

# MikroTik DNS Spoofing

Presented by Michael Takeuchi  
MUM, 14 October 2016 - Indonesia  
[michael@takeuchi.id](mailto:michael@takeuchi.id)

*Let's Securing Your Network And Yourself !*

# About Michael Takeuchi

- Using MikroTik RouterOS (v5.20) Since 14 December 2014
  - RouterOS x86 at PC
- Using MikroTik RouterBoard (v6.25) Since 10 July 2015
  - RB941-2ND
- 24 April 2016, MTCNA 1604NA934 with Kakek Guru-ku (Ziad Sobri)
- 31 July 2016, MTCRE 1607RE248 with Kakek Guru-ku (Ziad Sobri)
- 3 August 2016, [MikroTik Certified Consultant](#) on Indonesia
- Still in School, [SMK Taruna Bhakti Depok](#)
- Wanna Be MikroTik Certified Trainer

# About SMK Taruna Bhakti Depok (STARBHAK)

- A Vocational School was placed at
  - [Jl. Raya Pekapuran, RT 02/RW 07, Kel. Curug, Kec. Cimanggis, Depok City, West Java](#)
  - [\(021\) 8744810](#)
- Informatics School
- STARBHAK = **SMK Taruna Bhakti**
- Motto: Our Quality Ask to Be Different
- Network Engineering, Multimedia, Software Engineering, Broadcasting, Electrical Engineering Industry
- MikroTik Academy and many more
- Website: [www.smktarunabhakti.net](http://www.smktarunabhakti.net)

# About SMK Taruna Bhakti Depok (STARBHAK)

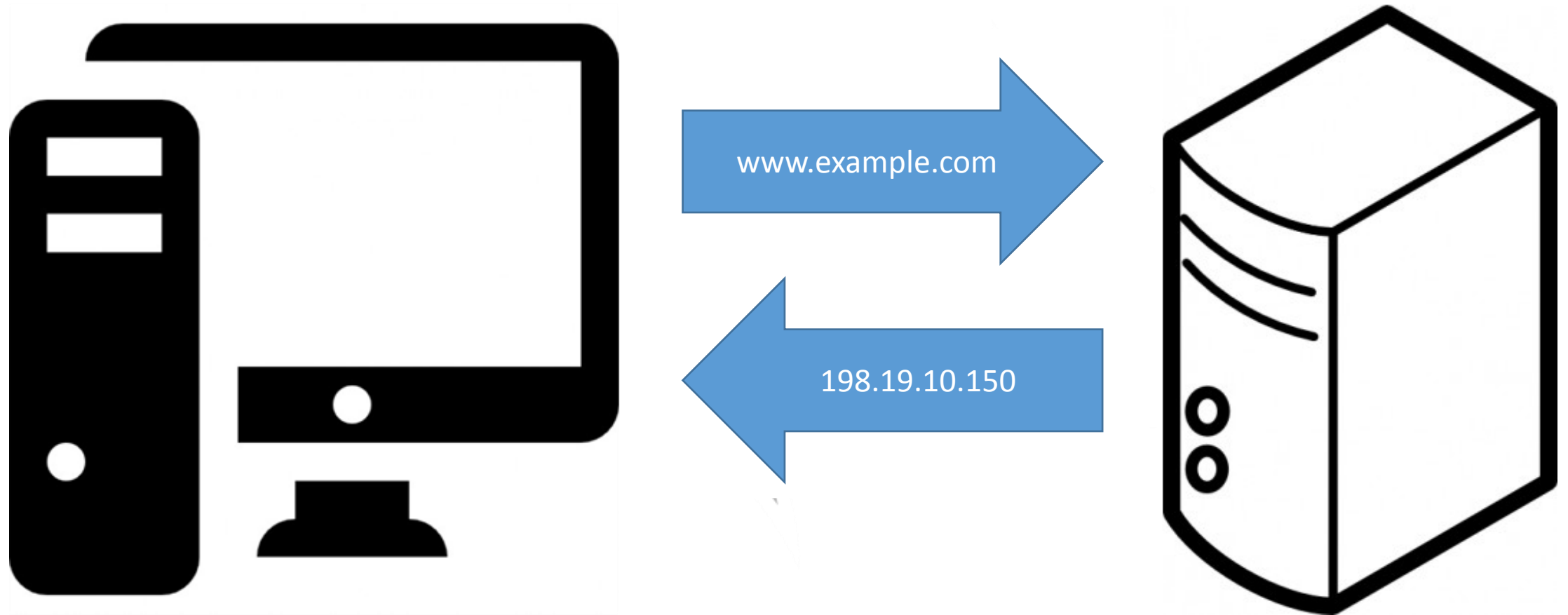


# About DNS (Domain Name System)

- As a Translator from Domain to Number (IP)
- A MikroTik router with DNS feature enabled can be set as a DNS Server
- MikroTik router can be specified as a Primary DNS Server under dhcp-server settings
- When allow-remote-request=yes The MikroTik router respond to TCP and UDP DNS request on port 53

