

# Site to Site VPN on ADSL with



---

**Prajak Thunyawiraphap**

([prajak@mikrotiktutorial.com](mailto:prajak@mikrotiktutorial.com))



MUM Thailand in May 22, 2014

# Introduce



## Ruamrudee International School

Technology Committee / Network Admin

2,400 users : Computer 1,300 Units

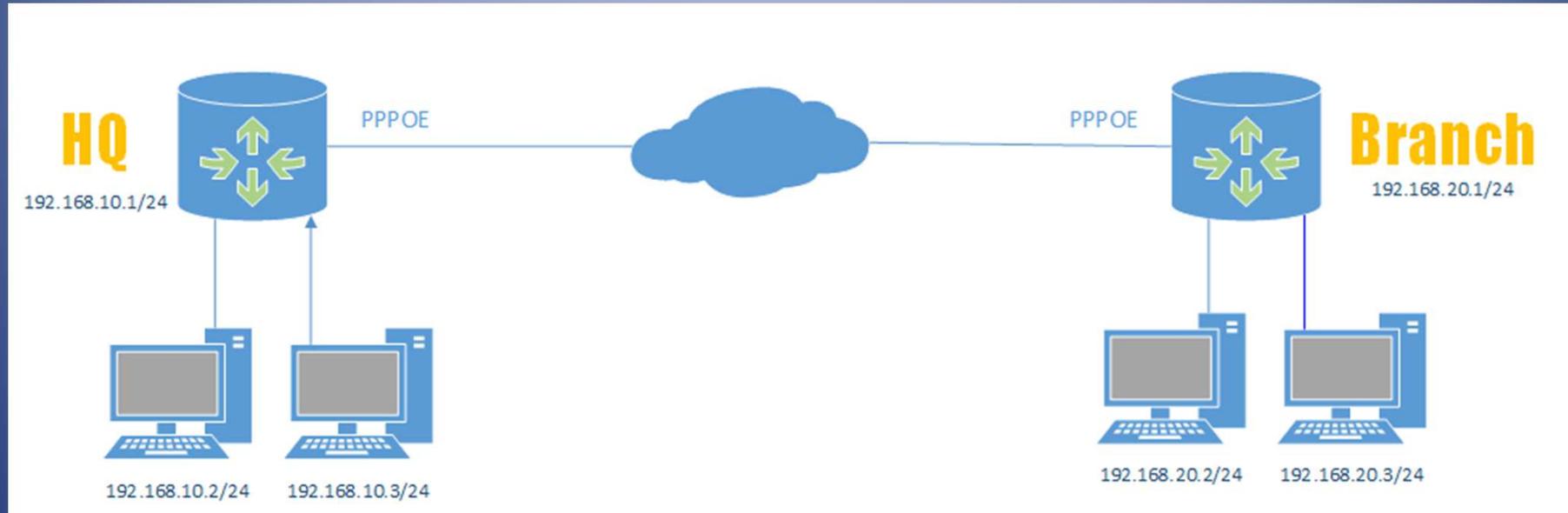
## Live Inc. Public Company

IT Director

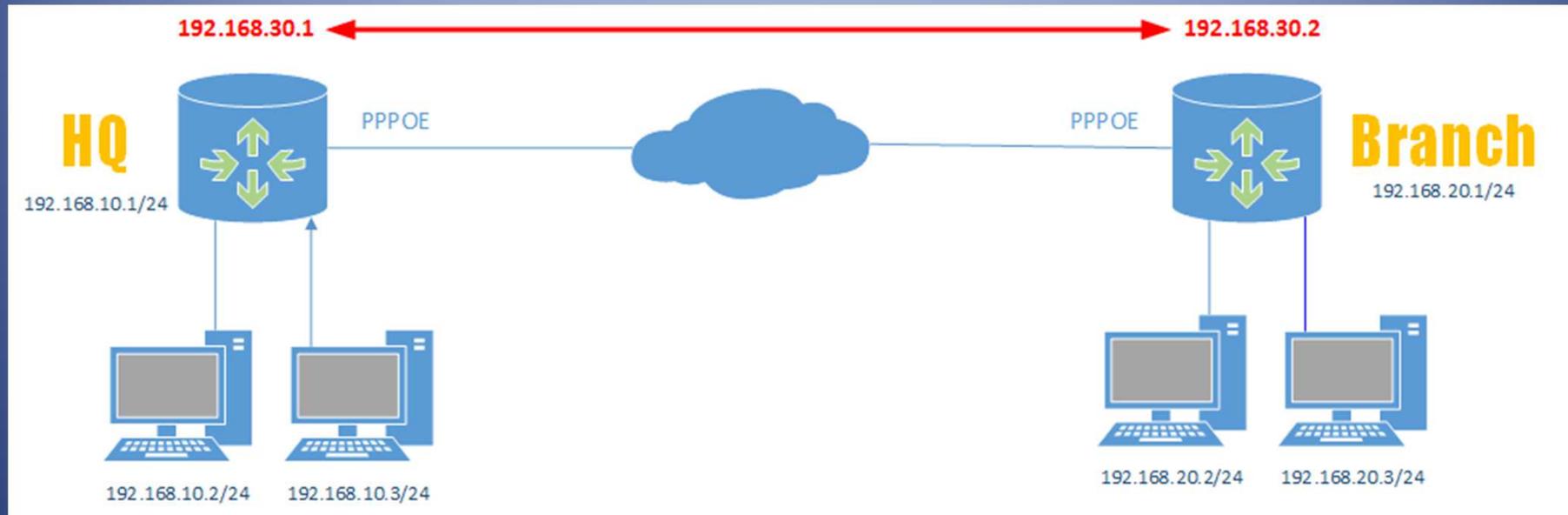
Broadcasting, High Availability system, Networking



# Scenario



# Scenario



# <http://wiki.mikrotik.com/wiki/Manual:IP/IPsec>

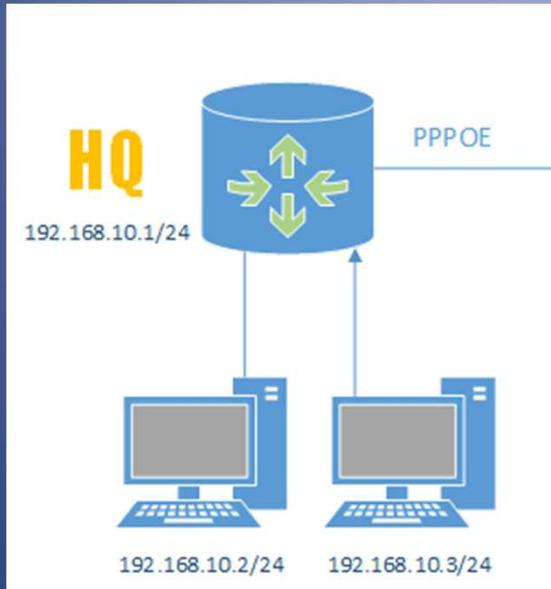
The image shows a Mikrotik WinBox interface with a diagram and configuration windows. The diagram at the top illustrates a Site to Site IPsec Tunnel connecting Office 1 (Public: 192.168.90.1/24, Local: 10.1.202.1/24) and Office 2 (Public: 192.168.80.1/24, Local: 10.1.101.1/24) through the Internet. The WinBox interface shows the menu path: IPsec > Peers > Add Peer. A dialog box for 'IPsec Peer' is open with the following configuration:

- Address: hq.mikrotiktutorial.com
- Port: 500
- Local Address: [Dropdown]
- Auth. Method: pre shared key
- Passive:
- Secret: [Text Field]

Numbered callouts indicate the following steps:

