



April 13 2016  
Marco Polo Hotel  
Manila, Philippines



**CYGNALTECHNOLOGIES**  
[www.cygnaltech.net](http://www.cygnaltech.net)

# Introduction



**CYGNALTECHNOLOGIES**  
[www.cygnaltech.net](http://www.cygnaltech.net)

- Dan Santillan (owner of Cygnal Technologies)
- A Dial-up ISP in the Middle East (1997-2000)  
(Providing internet access to Military bases and personnel)
- A WISP operator from 2000 to 2013
- Mikrotik ROS user since late 1998 to present



## What we do...

IT Solutions provider for SME and Corporate

- System Integrator
- P-t-P and P-MtP Solution Provider
- Software Development and integration with Mikrotik products
- IP-VPN Infra Provider (Traditional and Wireless)
- VPN provider / Cloud hosting / Managed Services.
- Hotspot Solution  
(Public Events , Schools, Hospitals, Resorts, Hotels, Manufacturing, Warehouse, etc..)

# IP Hotspot Masking



# Why hotspot security topic?

There's an increase demand for Mikrotik AP's for hotspot purpose. Philippines is new to hotspot service and majority of hotspot operators do not fully understand the security of a public hotspot or the lack of it

## Who can benefit from this topic?

- Malls and Store Chains who offer Limited Free Internet Access
- Hotel, Restaurants and Resorts
- Small Business Owners
- WISP's and ISP's
- Government and Private Companies
- Home users
- OR anyone who already deployed a Mikrotik hotspot but lacking of security



## Is Mikrotik Hotspot secure?

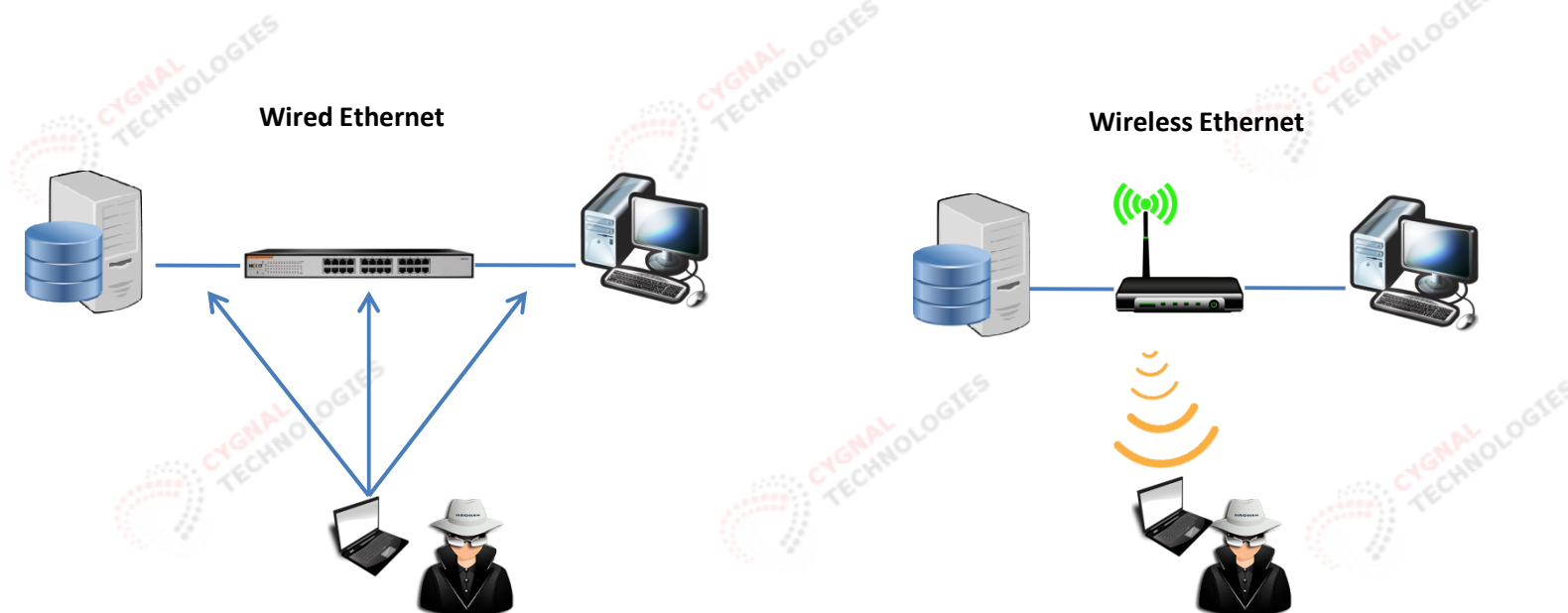
Can anyone penetrate the hotspot service and steal client's data or disrupt the hotspot service? If so... by what methods?



## Type of Attacks

- Passive Attack

The intent to steal information over wired or wireless communication by means of “eavesdropping”