From <http://wiki.mikrotik.com/wiki/Manual:IP/DNS>

# How DNS Works

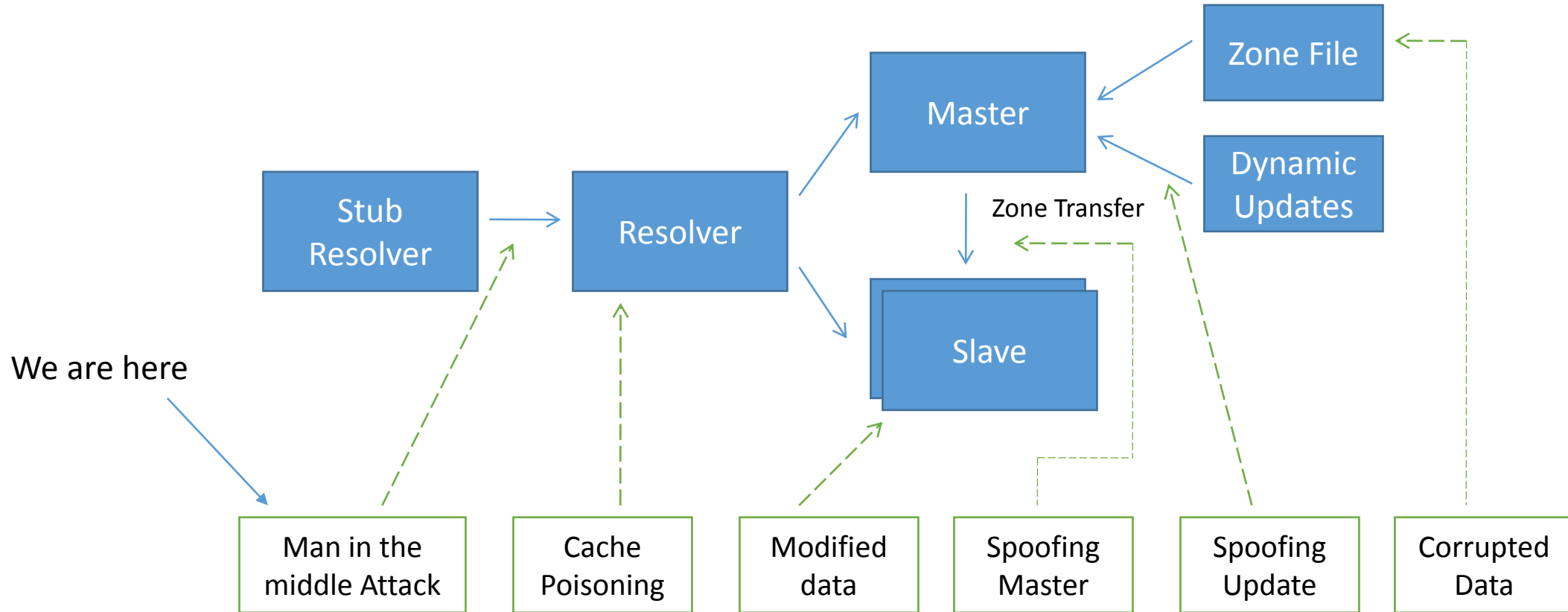


Requested with alphabet (Uniform Resource Locator, **URL**) and replied with number (IP)