- 1: IP menu
- 2: IPsec menu
- 3: Peers menu
- 4: Add Peer dialog box

# Basic Setup for HQ Router



## Prevent Confusion

```
/system identity  
set name=HQ
```

## Setup WAN PPPOE

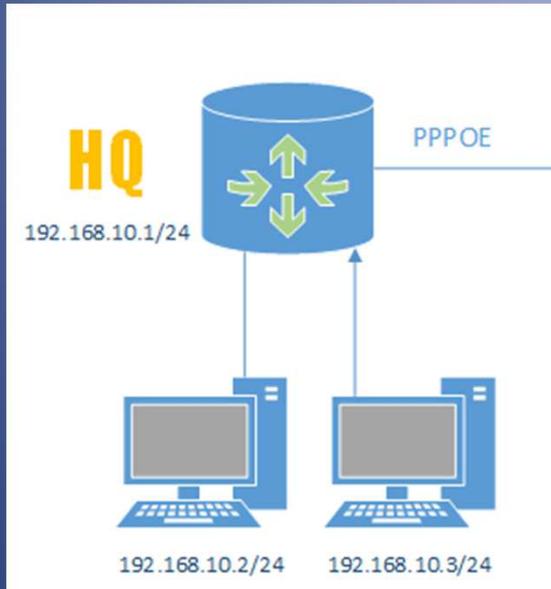
```
/interface pppoe-client  
add user=hq password=hq add-default-route=yes  
disabled=no name=pppoe-out1 profile=default use-  
peer-dns=yes interface=ether1
```

## Setup LAN IP

```
/ip address
```

```
add address=192.168.10.1/24 interface=ether2 network=192.168.10.0
```

# Basic Setup for HQ Router (cont.)



## Setup DHCP Service

```
/ip pool
add name=dhcp_pool1 ranges=192.168.10.100-
192.168.10.199
/ip dhcp-server
add address-pool=dhcp_pool1 disabled=no
interface=ether2 lease-time=1h name=dhcp1
/ip dhcp-server network
add address=192.168.10.0/24 dns-
server=192.168.10.1 gateway=192.168.10.1
```

## Setup DNS

```
/ip dns
set allow-remote-requests=yes
```

## Setup Masquerade (NAT)

```
/ip firewall nat
add action=masquerade chain=srcnat src-address=192.168.10.0/24
```

# Basic Setup for Branch Router

## Prevent Confusion

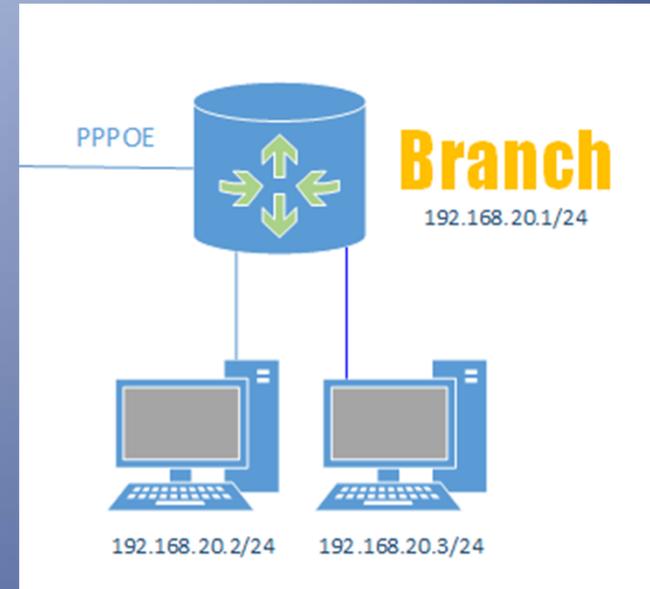
```
/system identity  
set name=Branch
```

## Setup WAN PPPOE

```
/interface pppoe-client  
add user=branch password=branch add-default-  
route=yes disabled=no name=pppoe-out1  
profile=default use-peer-dns=yes interface=ether1
```