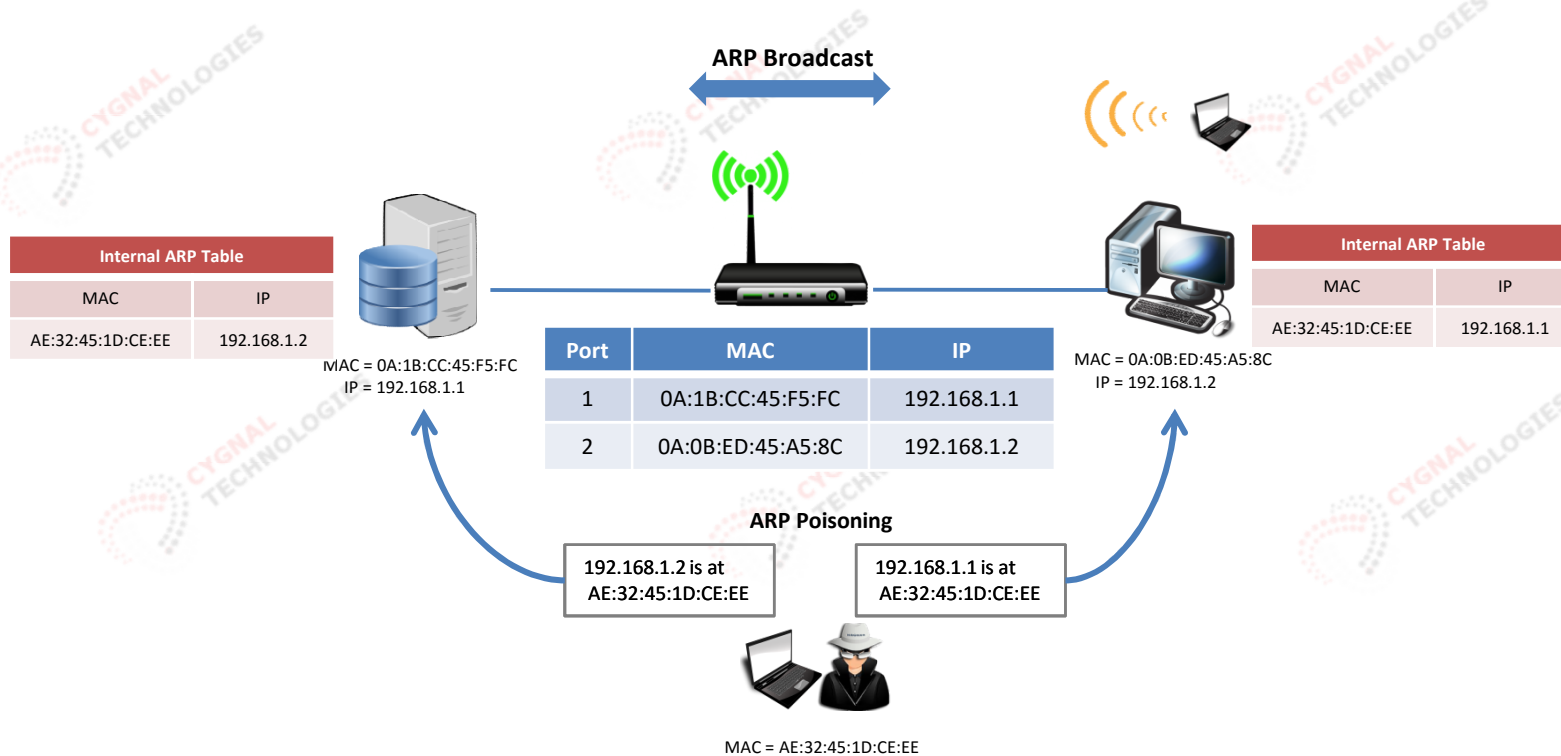


## Type of Attacks

- Passive Attack

The intent to steal information over wired or wireless communication by means of “eavesdropping”

ARP Poisoning is one of the oldest method of redirecting packets.





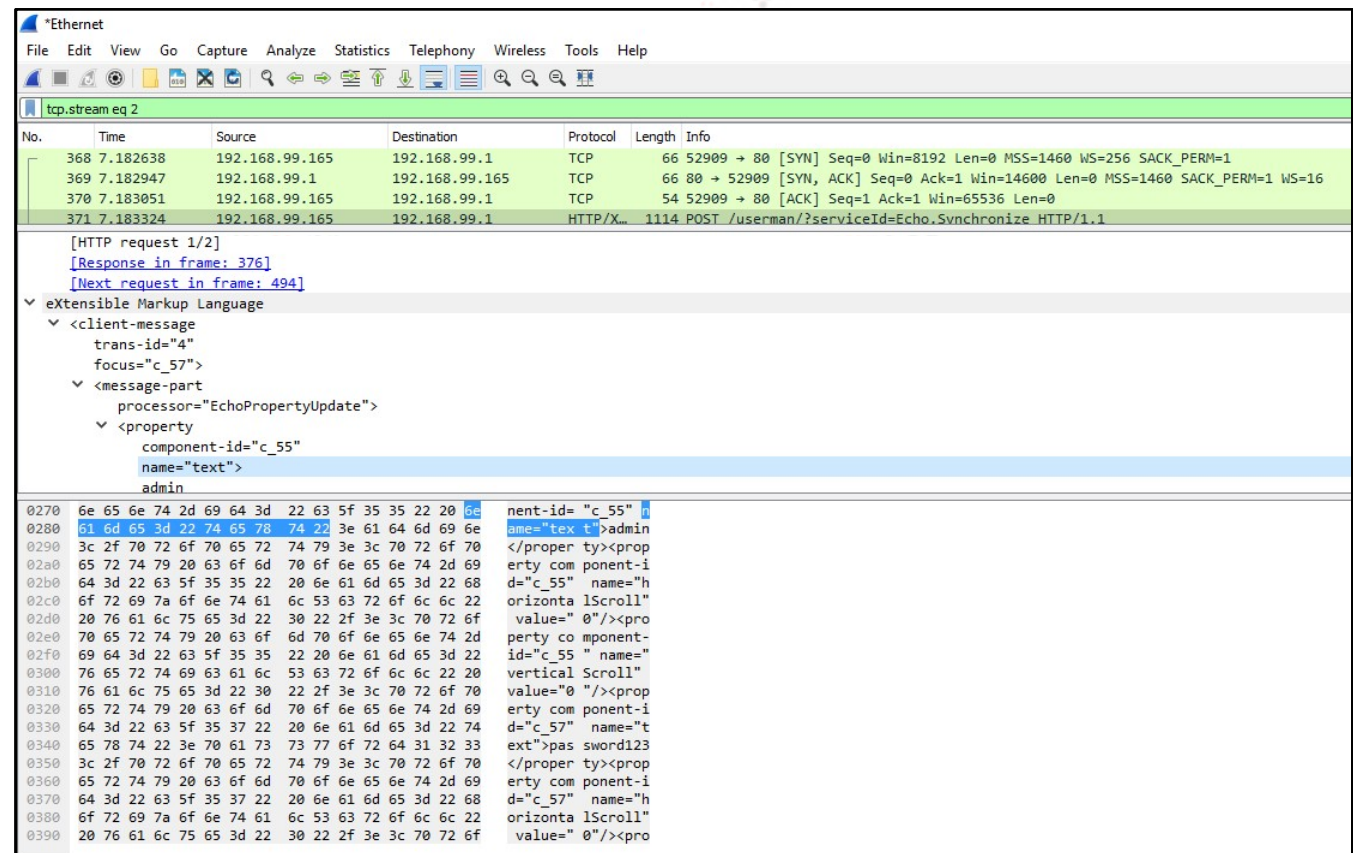


## Type of Attacks

- Passive Attack on wireless network, sniffing on Mikrotik Usermanager admin account accessed from the hotspot interface.



