MACROTICK.COM

Web filter using public DNS

MUM US - April, 2016

Jovan Strika, Macrotick

Enterprise Grade Routers

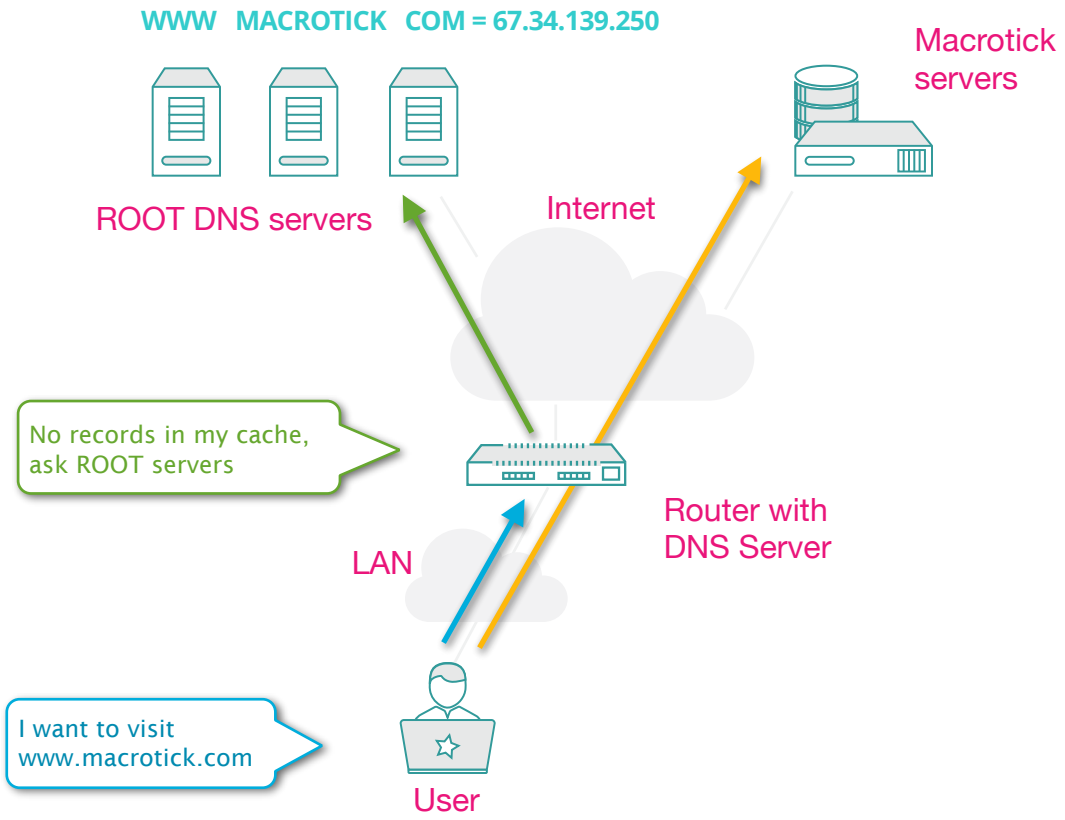
Networking equipment and management services based on MikroTik router boards

Cloud Services

Unique approach to network monitoring and management using MikroTik scripting capabilities