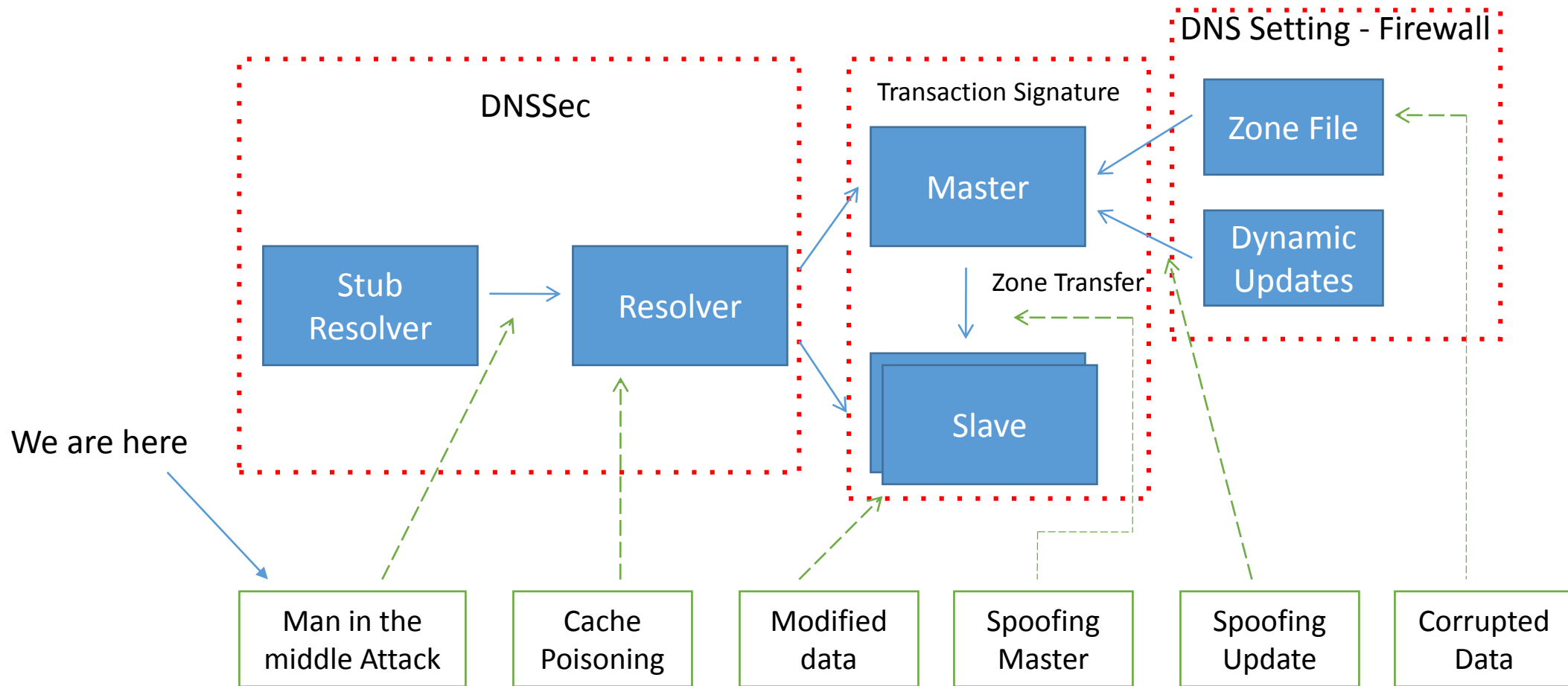
Read More: <https://howdns.works>

*images was taken from google images and modified by me*

# DNS Vulnerability



# Prevention





# DNSSEC/DNSCrypt

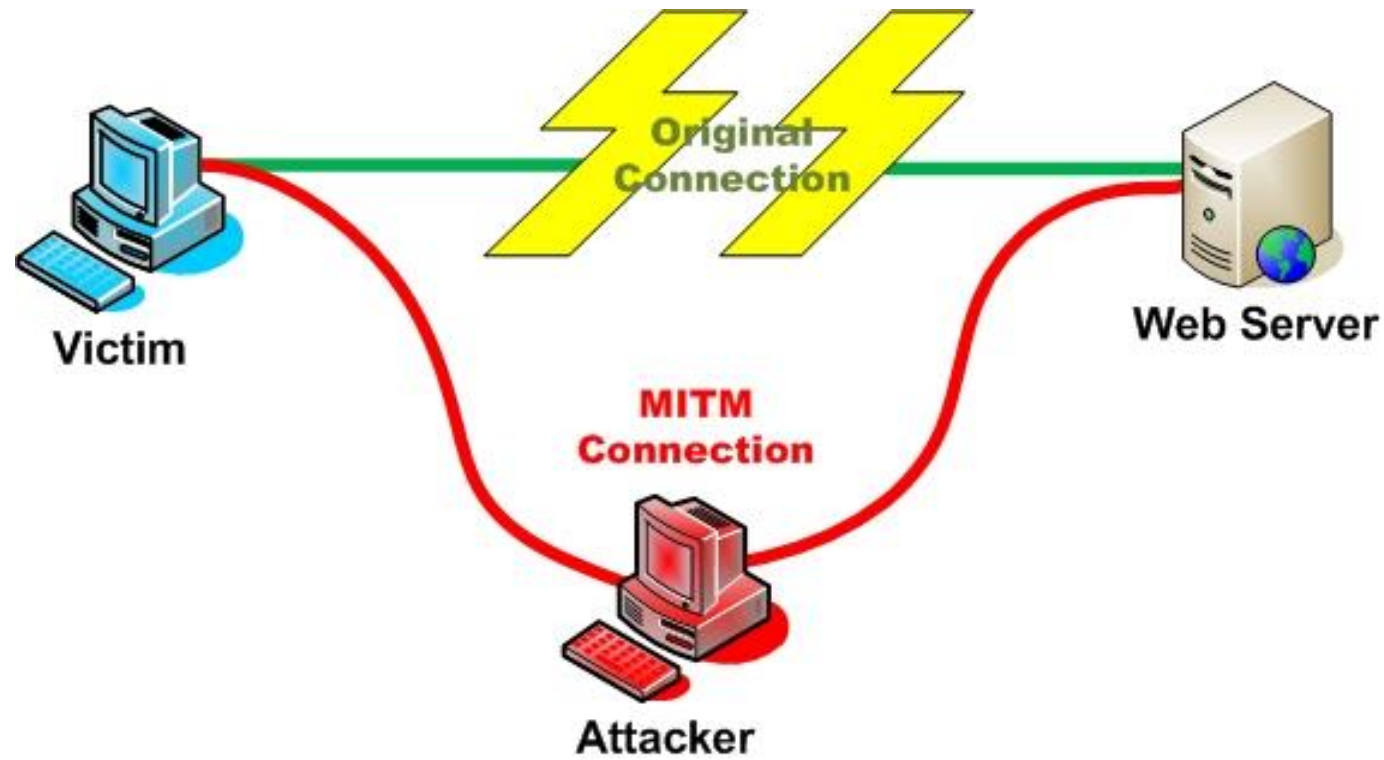
- DNS Security Extension
- DNSSEC used for verifying domain data with data on Authoritative DNS Server or Root DNS with Public Key/Digital Signature
- DNSCrypt are use Public Key to verifying DNS Server and using TCP/443

# TSIG

- Transaction Signature
- Is a method in which the master DNS server and secondary DNS server can do *zone-transfer* and *dynamic-update* if have same signature code

# About MITM (Man in The Middle) Attack

- MITM was Performed by Insider Attacker (On LAN)



*Images was Taken from Google Images*

# How DNS Spoofing Works?

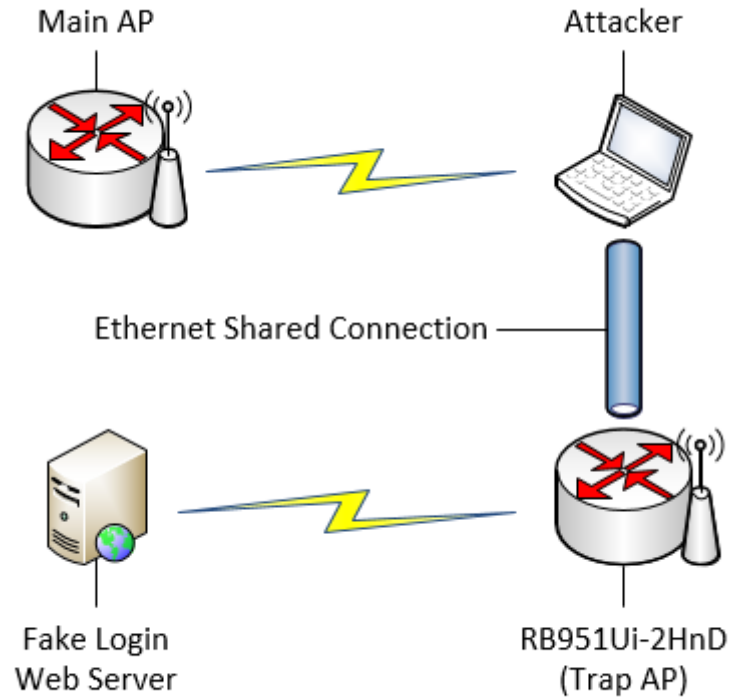
- When you are request [www.example.com](http://www.example.com) on browser, DNS will translate it to IP, Because Computer works with number, and we interact with name or domain when accessing website
- DNS Spoofing can manipulating an IP of Domain
- [www.example.com](http://www.example.com) IP is 198.19.10.150 and we will change to 192.168.1.4 (Fake Login Web Server IP)
- And we will using **MikroTik** feature to do DNS Spoofing