## Setup LAN IP

```
/ip address  
add address=192.168.20.1/24 interface=ether2 network=192.168.20.0
```



# Basic Setup for Branch Router (cont.)

## Setup DHCP Service

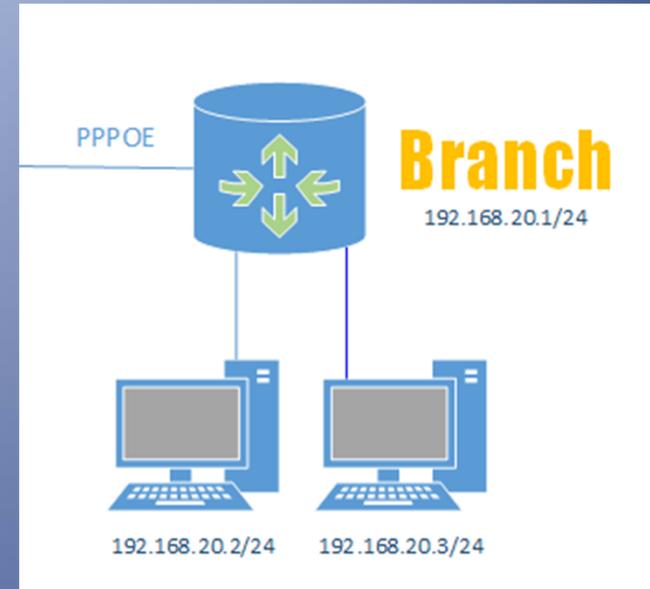
```
/ip pool
add name=dhcp_pool1 ranges=192.168.20.100-
192.168.20.199
/ip dhcp-server
add address-pool=dhcp_pool1 disabled=no
interface=ether2 lease-time=1h name=dhcp1
/ip dhcp-server network
add address=192.168.20.0/24 dns-
server=192.168.20.1 gateway=192.168.20.1
```

## Setup DNS

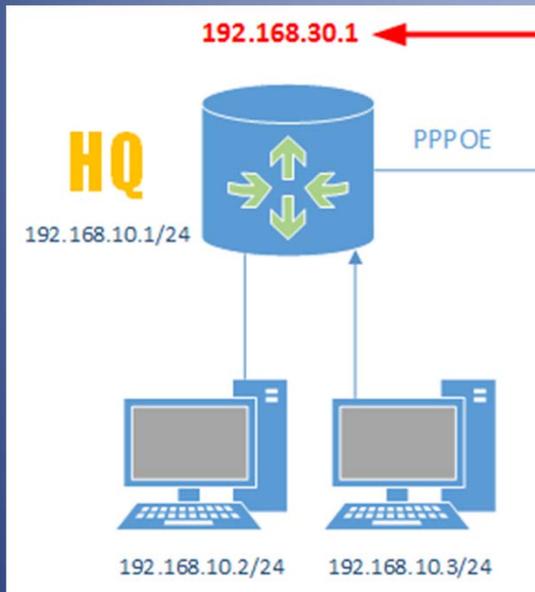
```
/ip dns
set allow-remote-requests=yes
```

## Setup Masquerade (NAT)

```
/ip firewall nat
add action=masquerade chain=srcnat src-address=192.168.20.0/24
```



# Setup L2TP Server on HQ



## Enable L2TP Server

```
/interface l2tp-server server  
set default-profile=Branch1 enabled=yes
```

## Create L2TP Profile

```
/ppp profile  
add name=Branch1
```

## Create Login account for branch

```
/ppp secret
```

```
add local-address=192.168.30.1  
name=branch1-l2tp  
password=branch1-l2tp profile=Branch1  
remote-address=192.168.30.2  
routes=192.168.20.0/24 service=l2tp
```

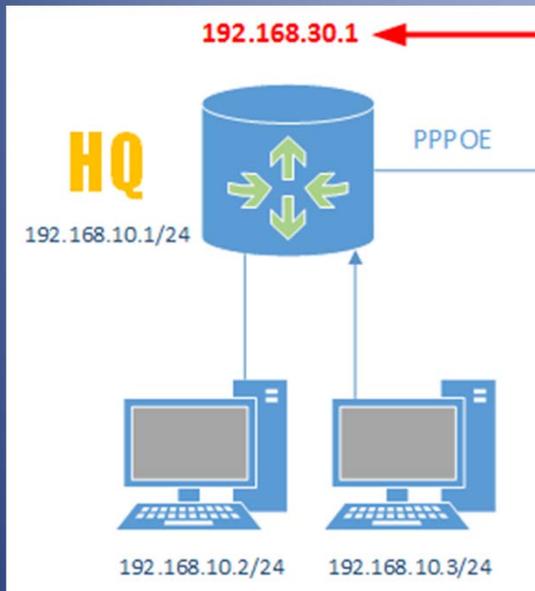
Route List	
Routes	Nexthops
DAS	0.0.0.0/0
DAC	192.168.10.0/24
DAS	192.168.20.0/24
DAC	192.168.30.2
DAC	192.168.200.1

The table shows the route list for the HQ router. A red arrow points to the entry for 192.168.20.0/24, which is reachable via 192.168.30.2 through the l2tp-branch1-l2tp profile.