Wireless listening + Wireshark



No.	Time	Source	Destination	Protocol	Length	Info
368	7.182638	192.168.99.165	192.168.99.1	TCP	66	52909 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
369	7.182947	192.168.99.1	192.168.99.165	TCP	66	80 → 52909 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=16
370	7.183051	192.168.99.165	192.168.99.1	TCP	54	52909 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
371	7.183324	192.168.99.165	192.168.99.1	HTTP/Xm	1114	POST /userman/?serviceId=Echo.Synchronize HTTP/1.1

```

[HTTP request 1/2]
[Response in frame: 376]
[Next request in frame: 494]
eXtensible Markup Language
  <client-message
    trans-id="4"
    focus="c_57">
    <message-part
      processor="EchoPropertyUpdate">
      <property
        component-id="c_55"
        name="text">
        admin
  
```

Offset	Hex	ASCII
0270	6e 65 6e 74 2d 69 64 3d 22 63 5f 35 35 22 20 6e	nent-id= "c_55" n
0280	61 6d 65 3d 22 74 65 78 74 22 3e 61 64 6d 69 6e	ame="text">admin
0290	3c 2f 70 72 6f 70 65 72 74 79 3e 3c 70 72 6f 70	</proper ty><prop
02a0	65 72 74 79 20 63 6f 6d 70 6f 6e 65 6e 74 2d 69	erty component-i
02b0	64 3d 22 63 5f 35 35 22 20 6e 61 6d 65 3d 22 68	d="c_55" name="h
02c0	6f 72 69 7a 6f 6e 74 61 6c 53 63 72 6f 6c 6c 22	orizonta lScroll"
02d0	20 76 61 6c 75 65 3d 22 30 22 2f 3e 3c 70 72 6f	value=" 0"/><pro
02e0	70 65 72 74 79 20 63 6f 6d 70 6f 6e 65 6e 74 2d	perty co mponent-
02f0	69 64 3d 22 63 5f 35 35 22 20 6e 61 6d 65 3d 22	id="c_55 " name="
0300	76 65 72 74 69 63 61 6c 53 63 72 6f 6c 6c 22 20	vertical Scroll"
0310	76 61 6c 75 65 3d 22 30 22 2f 3e 3c 70 72 6f 70	value="0 " /><prop
0320	65 72 74 79 20 63 6f 6d 70 6f 6e 65 6e 74 2d 69	erty component-i
0330	64 3d 22 63 5f 35 37 22 20 6e 61 6d 65 3d 22 74	d="c_57" name="t
0340	65 78 74 22 3e 70 61 73 73 77 6f 72 64 31 32 33	ext">pas sword123
0350	3c 2f 70 72 6f 70 65 72 74 79 3e 3c 70 72 6f 70	</proper ty><prop
0360	65 72 74 79 20 63 6f 6d 70 6f 6e 65 6e 74 2d 69	erty component-i
0370	64 3d 22 63 5f 35 37 22 20 6e 61 6d 65 3d 22 68	d="c_57" name="h
0380	6f 72 69 7a 6f 6e 74 61 6c 53 63 72 6f 6c 6c 22	orizonta lScroll"
0390	20 76 61 6c 75 65 3d 22 30 22 2f 3e 3c 70 72 6f	value=" 0"/><pro



## Type of Attacks

- Passive Attack on wireless network, sniffing on Mikrotik Usermanager admin account accessed from the hotspot interface.



```

Wireshark · Follow TCP Stream (tcp.stream eq 2) · wireshark_pcapng_3BC8D150-0D81-4E79-8714-FF9A25E827BA_20160307213631_a04180
POST /userman/?serviceId=Echo.Synchronize HTTP/1.1
Host: 192.168.99.1
Connection: keep-alive
Content-Length: 592
Origin: http://192.168.99.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/48.0.2564.116 Safari/537.36
Content-Type: text/xml
Accept: */*
Referer: http://192.168.99.1/userman
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8
Cookie: MWTSESSION=345389691991625943; username=admin2

<client-message trans-id="4" focus="c_57"><message-part processor="EchoPropertyUpdate"><property component-id="c_55"
name="text">admin</property><property component-id="c_55" name="horizontalScroll" value="0"/><property component-id="c_55"
name="verticalScroll" value="0"/><property component-id="c_57" name="text">password123</property><property component-
id="c_57" name="horizontalScroll" value="0"/><property component-id="c_57" name="verticalScroll" value="0"/></message-
part><message-part processor="EchoAction"><action component-id="c_57" name="action"/></message-part></client-message>HTTP/
1.1 200 OK
Connection: Keep-Alive
Content-Length: 20512
Content-Type: text/xml; charset=UTF-8
Date: Mon, 07 Mar 2016 13:41:53 GMT
Expires: 0

<?xml version="1.0" encoding="UTF-8"?><server-message async-interval="60000" modal-id="" root-layout-direction="ltr" trans-
id="5" xmlns="http://www.nextapp.com/products/echo2/svrmsg/servermessage"><libraries><library service-id="/mwt/core/js/
ContentPane.js" /><library service-id="/mwt/core/js/TextComponent.js" /><library service-id="/mwt/core/js/Button.js" /
><library service-id="/mwt/core/js/WindowPane.js" /><library service-id="/mwt/core/js/SplitPane.js" /><library service-
id="/mwt/core/js/Table.js" /><library service-id="/mwt/core/js/TableUpdate.js" /><library service-id="/mwt/extras/js/
ExtrasUtil.js" /><library service-id="/mwt/extras/js/Menu.js" /><library service-id="/mwt/extras/js/MenuUpdate.js" /
><library service-id="/mwt/extras/js/Pagination.js" /><library service-id="/mwt/extras/js/PerPageField.js" /></
libraries><message-part-group id="init" /><message-part-group id="preremove"><message-part
processor="EchoContentPane.MessageProcessor"><dispose><item eid="c_2" /></dispose></message-part><message-part
processor="EchoTextComponent.MessageProcessor"><dispose><item eid="c_55" /></dispose><dispose><item eid="c_57" /></
dispose></message-part><message-part processor="EchoButton.MessageProcessor"><dispose><item eid="c_58" /></dispose></
message-part><message-part processor="EchoWindowPane.MessageProcessor"><dispose eid="c_50" /></message-part></message-part-
group><message-part-group id="remove"><message-part processor="EchoDomUpdate.MessageProcessor"><dom-remove-children target-
id="c_root" /></message-part></message-part-group></message-part-group id="update"><message-part

```



## Type of Attacks

- Active Attack on an opened wireless network.

