

MACROTICK.COM

Web filter using public DNS

MUM US - April, 2016

Jovan Strika, Macrotick



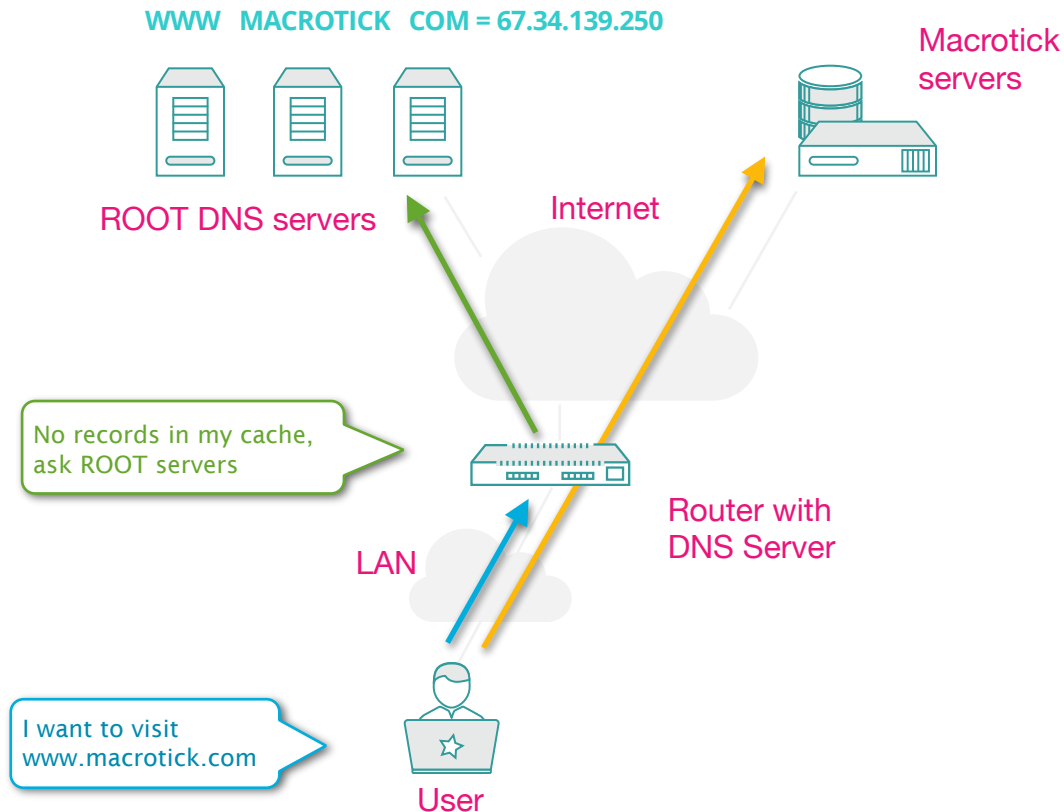
Networking equipment and management services based on
MikroTik router boards



Unique approach to network monitoring and management using MikroTik scripting capabilities