# Static DNS

*Yes, we will using **Static DNS** feature to do it*

Demonstration

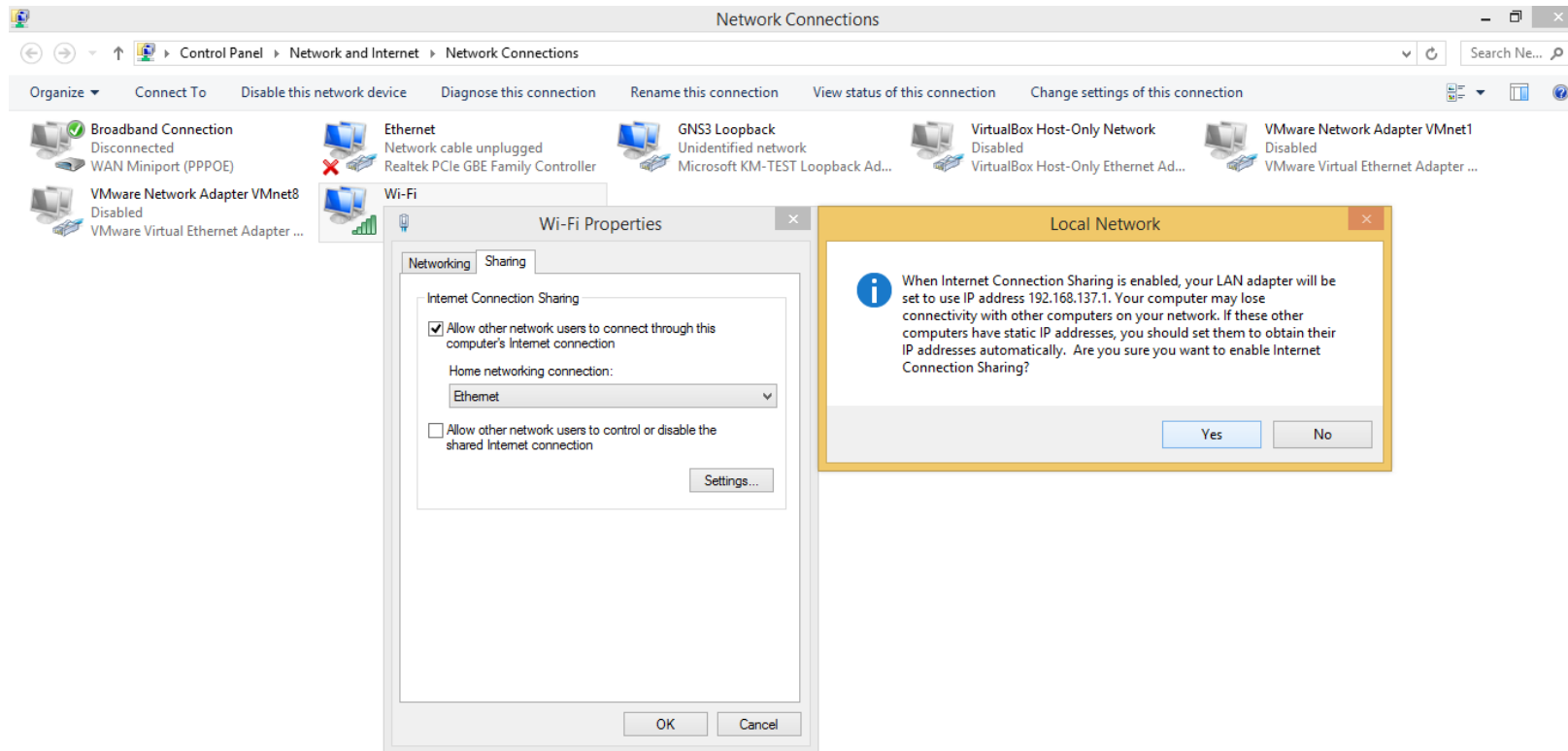
# 0. Topology



Main AP (victim) – Attacker – Ethernet Shared Connection

RouterBoard AP as Attacker AP (With Connected Attacker Web Server And Your Victim)

# 1. Ethernet Shared Connection (Attacker Windows)



Go To Control Panel\Network and Internet\Network Connections

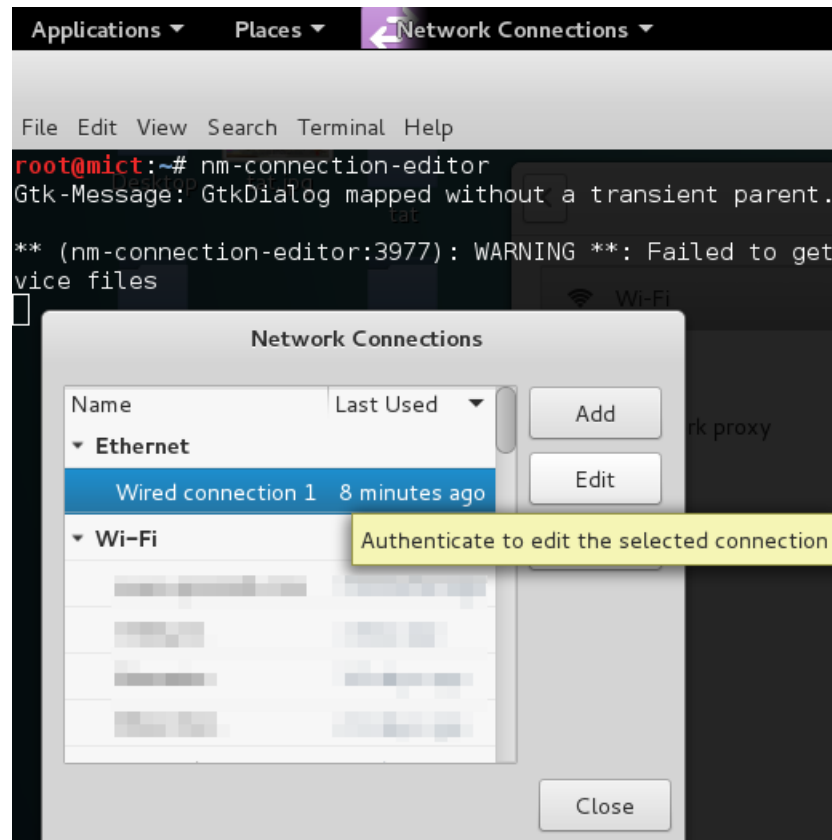
And do Right Click on Your Internet Connection Adapter (wifi) then choose properties, and then click Sharing Tab and **Check Allow other network users to connect through this computer's Internet Connection**