Similar to passive attack but with intention to disrupt the system, such as

- ARP Poisoning
- Malformed Packet Injection
- DNS Spoofing / Poisoning
- Broadcast Storm

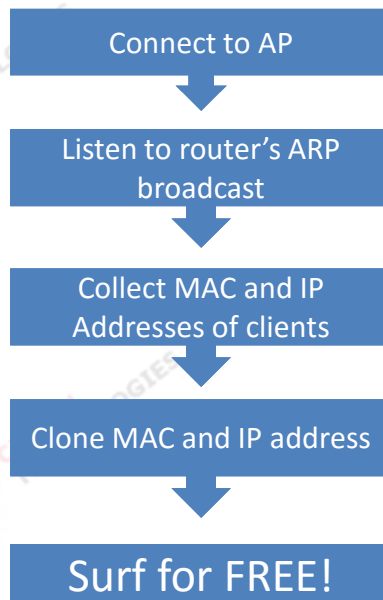




## Type of Attacks

- Piggybacking (the most common form of attack used by freeloaders)

An attack with the intent to use the internet for free, not to steal data or disrupt the system.



**Attackers main objective is to collect the following.**

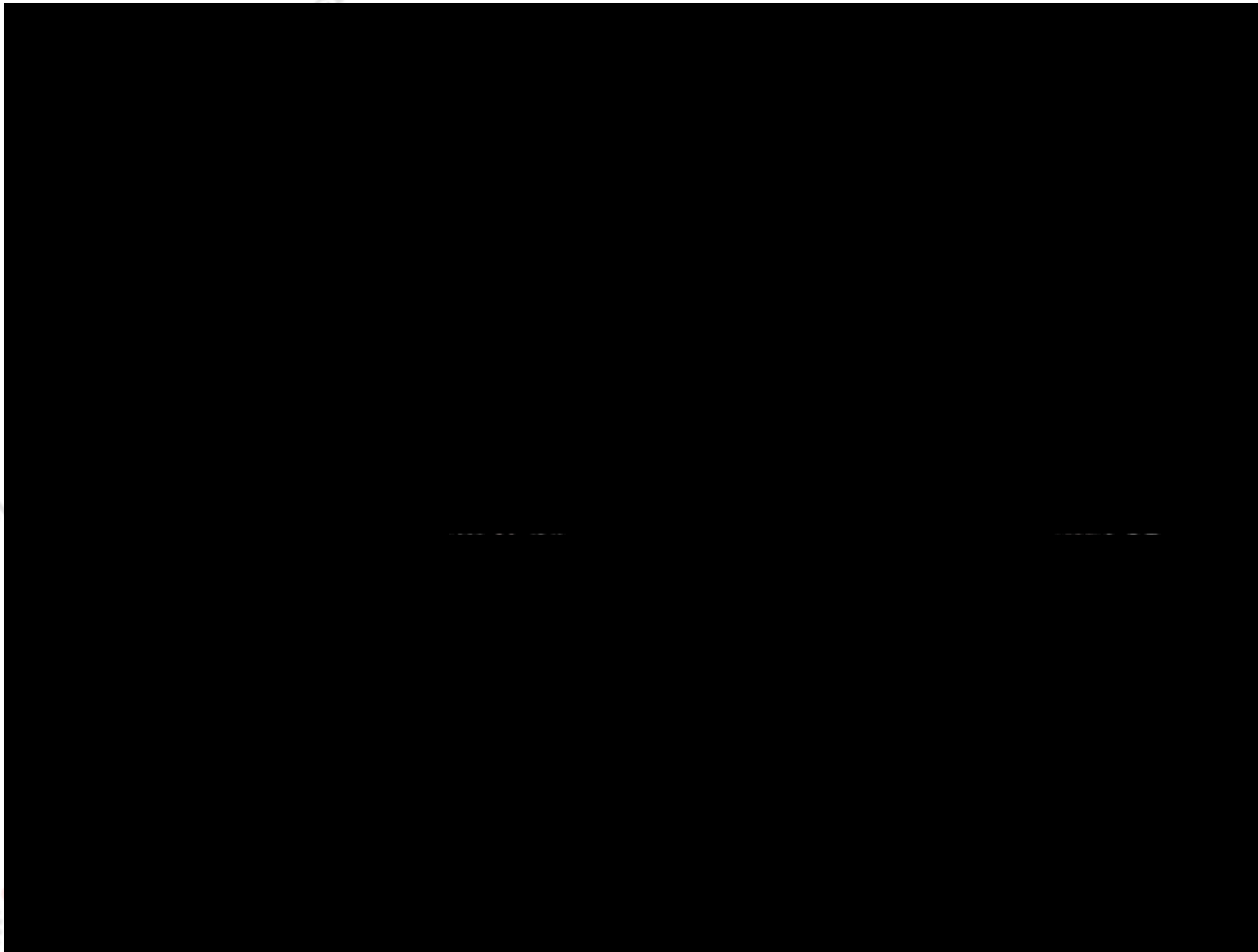
- *MAC Address*
- *IP Address / Subnet*
- *Gateway Address*
- *DHCP and DNS Addresses*

**The topic we will focused on...**

To prevent “attacker/ script kiddies” to clone client MAC and IP address by confusing them with invalid information.