Web filter using public DNS service

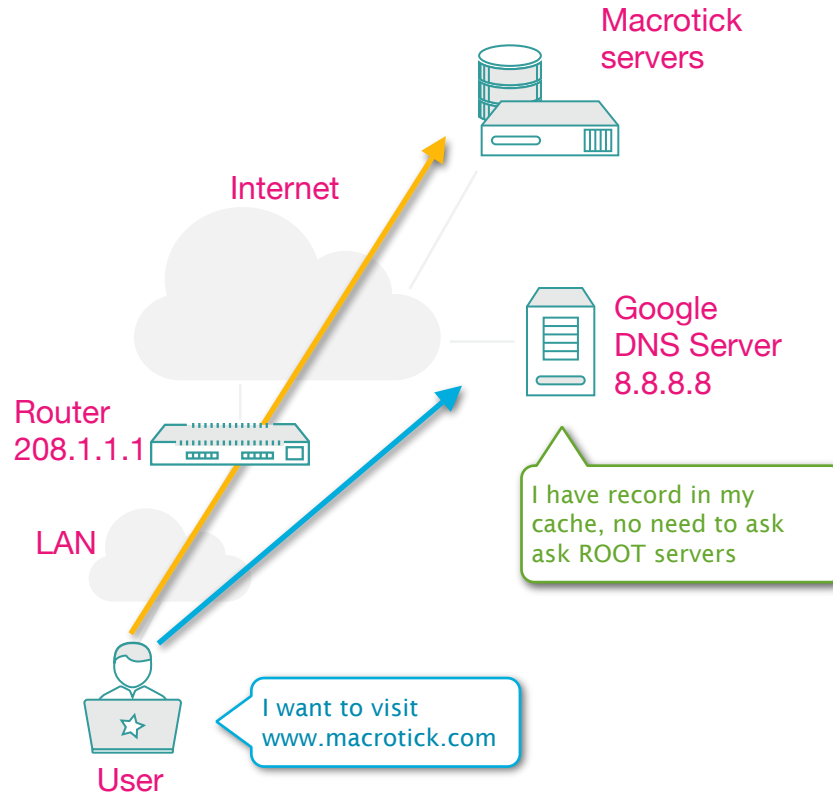
- Why we need DNS and how it works
- Anycast and DNS
- OpenDNS and Classification of the Internet
- Configuring Mikrotik to use OpenDNS
- Advantages and disadvantage



What can be your DNS server?

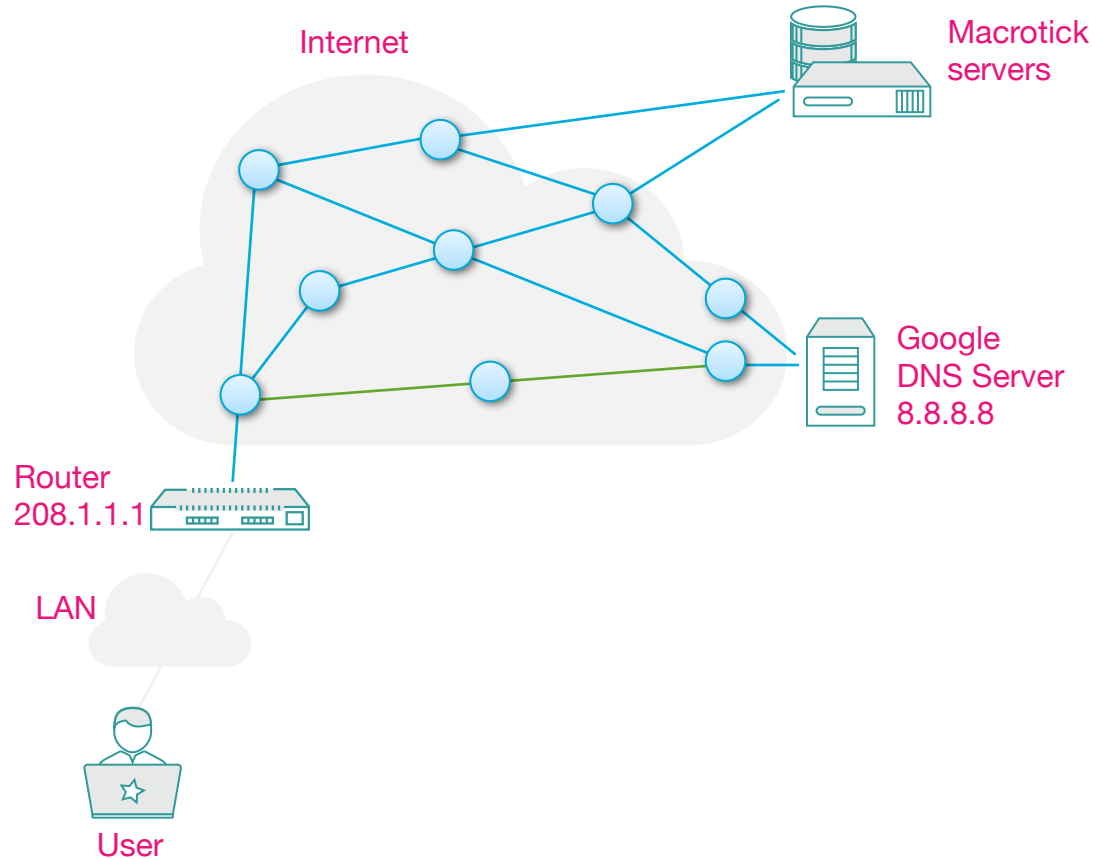
- Your Router
- Your Server
- Your ISP
- Or another DNS Provider