Web filter using public DNS service

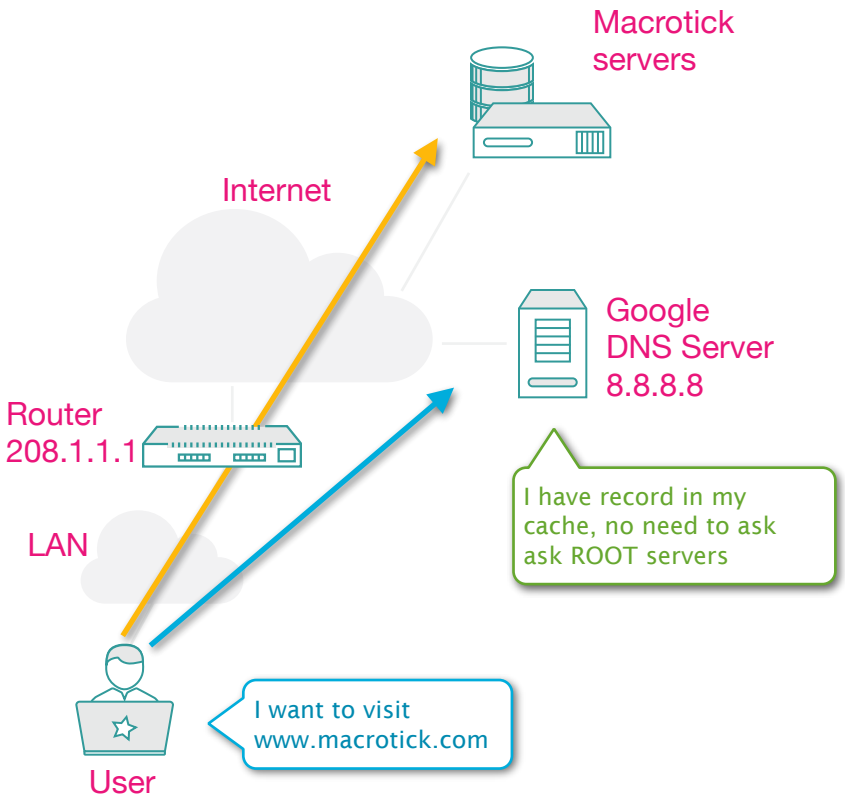
- Why we need DNS and how it works
- Anycast and DNS
- OpenDNS and Classification of the Internet
- Configuring Mikrotik to use OpenDNS
- Advantages and disadvantage



What can be your DNS server?