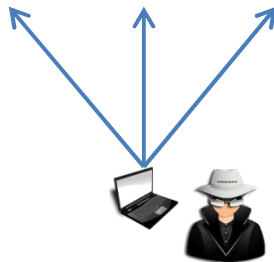
## Piggyback on Mikrotik Hotspot (using Standard Wizard Setup)



# How to secure?

Isolate and contain the network from external access (i.e. secured server room)  
Hide cables or use a conduits.  
Use 802.1x port authentication

## Wired Ethernet



Copper wire

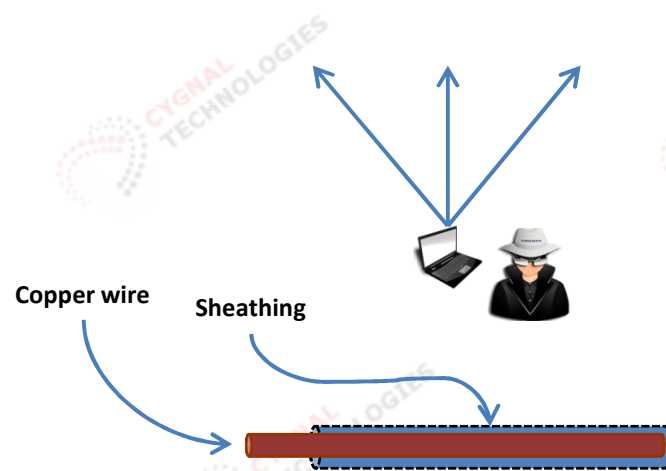


Wired Network is a lot easier to protect from A Direct Attack.

# How to secure?

Isolate and contain the network from external access (i.e. secured server room)  
Hide cables or use a conduits.  
Use 802.1x port authentication

## Wired Ethernet



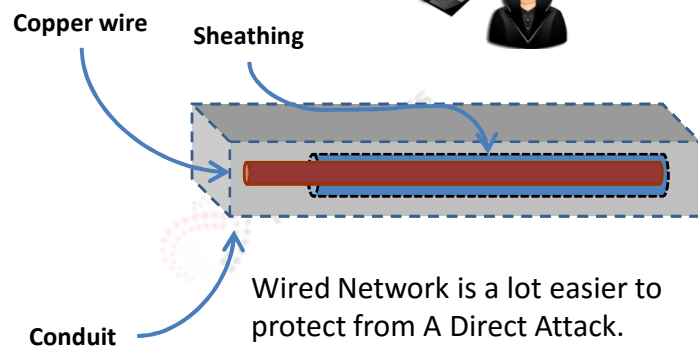
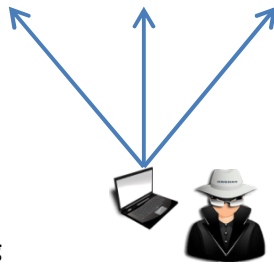
Wired Network is a lot easier to protect from A Direct Attack.



# How to secure?

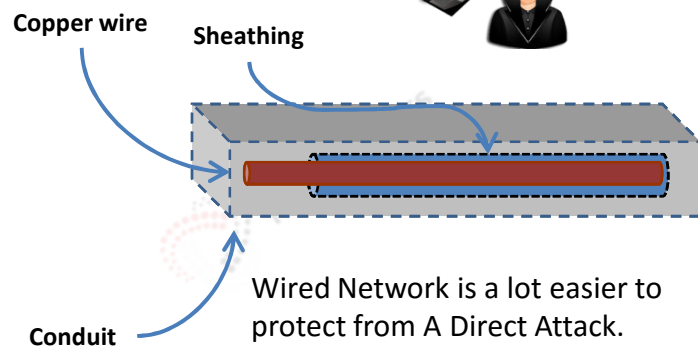
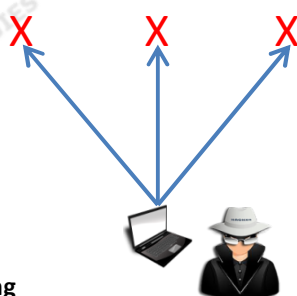
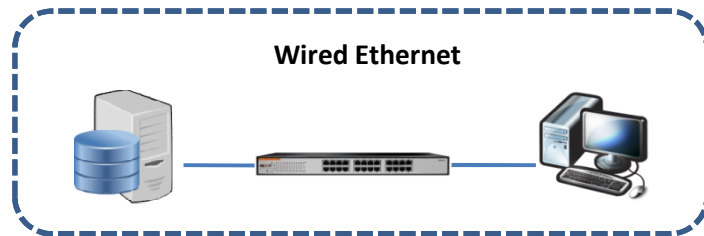
Isolate and contain the network from external access (i.e. secured server room)  
Hide cables or use a conduits.  
Use 802.1x port authentication

## Wired Ethernet



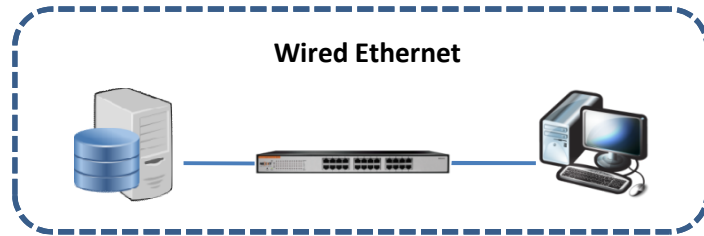
# How to secure?

Isolate and contain the network from external access (i.e. secured server room)  
 Hide cables or use a conduits.  
 Use 802.1x port authentication