Using Public DNS Providers



- DNS server not installed on the Router
- Router is just forwarding DNS request
- Public DNS server will respond to your request

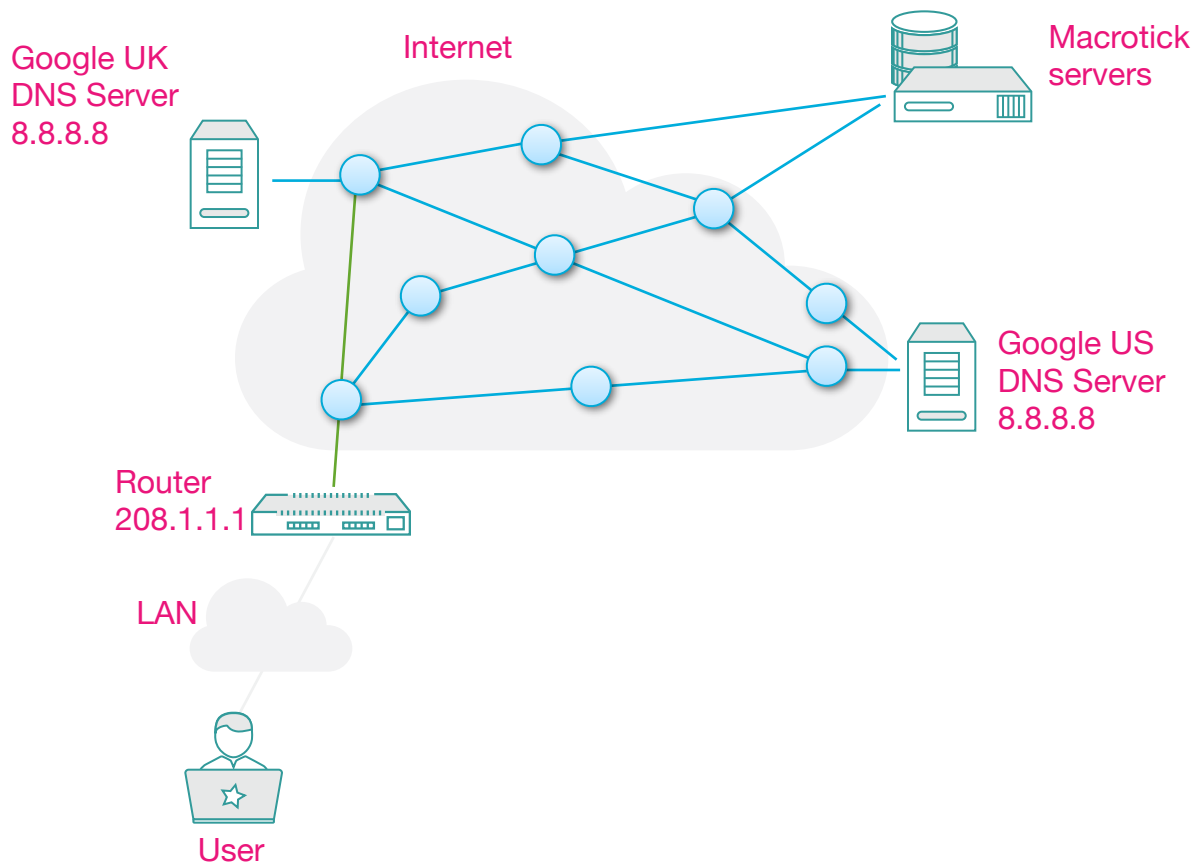
Simplified BGP and Unicast Routing



Routing the Internet

- Routers are using BGP protocol to exchange routing information
- They will use the closes path to get to destination
- More than one path will ensure redundancy

