolvers for external resolution you need to modify the file **named.conf.options** and add the OpenDNS resolvers as forwarders.

This can be done in one of two ways:

- Via the command line, Shell\SSH
- Via a GUI if you have Webmin installed on your BIND server

Shell\SSH Instructions

1. Connect directly to your server or SSH to it.
2. Go into **/etc/bind/**

Note: this is the default location, so you may need to change this based on your configuration.
3. Edit **named.conf.options** in your favorite text editor.
4. Click **Edit**.
5. In **named.conf.options**, look for a line that starts with **forwarders {**

If the forwarders are already configured then just change the current resolver IPs to OpenDNS' IP addresses, which are 208.67.222.222 and 208.67.220.220.

If the line starting with **forwarders** { isn't there, you can add it right above the last } ;

```
forwarders {  
    208.67.222.222;  
    208.67.220.220;  
};
```

6. Save the file to confirm your changes.

Webmin Instructions

These steps produce a result that is the exact same as the above, except that the Webmin GUI will modify the file **named.conf.options** for you.

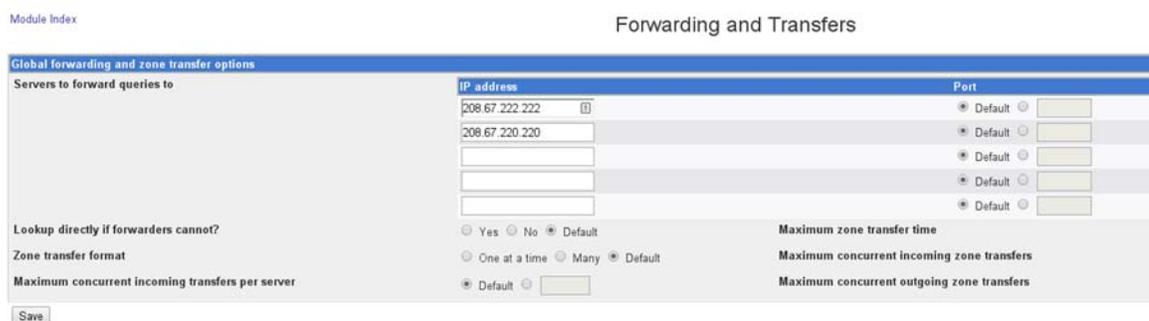
1. Log into Webmin.
2. Navigate to **Servers > BIND DNS Server**.



3. Choose **Forwarding and Transfers**.



4. Add OpenDNS' IP addresses, which are 208.67.222.222 and 208.67.220.220, under the Servers to forward queries to section:



5. Click **Save** to confirm the changes.

Open DNS Service and Support

OpenDNS customers should continue to use the existing process for configuration and support on OpenDNS technology. Cisco will notify you in advance of any change to the support process.

OpenDNS support: <https://www.opendns.com/support/>

Legal Information

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Cisco Copyright

© 2014 Cisco Systems, Inc. All rights reserved.