Click yes to create DHCP Server on your Ethernet Adapter



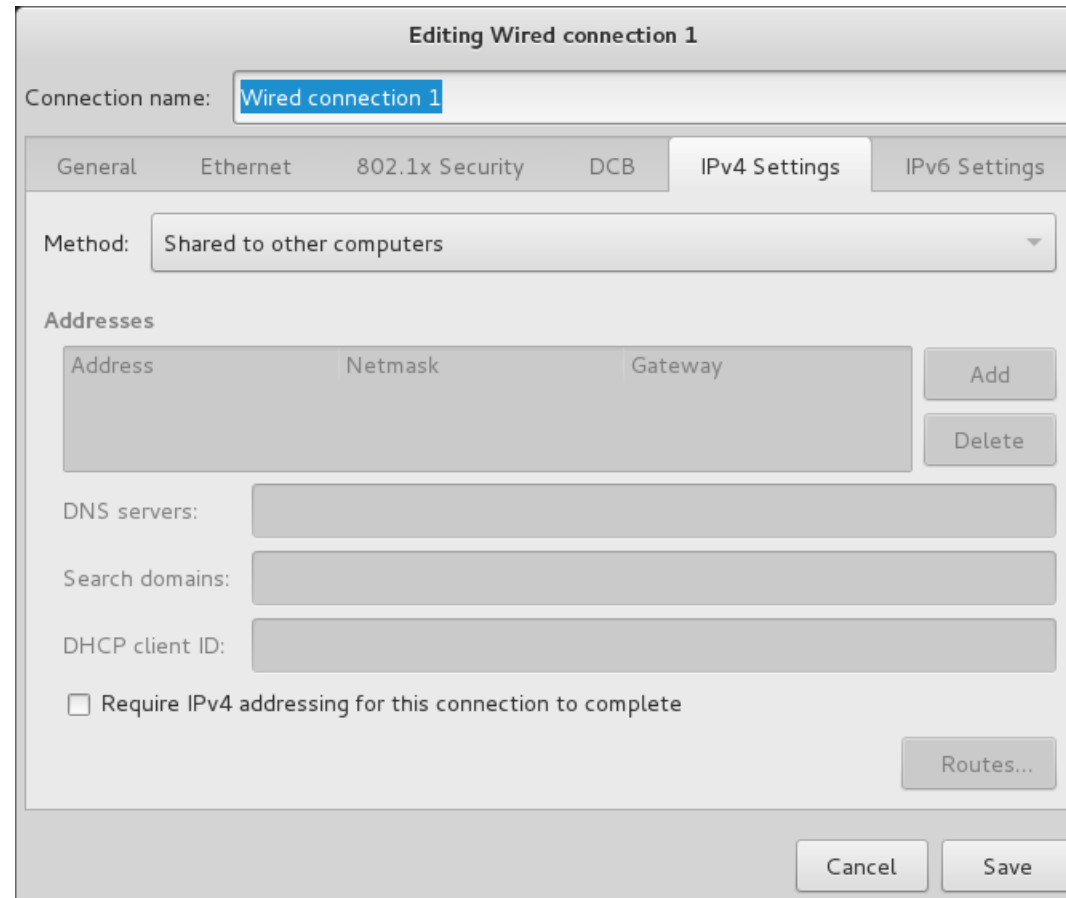
# 1. Ethernet Shared Connection (Attacker Linux)

Type **nm-connection-editor** on terminal than edit Wired connection 1



# 1. Ethernet Shared Connection (Attacker Linux)

Go To IPv4 Settings than change method to **Shared to other computers**



The image shows a screenshot of the 'Editing Wired connection 1' dialog box in a Linux network configuration tool. The 'IPv4 Settings' tab is selected, and the 'Method' dropdown menu is set to 'Shared to other computers'. The 'Addresses' section is empty, and the 'DNS servers', 'Search domains', and 'DHCP client ID' fields are also empty. The 'Require IPv4 addressing for this connection to complete' checkbox is unchecked. The 'Routes...' button is visible at the bottom right of the dialog box. The 'Cancel' and 'Save' buttons are at the bottom of the dialog box.

Editing Wired connection 1

Connection name: Wired connection 1

General Ethernet 802.1x Security DCB IPv4 Settings IPv6 Settings

Method: Shared to other computers

Addresses

Address	Netmask	Gateway
---------	---------	---------

DNS servers:

Search domains:

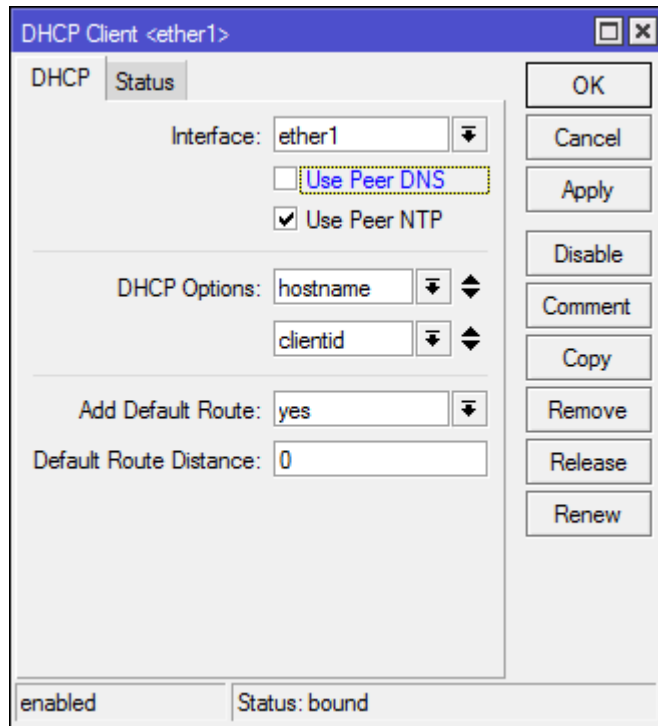
DHCP client ID:

Require IPv4 addressing for this connection to complete

Routes...