AnyCast routing



Routing the Internet

- When using Anycast, DNS request will always connect to the 'closest' (from a routing protocol perspective) DNS server.
- This reduces latency, and provides a level of load-balancing



Why AnyCast

- Same IP anywhere
- Makes DNS more reliable - 100% uptime
- Improves DNS performance
- Provides resilience against DDoS attacks
- Easy to scale- just add another orange dot

OpenDNS
Community

Submit and tag domains

Your domains

mail.yahoo.com
mail.google.com
gmail.com
hotmail.com

Add a tag and submit

-- Select a tag --

Submit

One domain per line, 100 max.

Verify other users' tags

Domain	Tag	Is this an appropriate tag?
mail.yahoo.com	Webmail added by aaron	<input type="button" value="YES"/> <input type="button" value="NO"/> <input type="button" value="NOT SURE"/>
mail.google.com	Webmail added by aaron	<input type="button" value="YES"/> <input type="button" value="NO"/> <input type="button" value="NOT SURE"/>
gmail.com	Webmail added by aaron	<input type="button" value="YES"/> <input type="button" value="NO"/> <input type="button" value="NOT SURE"/>
hotmail.com	Webmail added by aaron	<input type="button" value="YES"/> <input type="button" value="NO"/> <input type="button" value="NOT SURE"/>

Next level of DNS service with OpenDNS

- Each DNS request is mapped to domain
- Most of domains are classified by category
- Anyone can submit domain and suggest category
- Community will vote if they agree

Web Content Filtering

Choose your filtering level

- ☐ **High** Protects against all adult-related sites, illegal activity, social networking sites, video sharing sites, and general time-wasters. [26 categories in this group - View - Customize](#)
- ☐ **Moderate** Protects against all adult-related sites and illegal activity. [13 categories in this group - View - Customize](#)
- ☐ **Low** Protects against pornography. [4 categories in this group - View - Customize](#)
- ☐ **None** Nothing blocked.
- ☒ **Custom** Choose the categories you want to block.

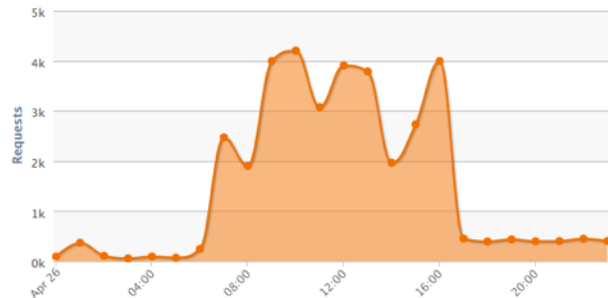
- | | | |
|---|---|---|
| <input checked="" type="checkbox"/> Academic Fraud | <input checked="" type="checkbox"/> Adult Themes | <input checked="" type="checkbox"/> Adware |
| <input checked="" type="checkbox"/> Alcohol | <input type="checkbox"/> Anime/Manga/Webcomic | <input type="checkbox"/> Auctions |
| <input type="checkbox"/> Automotive | <input type="checkbox"/> Blogs | <input type="checkbox"/> Business Services |
| <input checked="" type="checkbox"/> Chat | <input checked="" type="checkbox"/> Classifieds | <input checked="" type="checkbox"/> Dating |
| <input checked="" type="checkbox"/> Drugs | <input type="checkbox"/> Ecommerce/Shopping | <input type="checkbox"/> Educational Institutions |
| <input type="checkbox"/> File Storage | <input type="checkbox"/> Financial Institutions | <input type="checkbox"/> Forums/Message boards |
| <input checked="" type="checkbox"/> Gambling | <input type="checkbox"/> Games | <input checked="" type="checkbox"/> German Youth Protection |
| <input type="checkbox"/> Government | <input checked="" type="checkbox"/> Hate/Discrimination | <input type="checkbox"/> Health and Fitness |
| <input type="checkbox"/> Humor | <input checked="" type="checkbox"/> Instant Messaging | <input type="checkbox"/> Jobs/Employment |
| <input checked="" type="checkbox"/> Lingerie/Bikini | <input checked="" type="checkbox"/> Movies | <input type="checkbox"/> Music |
| <input type="checkbox"/> News/Media | <input type="checkbox"/> Non-Profits | <input checked="" type="checkbox"/> Nudity |
| <input checked="" type="checkbox"/> P2P/File sharing | <input type="checkbox"/> Parked Domains | <input checked="" type="checkbox"/> Photo Sharing |
| <input type="checkbox"/> Podcasts | <input type="checkbox"/> Politics | <input checked="" type="checkbox"/> Pornography |
| <input type="checkbox"/> Portals | <input checked="" type="checkbox"/> Proxy/Anonymizer | <input type="checkbox"/> Radio |
| <input type="checkbox"/> Religious | <input type="checkbox"/> Research/Reference | <input type="checkbox"/> Search Engines |
| <input checked="" type="checkbox"/> Sexuality | <input checked="" type="checkbox"/> Social Networking | <input type="checkbox"/> Software/Technology |
| <input checked="" type="checkbox"/> Sports | <input checked="" type="checkbox"/> Tasteless | <input checked="" type="checkbox"/> Television |
| <input type="checkbox"/> Tobacco | <input type="checkbox"/> Travel | <input checked="" type="checkbox"/> Video Sharing |
| <input type="checkbox"/> Visual Search Engines | <input type="checkbox"/> Weapons | <input checked="" type="checkbox"/> Web Spam |
| <input type="checkbox"/> Webmail | | |