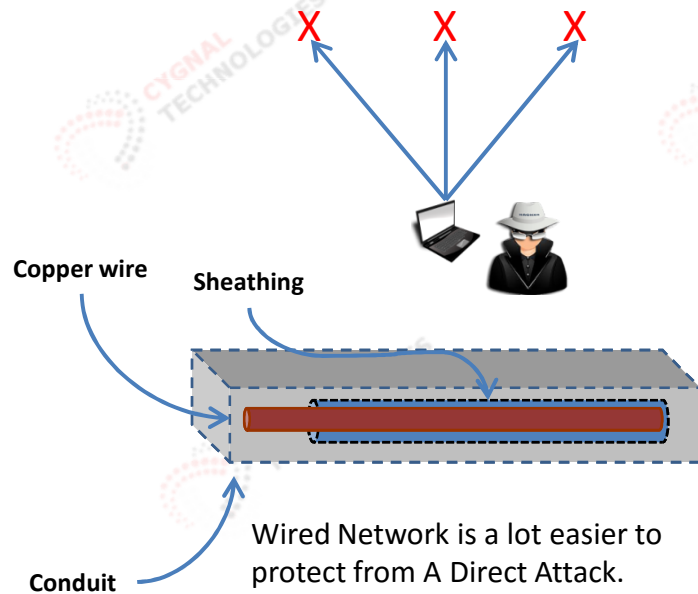
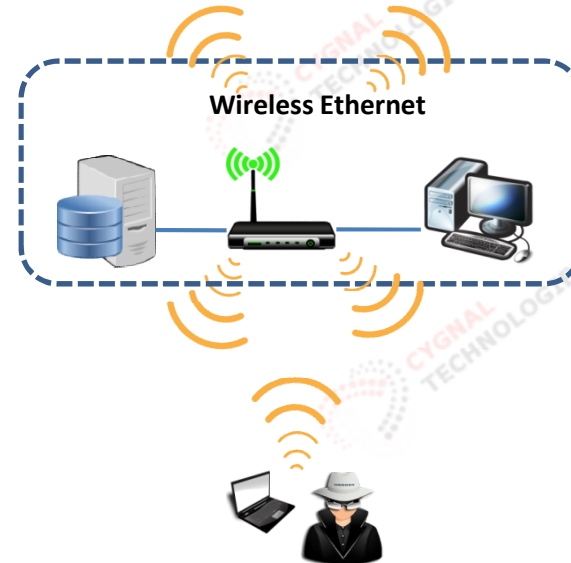


# How to secure?

Isolate and contain the network from external access (i.e. secured server room)  
 Hide cables or use a conduits.  
 Use 802.1x port authentication



Wireless cannot be contained or isolated, as radio waves can pass through walls and obstructions



An open wireless network is 100% vulnerable to all kinds of Direct Attack.

Radio signal do not have a "physical protection" like the sheathing and conduit to protect it, instead, we encapsulate the data with an encryption such as WEP/WPA/WPA2 etc..

# Things to remember!

**Public hotspot is inherently not secured as it must be open for public use.**

WPA/WPA2 and other encryptions cannot be used on Public Hotspot otherwise, the public cannot connect to it without the key.

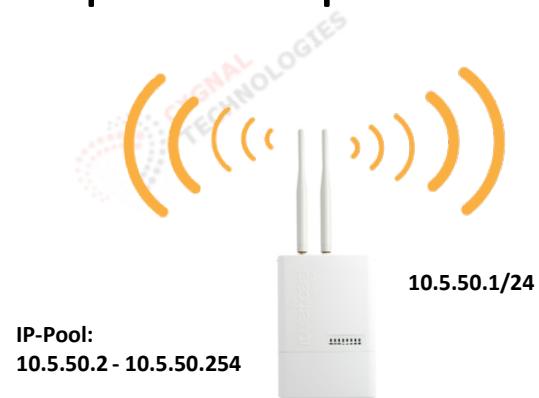
**Mikrotik hotspot "Security" is based on a simple Firewall Rules manipulation and some internal process.**

Rejecting unauthenticated user's IP address with TCP-RESET, ICMP 3:0, 3:1, etc.

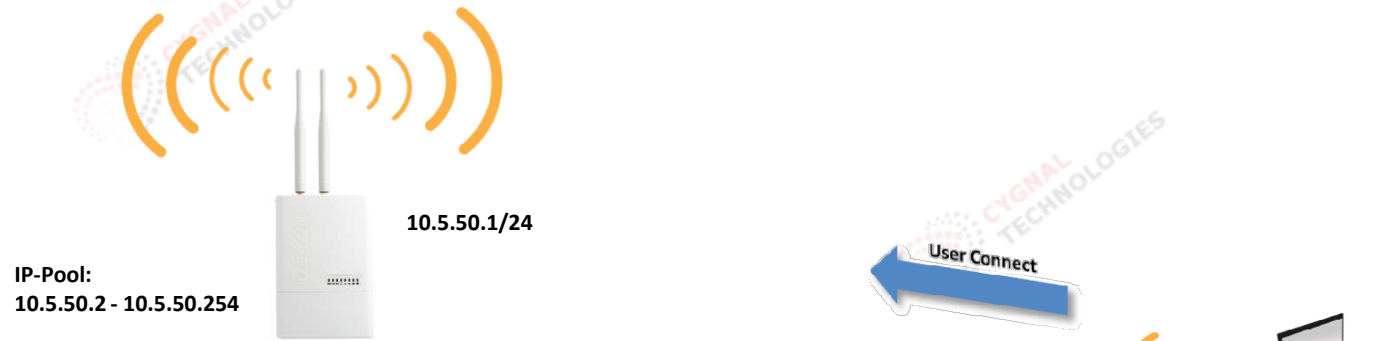
Can be circumvented by ignoring these flags

#	Action	Chain	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Reject With	Bytes	Packets
0 D	jump	forward							54.4 KiB	153
1 D	jump	forward							2785 B	41
2 D	jump	input							42.3 KiB	450
3 D	drop	input	6 (tcp)		64872-64...				0 B	0
4 D	jump	hs-input							42.3 KiB	450
5 D	acc...	hs-input	17 (u...		64872				4356 B	69
6 D	acc...	hs-input	6 (tcp)		64872-64...				38.1 KiB	381
7 D	jump	hs-input							0 B	0
8 D	reject	hs-unauth	6 (tcp)					tcp reset	893 B	17
9 D	reject	hs-unauth						icmp net prohibited	53.5 KiB	136
10 D	reject	hs-unauth-to						icmp host prohibited	2785 B	41