## Make NAT Exception for VPN Traffic

```
/ip firewall nat  
add chain=srcnat dst-address=192.168.20.0/24 src-address=192.168.10.0/24
```

# L2TP Server Setup on HQ (cont.)



Make Sure VPN Exception is on top of NAT rule

The screenshot shows the Mikrotik Firewall configuration interface. The 'NAT' tab is selected. The table below shows the NAT rules:

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Po
0	✓ accept	srcnat	192.168.10.0/24	192.168.20.0/24			
1	≡ masquerade	srcnat	192.168.10.0/24				

A red arrow points to the 'Dst. Address' field of Rule 0, which is 192.168.20.0/24.

Setup DynDNS Script on HQ Router

[http://wiki.mikrotik.com/wiki/Dynamic\\_DNS\\_Update\\_Script\\_for\\_dynDNS](http://wiki.mikrotik.com/wiki/Dynamic_DNS_Update_Script_for_dynDNS)

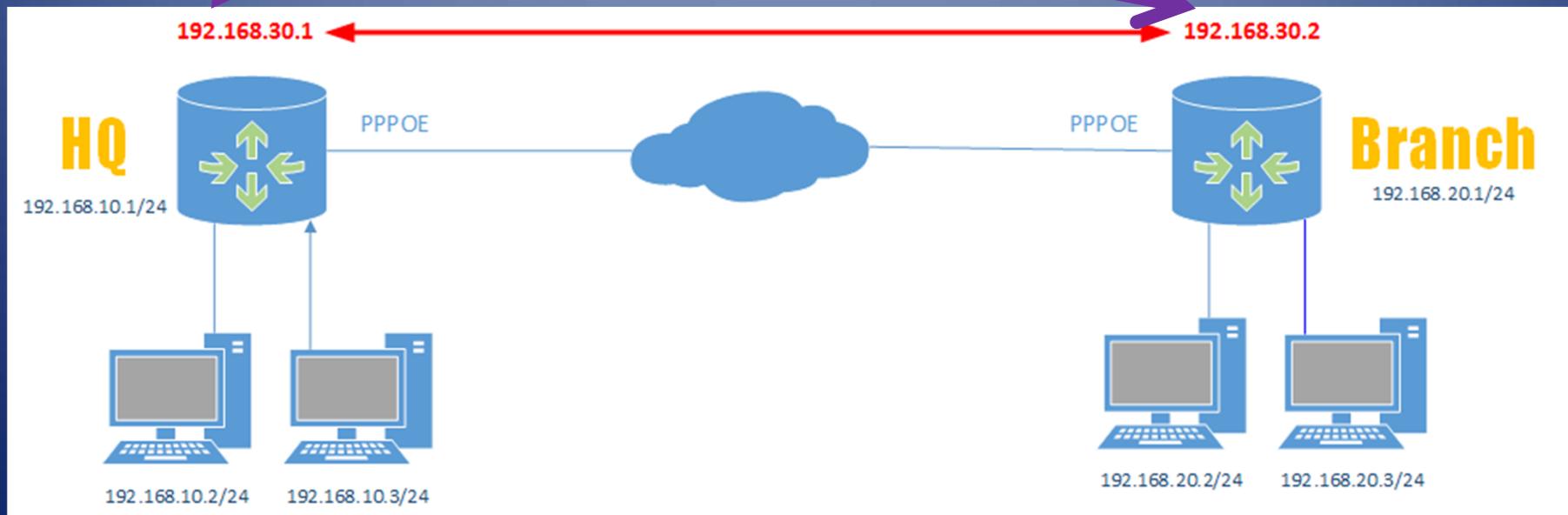
(Scripts for RoS 4.x, 5.x, 6.x and Scheduler)

Remark : in this example I set dynamic DNS name "hq.mikrotiktutorial.com"

# L2TP Server Setup on HQ (explain)

```
/ppp secret  
add local-address=192.168.30.1  
name=branch1-l2tp  
password=branch1-l2tp profile=Branch1  
remote-address=192.168.30.2  
routes=192.168.20.0/24 service=l2tp
```

Route List			
Routes	Nexthops	Rules	VRF
DAS	0.0.0.0/0	192.168.200.1 reachable pppoe-out1	
DAC	192.168.10.0/24	ether2 reachable	
DAS	192.168.20.0/24	192.168.30.2 reachable <l2tp-branch1-l2tp>	
DAC	192.168.30.2	pppoe-out1 reachable	
DAC	192.168.200.1	pppoe-out1 reachable	