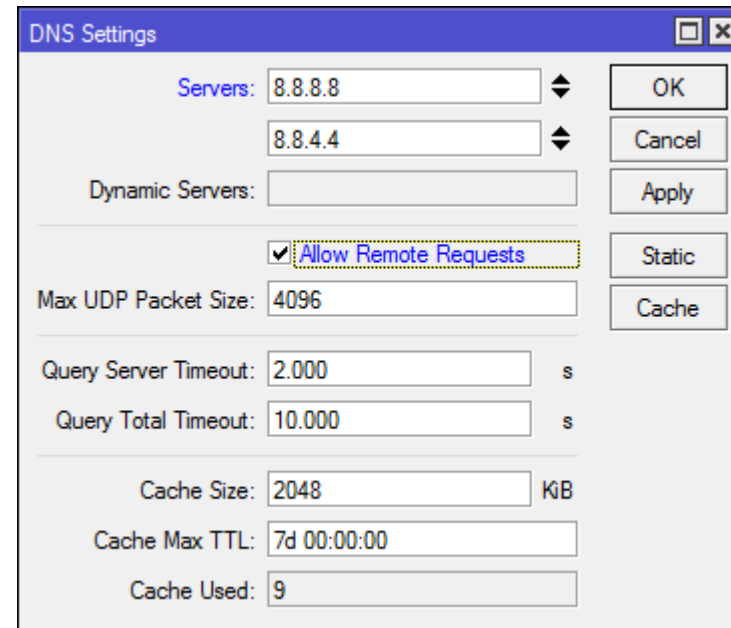
Cancel Save

## 2. Configure Internet on RouterBoard (DHCP & DNS)



The screenshot shows the 'DHCP Client <ether1>' configuration window. The 'DHCP' tab is active. The 'Interface' is set to 'ether1'. The 'Use Peer DNS' checkbox is unchecked and highlighted with a yellow dashed box. The 'Use Peer NTP' checkbox is checked. Under 'DHCP Options', 'hostname' and 'clientid' are selected. 'Add Default Route' is set to 'yes' and 'Default Route Distance' is '0'. The status bar at the bottom shows 'enabled' and 'Status: bound'. A vertical column of buttons on the right includes OK, Cancel, Apply, Disable, Comment, Copy, Remove, Release, and Renew.

Create DHCP Client without Dynamic DNS



The screenshot shows the 'DNS Settings' configuration window. The 'Servers' field contains '8.8.8.8' and '8.8.4.4'. The 'Dynamic Servers' field is empty. The 'Allow Remote Requests' checkbox is checked and highlighted with a yellow dashed box. The 'Max UDP Packet Size' is '4096'. The 'Query Server Timeout' is '2.000 s' and the 'Query Total Timeout' is '10.000 s'. The 'Cache Size' is '2048 KB', 'Cache Max TTL' is '7d 00:00:00', and 'Cache Used' is '9'. Buttons on the right include OK, Cancel, Apply, Static, and Cache.

Create DNS & Allow Remote Request

## 2. Configure Internet on RouterBoard (NAT)

The 'New NAT Rule' dialog box is shown with the 'General' tab selected. The 'Chain' is set to 'srcnat'. The 'Out. Interface' is set to 'ether1'. Other fields like 'Src. Address', 'Dst. Address', 'Protocol', 'Src. Port', 'Dst. Port', 'Any. Port', 'In. Interface', 'Packet Mark', 'Connection Mark', 'Routing Mark', 'Routing Table', and 'Connection Type' are empty.

The 'New NAT Rule' dialog box is shown with the 'Action' tab selected. The 'Action' is set to 'masquerade'. The 'Log' checkbox is unchecked. The 'Log Prefix' field is empty.

NAT Configuration

```
/ip firewall nat add chain=srcnat out-interface=ether1 action=masquerade
```

The Firewall configuration window shows the NAT tab. The rule list is as follows:

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Interface	Out. Interface	Bytes	Packets
0	masquerade	srcnat							ether1	0 B	0

# 3. Configure Access Point

Interface <wlan1>

General Wireless HT HT MCS WDS Nstreme NV2 Status Traffic

Mode: ap bridge

Band: 2GHz-B/G/N

Channel Width: 20MHz

Frequency: 2412 MHz

SSID: MikroTik

Scan List: default

Wireless Protocol: any

Security Profile: default

WPS Mode: push button

Bridge Mode: enabled

VLAN Mode: no tag

VLAN ID: 1

Default AP Tx Rate: bps

Default Client Tx Rate: bps

Default Authenticate

Default Forward

Hide SSID

OK

Cancel

Apply

Disable

Comment

Advanced Mode

Torch

WPS Accept

WPS Client

Setup Repeater

Scan...

Freq. Usage...

Align...

Sniff...

Snooper...