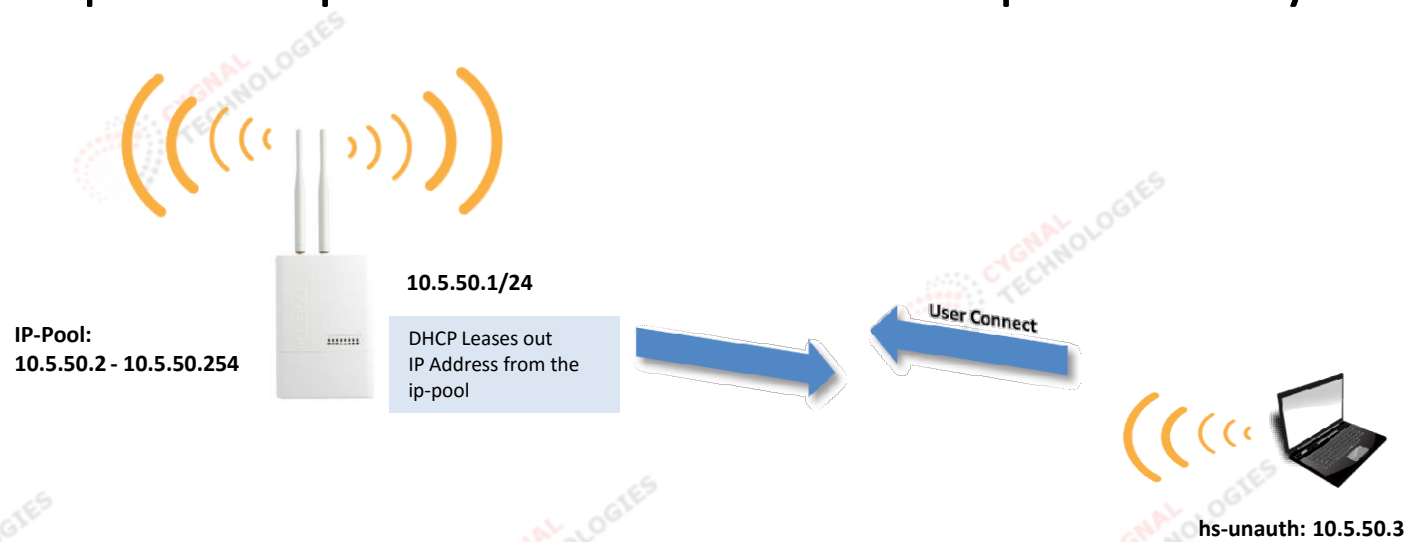
# Simplified explanation of Mikrotik Hotspot Security



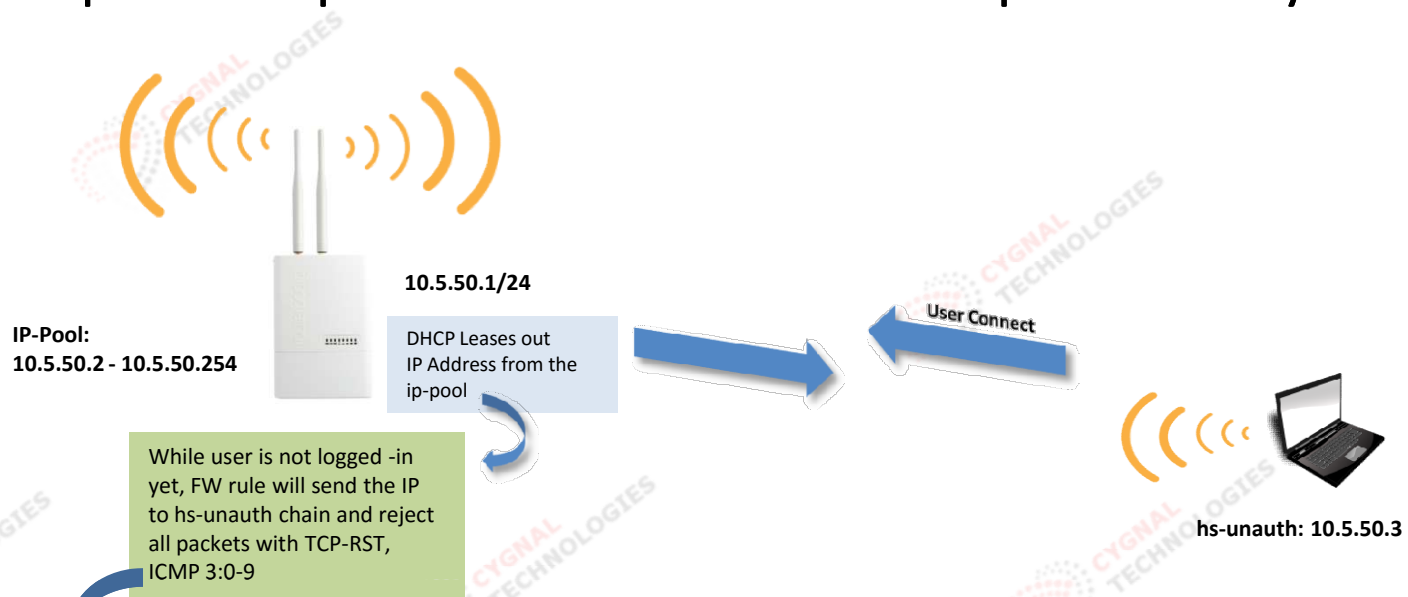
# Simplified explanation of Mikrotik Hotspot Security



# Simplified explanation of Mikrotik Hotspot Security



# Simplified explanation of Mikrotik Hotspot Security



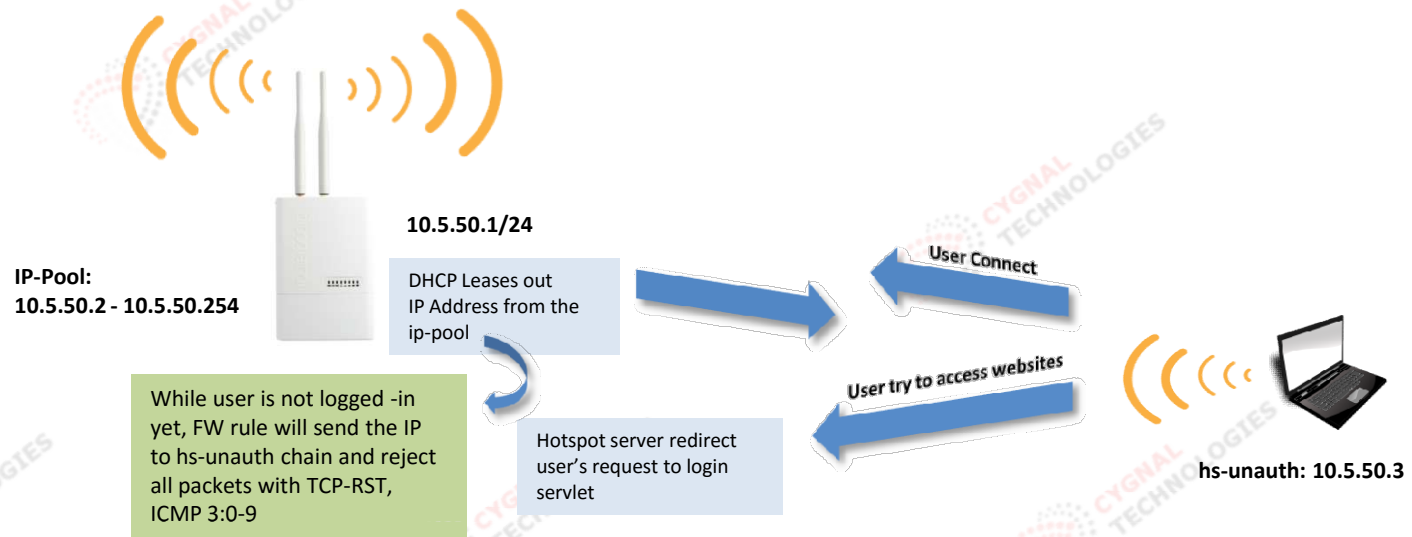
Pinging any sites will result to **Destination net unreachable**