# L2TP Client Setup on Branch

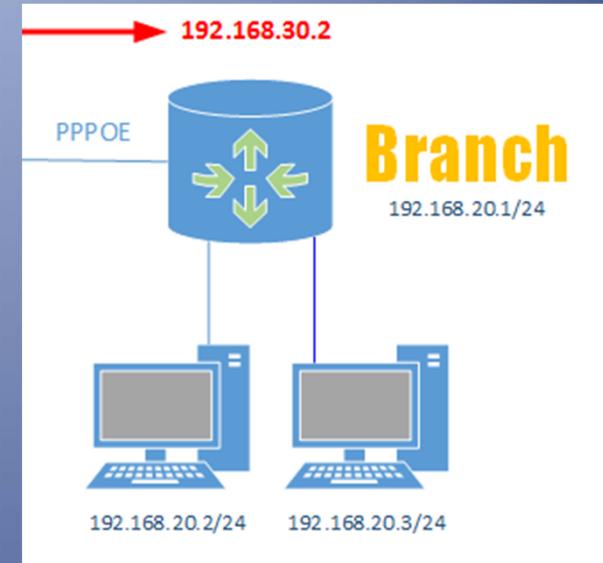
## Create L2TP Client Connection

```
/interface l2tp-client
add name=l2tp-to-hq user=branch1-l2tp
password=branch1-l2tp add-default-route=no
connect-to=hq.mikrotiktutorial.com disabled=no
name=l2tp-to-hq profile=default-encryption
```

## Route back to HQ

```
/ip firewall nat
add chain=srcnat dst-address=192.168.10.0/24 src-
address=192.168.20.0/24 ← Don't forget to move this line on top of default NAT rule.
```

```
/ip route
add dst-address=192.168.10.0/24 gateway=l2tp-to-hq
```

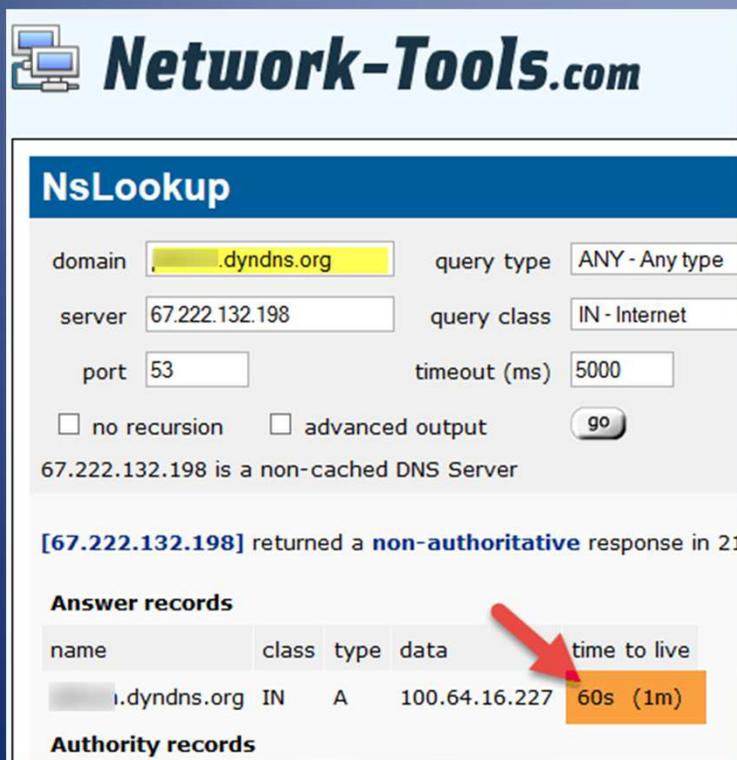


#	Action	Chain	Src. Address	Dst. Address	Photo...	S
0	✓ accept	srcnat	192.168.20.0/24	192.168.10.0/24		
1	⇄ masquerade	srcnat	192.168.20.0/24			

# What's else?

- DNS TTL

- <http://network-tools.com/nslookup/>



Network-Tools.com

### Nslookup

domain  query type   
server  query class   
port  timeout (ms)   
 no recursion  advanced output