Reset Configuration

Address <192.168.1.1/24>

Address: 192.168.1.1/24

Network: 192.168.1.0

Interface: wlan1

OK

Cancel

Apply

Disable

Comment

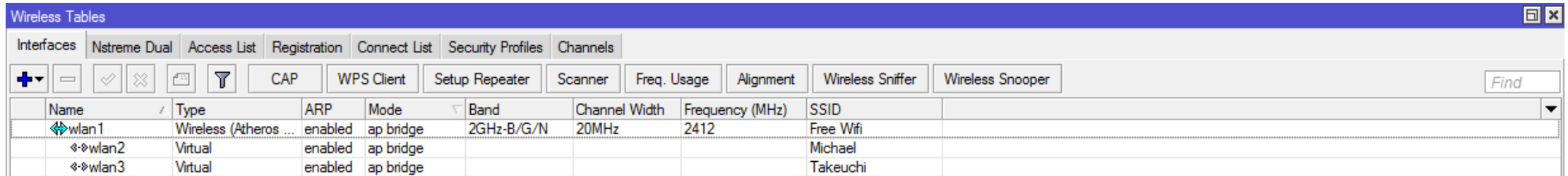
Copy

Remove

enabled

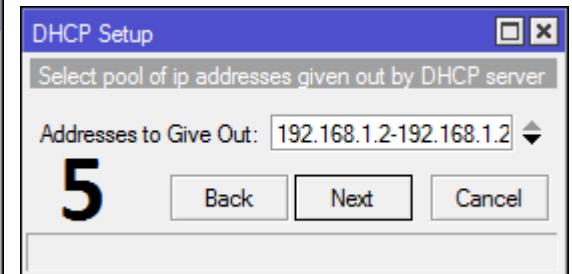
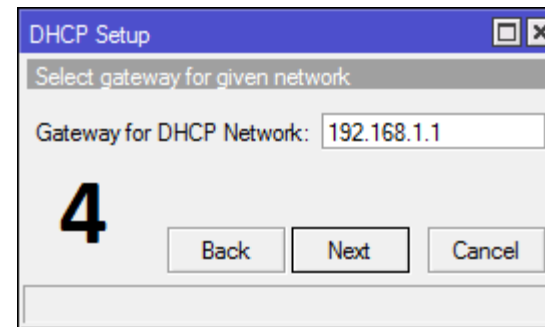
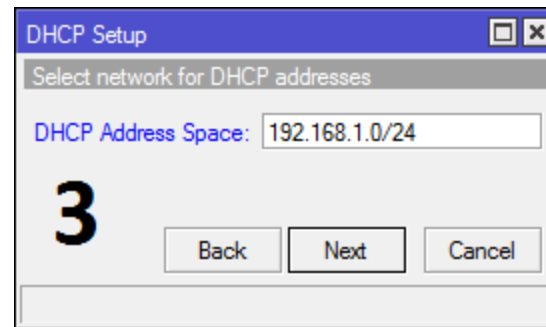
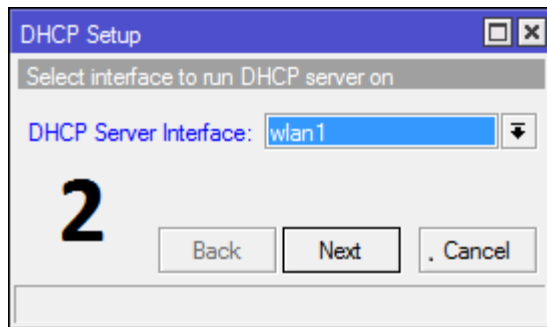
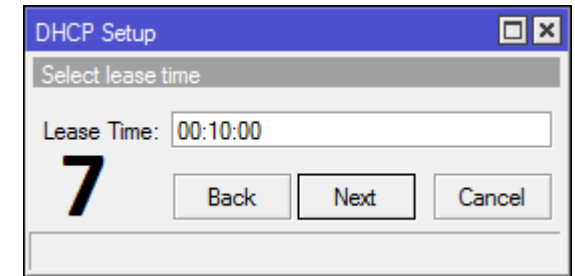
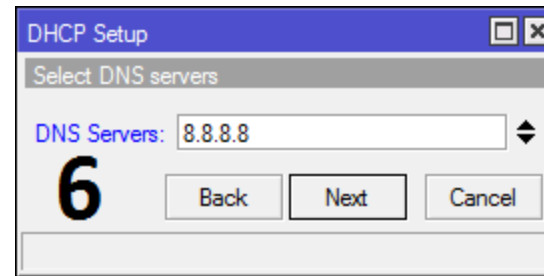
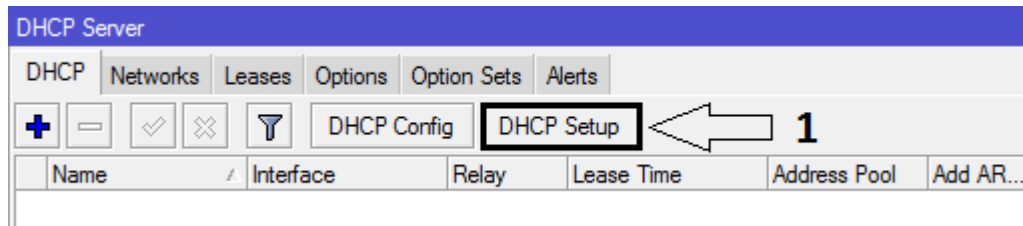
Create AP with AP Bridge Mode and set an IP Address

# 4. DHCP Server & Multiple SSID

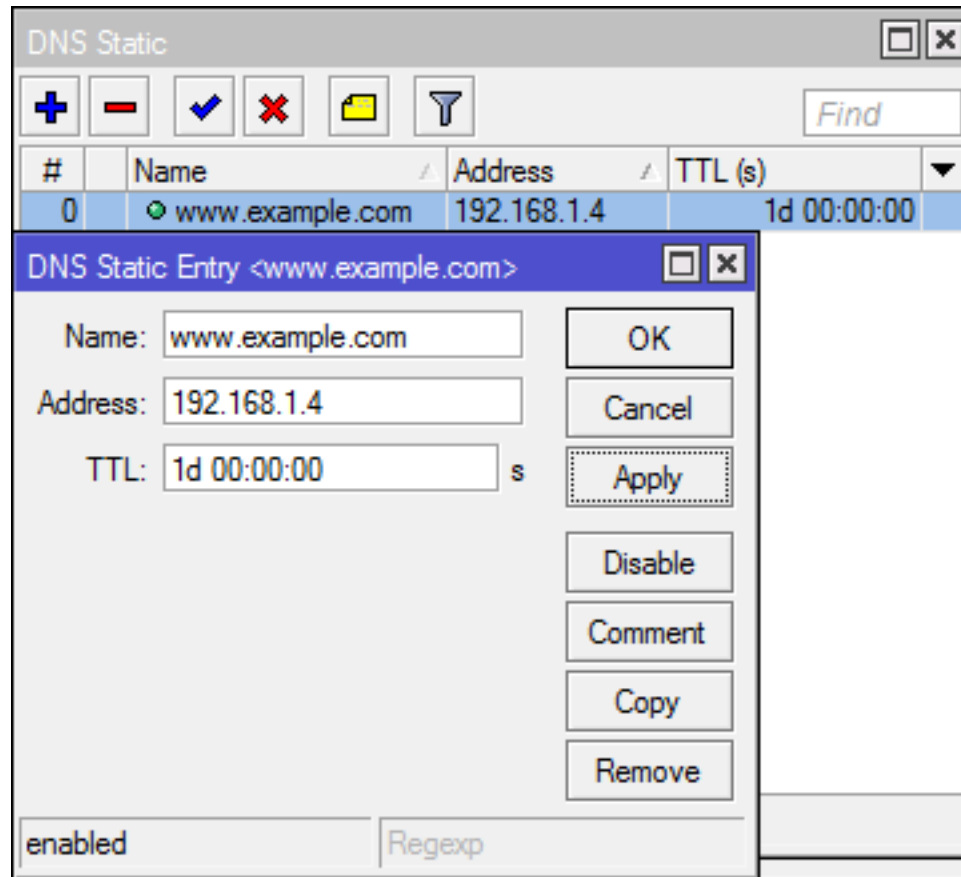


Name	Type	ARP	Mode	Band	Channel Width	Frequency (MHz)	SSID
wlan1	Wireless (Atheros ...)	enabled	ap bridge	2GHz-B/G/N	20MHz	2412	Free Wifi
wlan2	Virtual	enabled	ap bridge				Michael
wlan3	Virtual	enabled	ap bridge				Takeuchi