Looking for [security categories?](#)

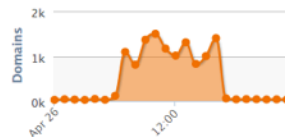
OpenDNS Features

- Chose categories that you want to block based on your public IP address
- Add custom domains to white/black list
- Get statistics of your DNS queries

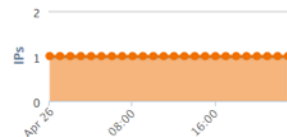
Recent Activity (all your networks, last day)



Unique Domains



Unique IPs



Request Types

Type	Requests
A	26860
NS	5
SOA	2
PTR	5
AAAA	9132
ANY	7

Domains

Domain	Requests
*,amazonaws.com	1658
*,l.google.com	1639
*,mcafee.com	1393
*,akamaiedge.net	1378
*,akamai.net	1322
ads.pubmatic.com	1160

How to use OpenDNS with Mikrotik router

Mikrotik with DNS server

- Enable local DNS server on Mikrotik and use OpenDNS servers to forward request if not found in local cache
- Setup DHCP server to provide router LAN IP address as DNS server
- Add NAT firewall rule to redirect traffic to local port 53

```
/ip dns set allow-remote-requests=yes  
servers=208.67.222.222,208.67.220.220  
  
/ip firewall nat  
add action=redirect chain=dstnat dst-address-type=!local dst-  
port=53 protocol=udp to-addresses=0.0.0.0 to-ports=53  
  
/ip dhcp-server network add address=192.168.88.0/24  
gateway=192.168.88.1 dns-server=192.168.88.1
```

Mikrotik without DNS server

- Disable DNS server on Mikrotik
- Setup DHCP server to OpenDNS servers as DNS servers
- Workstations will send DNS requests directly to OpenDNS servers
- Add NAT firewall rule to redirect traffic to OpenDNS server port 53

```
/ip dns set allow-remote-requests=no  
  
/ip firewall nat  
add action=redirect chain=dstnat dst-address-type=!local dst-  
port=53 protocol=udp to-addresses=208.67.222.222 to-ports=53  
  
/ip dhcp-server network add address=192.168.88.0/24  
gateway=192.168.88.1 dns-  
server=208.67.222.222,208.67.220.220
```

How to Handle Dynamic IP address



Using Updater Clients from OpenDNS

- Install OpenDNS updater software on Windows or MAC
- Updater will recognize when IP addresses are changed and it will update your OpenDNS network settings.