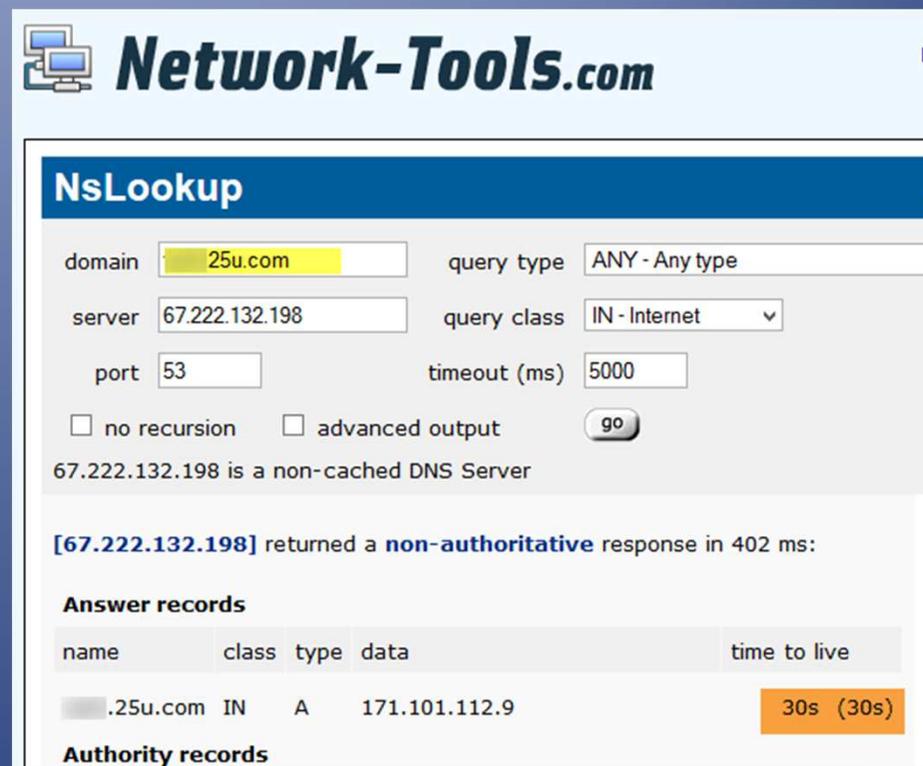
67.222.132.198 is a non-cached DNS Server

[67.222.132.198] returned a **non-authoritative** response in 21 ms

**Answer records**

name	class	type	data	time to live
.dyndns.org	IN	A	100.64.16.227	60s (1m)

**Authority records**



Network-Tools.com

### Nslookup

domain  query type   
server  query class   
port  timeout (ms)   
 no recursion  advanced output

67.222.132.198 is a non-cached DNS Server

[67.222.132.198] returned a **non-authoritative** response in 402 ms:

**Answer records**

name	class	type	data	time to live
.25u.com	IN	A	171.101.112.9	30s (30s)