- **Your Router**
- **Your Server**
- **Your ISP**

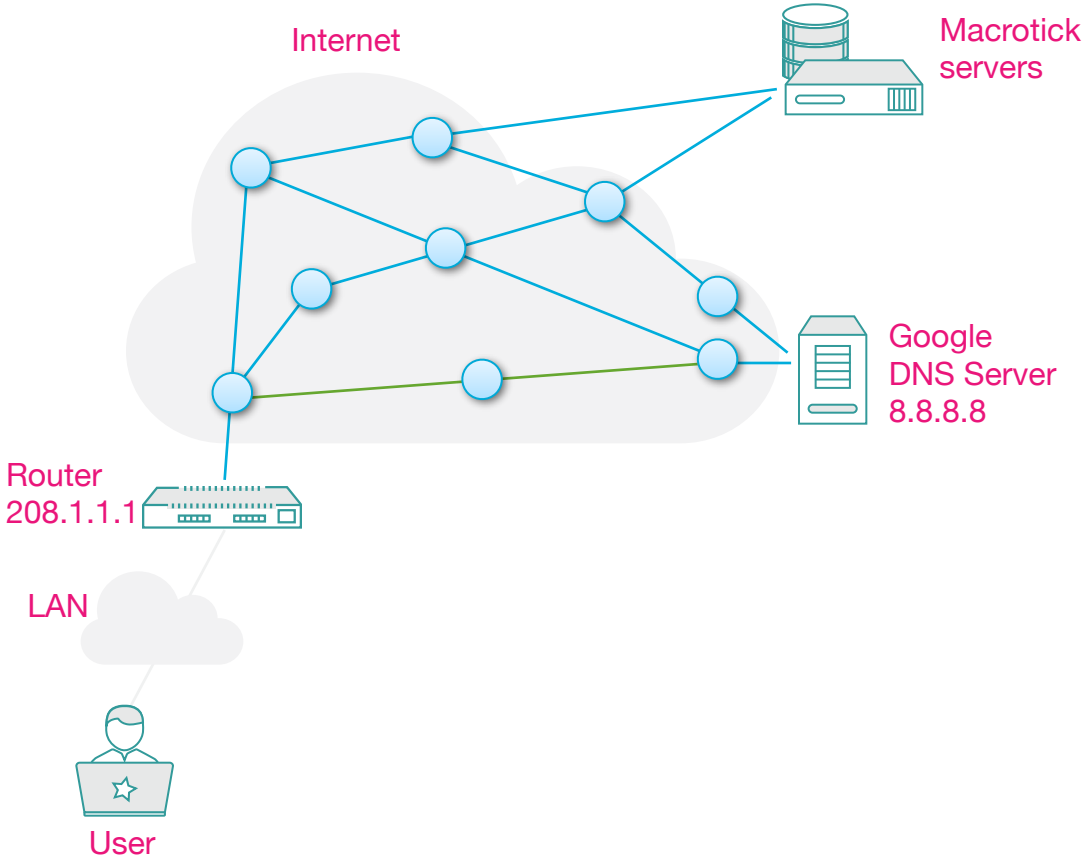
- **Or another DNS Provider**



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

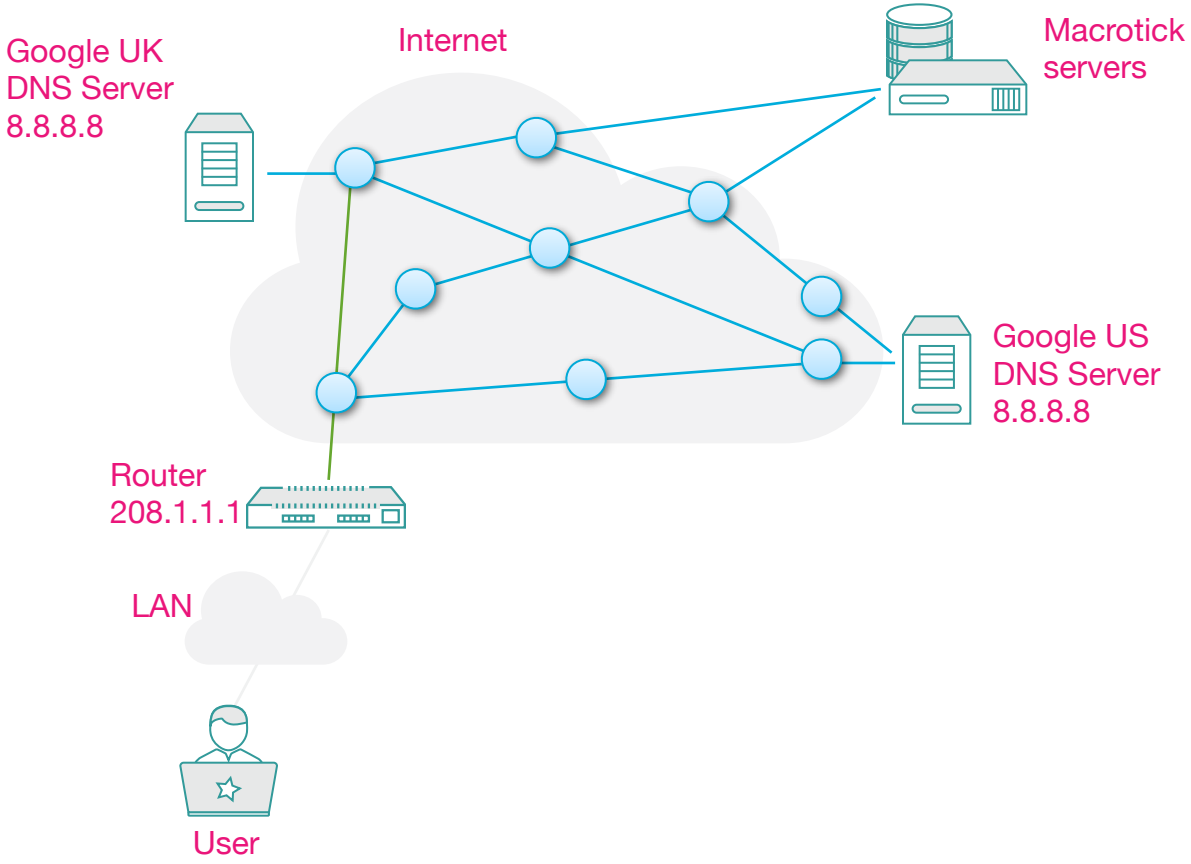
Simplified BGP and Unicast Routing



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 for DNS server

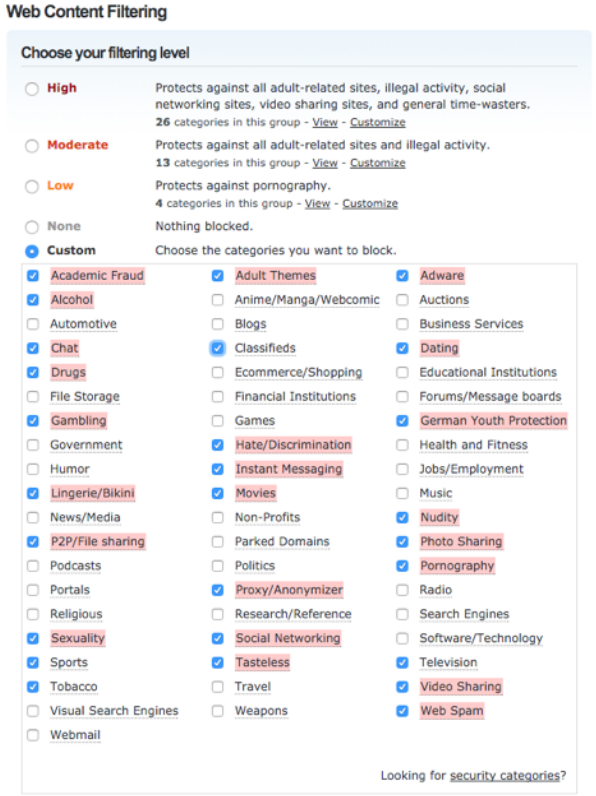
Why AnyCast

- 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 and Internet Classification

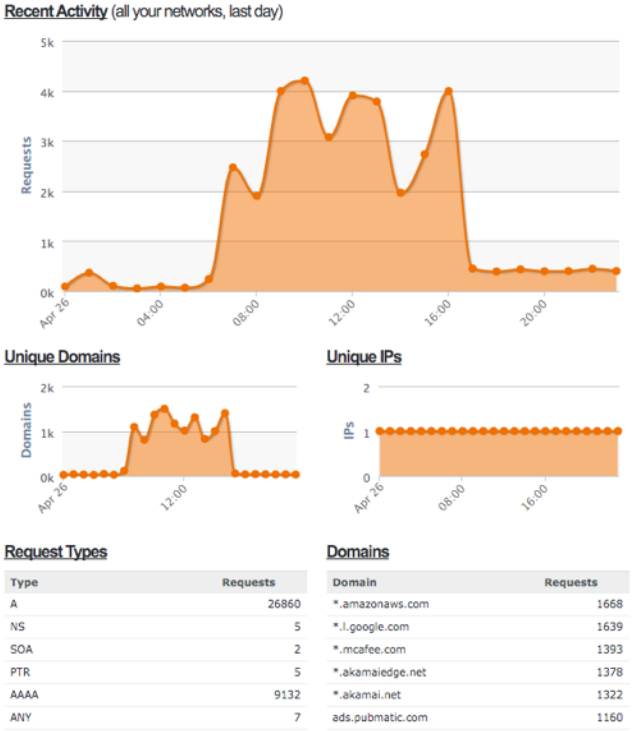
Next level of DNS service with OpenDNS

- 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



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



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

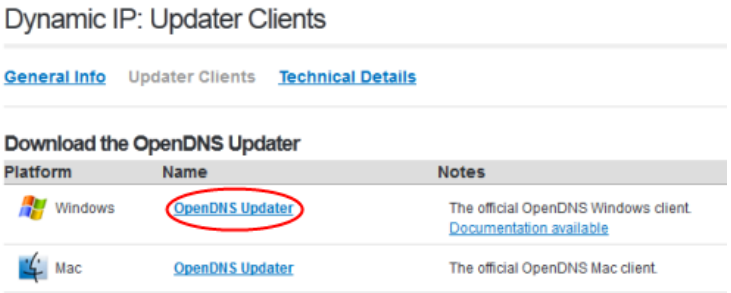
- Disable DNS server on Mikrotik
- Setup DHCP server to OpenDNS servers as DNS servers
- Workstations will send DNS requests directly to OpenDNS servers
- Add NAT firewall rule to redirect traffic to OpenDNS server port 53

```
/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.



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

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)

Solving Limitation through Integration

OpenDNS Integration

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

- What next

THANK YOU !

Questions?