Dynamic IP: Updater Clients

[General Info](#) [Updater Clients](#) [Technical Details](#)

Download the OpenDNS Updater

Platform	Name	Notes
 Windows	OpenDNS Updater	The official OpenDNS Windows client. Documentation available
 Mac	OpenDNS Updater	The official OpenDNS Mac client.

Using Mikrotik script

- Script developed by Alexander Harrison who works for OpenDNS
- Using HTTP to send update to OpenDNS API
- 2 versions of the script available:
 - Always send update
 - Only send updates when a new IP is detected

<https://support.opendns.com/entries/69688114-Mikrotik-WinBox-Dynamic-Update-Script>

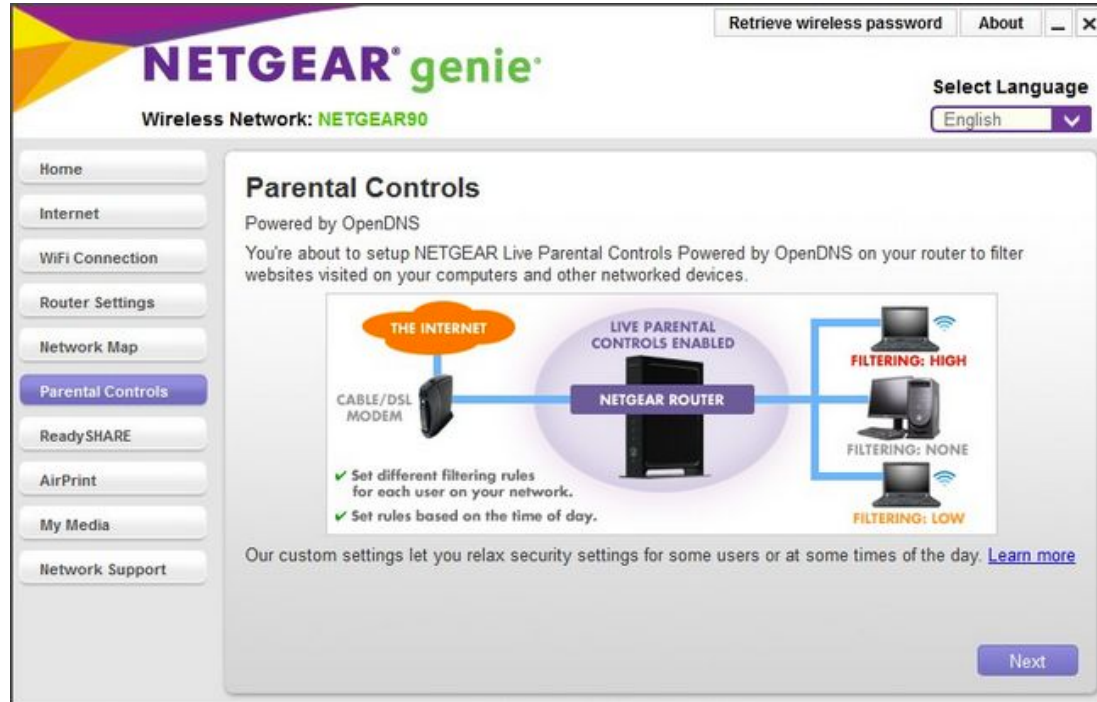
How to use OpenDNS with Mikrotik router

Advantages

- Web filter - of course
- Simple to use
- Cloud based, no local hardware/software to install
- Your data analytics and statistics
- Added security - recognize and prevent before an attack
- More reliable and redundant DNS

Limitations

- You must get a Public IP from your ISP
- Content may be sent through proxy (originally they were adding ads)
- One filter for all users - no custom filter rules per internal IP or user (unless they use VPN per device)
- No scheduling (block specific categories during work hours)



OpenDNS Integration

- Integrated in Netgear router
- Parental Controls
- Rules per user
- Rules based on time of day
- What next

THANK YOU !

Questions?