**Authority records**

Q & A

# Thank you

<http://www.mikrotiktutorial.com>

```
# HQ
# may/22/2014 05:58:13 by RouterOS 6.13
#
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip hotspot user profile
set [ find default=yes ] idle-timeout=none keepalive-timeout=2m \
  mac-cookie-timeout=3d
/ip ipsec proposal
set [ find default=yes ] enc-algorithms=3des
/ip pool
add name=dhcp_pool1 ranges=192.168.10.100-192.168.10.199
/ip dhcp-server
add address-pool=dhcp_pool1 disabled=no interface=ether2 lease-time=1h name=\
  dhcp1
/port
set 0 name=serial0
set 1 name=serial1
/ppp profile
add name=Branch1
/interface pppoe-client
add ac-name="" add-default-route=yes allow=pap,chap,mschap1,mschap2 \
  default-route-distance=1 dial-on-demand=no disabled=no interface=ether1 \
  keepalive-timeout=60 max-mru=1480 max-mtu=1480 mrru=1600 name=pppoe-out1 \
  password=hq profile=default service-name="" use-peer-dns=yes user=hq
/system logging action
set 0 memory-lines=100
set 1 disk-lines-per-file=100
/interface l2tp-server server
set default-profile=Branch1 enabled=yes
/ip address
add address=192.168.10.1/24 interface=ether2 network=192.168.10.0
add address=192.168.200.100/24 disabled=yes interface=ether1 network=\
  192.168.200.0
/ip dhcp-server network
add address=192.168.10.0/24 dns-server=192.168.10.1 gateway=192.168.10.1
/ip dns
set allow-remote-requests=yes
/ip firewall filter
add action=drop chain=forward disabled=yes src-address=192.168.20.0/24
/ip firewall nat
add chain=srcnat dst-address=192.168.20.0/24 src-address=192.168.10.0/24
add action=masquerade chain=srcnat src-address=192.168.10.0/24
/ip upnp
set allow-disable-external-interface=no
/ppp secret
add local-address=192.168.30.1 name=branch1-l2tp password=branch1-l2tp profile=\
  Branch1 remote-address=192.168.30.2 routes=192.168.20.0/24 service=l2tp
/system identity
set name=HQ
/system lcd
set contrast=0 enabled=no port=parallel type=24x4
/system lcd page
set time disabled=yes display-time=5s
set resources disabled=yes display-time=5s
set uptime disabled=yes display-time=5s
set packets disabled=yes display-time=5s
set bits disabled=yes display-time=5s
set version disabled=yes display-time=5s
set identity disabled=yes display-time=5s
set pppoe-out1 disabled=yes display-time=5s
set <l2tp-branch1-l2tp> disabled=yes display-time=5s
set ether1 disabled=yes display-time=5s
set ether2 disabled=yes display-time=5s
```

```
#Branch
# may/22/2014 05:58:56 by RouterOS 6.13
#
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip hotspot user profile
set [ find default=yes ] idle-timeout=none keepalive-timeout=2m mac-cookie-timeout=3d
/ip ipsec proposal
set [ find default=yes ] enc-algorithms=3des
/ip pool
add name=dhcp_pool1 ranges=192.168.20.100-192.168.20.199
/ip dhcp-server
add address-pool=dhcp_pool1 disabled=no interface=ether2 lease-time=1h name=dhcp1
/port
set 0 name=serial0
set 1 name=serial1
/interface l2tp-client
add add-default-route=no allow=pap, chap, mschap1, mschap2
connect-to=hq.mikrotiktutorial.com dial-on-demand=no \
    disabled=no keepalive-timeout=60 max-mru=1450 max-mtu=1450 mrru=1600 name=l2tp-to-hq
    password=branch1-l2tp \
    profile=default-encryption user=branch1-l2tp
/interface pppoe-client
add ac-name="" add-default-route=yes allow=pap, chap, mschap1, mschap2
default-route-distance=1 dial-on-demand=no \
    disabled=no interface=ether1 keepalive-timeout=60 max-mru=1480 max-mtu=1480
    mrru=1600 name=pppoe-out1 \
    password=branch1 profile=default service-name="" use-peer-dns=yes user=branch1
/system logging action
set 0 memory-lines=100
set 1 disk-lines-per-file=100
/ip address
add address=192.168.20.1/24 interface=ether2 network=192.168.20.0
/ip dhcp-server network
add address=192.168.20.0/24 dns-server=192.168.20.1 gateway=192.168.20.1
/ip dns
set allow-remote-requests=yes
/ip firewall nat
add chain=srcnat dst-address=192.168.10.0/24 src-address=192.168.20.0/24
add action=masquerade chain=srcnat src-address=192.168.20.0/24
/ip route
add distance=1 dst-address=192.168.10.0/24 gateway=l2tp-to-hq
/ip upnp
set allow-disable-external-interface=no
/system identity
set name="Branch 1"
/system lcd
set contrast=0 enabled=no port=parallel type=24x4
/system lcd page
set time disabled=yes display-time=5s
set resources disabled=yes display-time=5s
set uptime disabled=yes display-time=5s
set packets disabled=yes display-time=5s
set bits disabled=yes display-time=5s
set version disabled=yes display-time=5s
set identity disabled=yes display-time=5s
set pppoe-out1 disabled=yes display-time=5s
set l2tp-to-hq disabled=yes display-time=5s
set ether1 disabled=yes display-time=5s
set ether2 disabled=yes display-time=5s
```