Create Multiple SSID, Choose Interesting Wifi Name (SSID)  
Then go to IP > DHCP Server > DHCP Setup

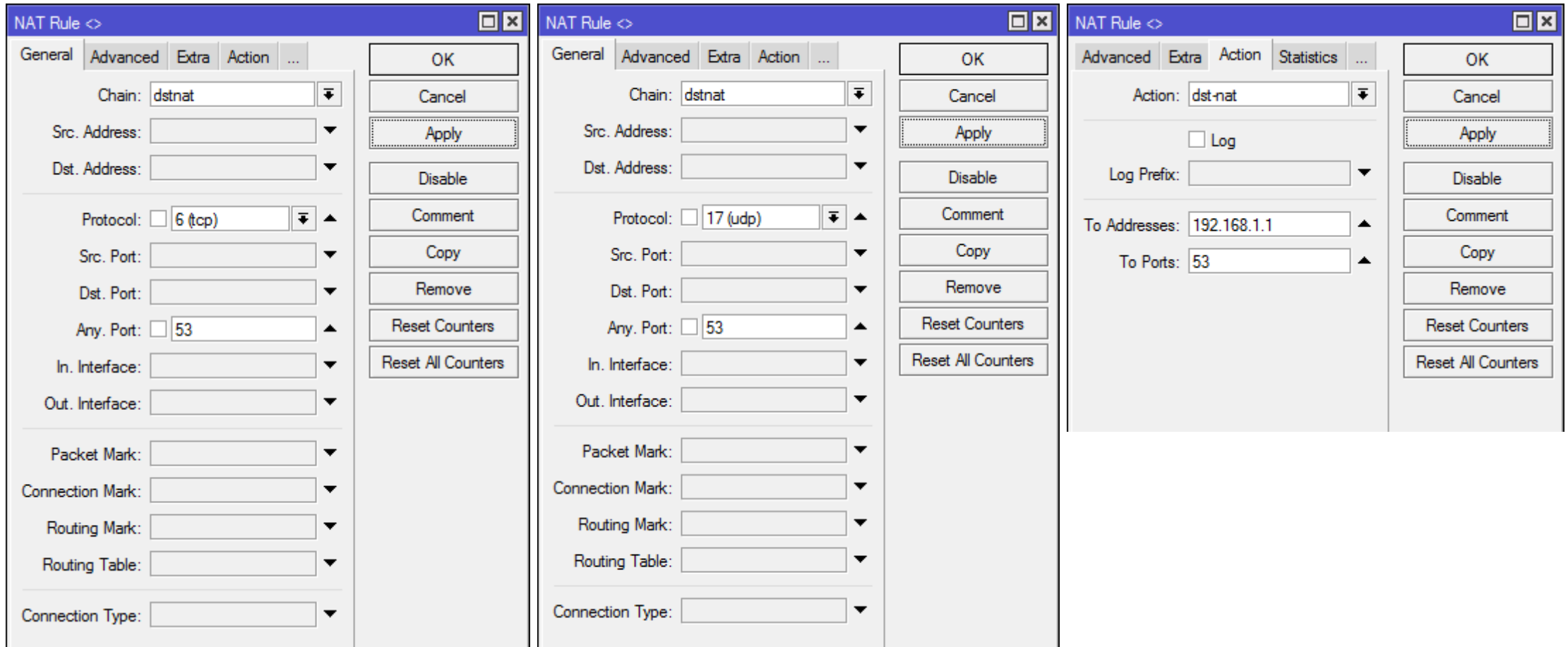


# 5. Spoofing



Address are filled with Attacker Web Server IP Address  
Name are filled with Domain Name that we want to Spoof

# 6. Transparent DNS (TCP & UDP)



Setup new rule with same action, port and chain, but has different protocol



## 7. Force people Connect to Your AP

- Disconnecting other people from Main Access Point (Deauth) and make them connect to your Trap Access Point (without password)

How to do it? It's Secret :P it's too dangerous

But... I will tell you on back stage if you ask something to me on Questions & Answers Session

## 8. DNS Spoofing Target

- Social Media Account
- Bank Account
- Forum Account
- Another Account
- Create Fake Website
- **Sending Malware**

# 9. How to Secure Your System and Your Self?

Yourself :

Don't Trust Free Wifi  
Awareness

Network Engineer :

Use Transport Layer Security (TLS)

Web Developer :

Use Secure Socket Layer (SSL)

# 10. Summary

I was setup a fake login web server on 192.168.1.4 and when an user access [www.example.com](http://www.example.com) they will redirected to my fake login pages with domain [www.example.com](http://www.example.com) , this is so tricky for common users and this things can be applied on another login pages or you can manipulate some software link download and change it with your malware and controll they device hahaha \*so evils, be aware !

Questions & Answers



Question  
&  
Answer

# Contact Me

- Facebook: <https://www.facebook.com/mict404>  
(Michael Takeuchi)
- LinkedIn: <https://www.linkedin.com/in/michael-takeuchi>  
(Michael Takeuchi)
- WhatApps: +62 812-8188-9660
- Phone: +62 896-2626-2669
- Twitter: [@mict404](https://twitter.com/mict404)
- Blog: <http://www.takeuchi.id>
- Email: [michael@takeuchi.id](mailto:michael@takeuchi.id)

**Thank You !**  
**For Time and Your Attention**

*and see u in the next MUM*