#	Action	Chain	Protocol	Dst. Port	Reject With	Jump Target
0	D jump	forward				hs-unauth
1	D jump	forward				hs-unauth-to
2	D jump	input				hs-input
3	D drop	input	6 (tcp)	64872-64875		
4	D jump	hs-input				pre-hs-input
5	D acc...	hs-input	17 (udp)	64872		
6	D acc...	hs-input	6 (tcp)	64872-64875		
7	D jump	hs-input				hs-unauth
8	D reject	hs-unauth	6 (tcp)		tcp reset	
9	D reject	hs-unauth			icmp net prohibited	
10	D reject	hs-unauth-to			icmp host prohibited	
::: place hotspot rules here						
11	X pas...	unused-hs-c...				

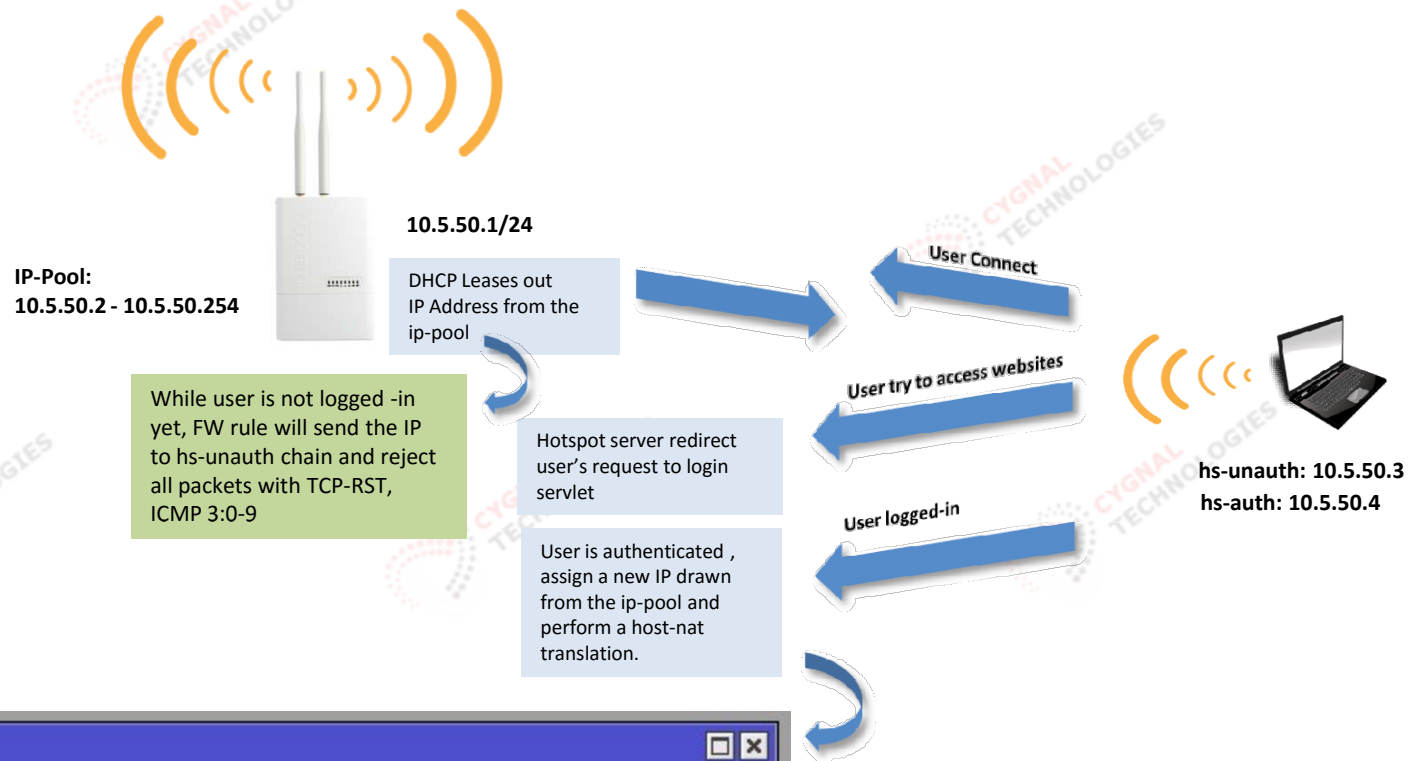
12 items



# Simplified explanation of Mikrotik Hotspot Security



# Simplified explanation of Mikrotik Hotspot Security



Hotspot						
Active	Hosts	IP Bindings	Service Ports	Walled Garden	Walled Garden IP List	...
						Find
	MAC Address	Address	To Address	Server	Idle Time	
H	50:C8:E5:6B:38:3B	10.5.50.2	10.5.50.2	hs-server	00:01:49	
A	B4:6D:83:F1:48:61	10.5.50.3	10.5.50.4	hs-server	00:00:11	
2 items						

*With Mikrotik Standard hotspot wizard setup, the hs-unauth and hs-auth IP addresses will be drawn from the same ip pool of 10.5.50.0/24.*

*By default, the entire subnet is masqueraded*

## Why with the concern?

- Philippine is fairly new to Hotspot service, especially using Mikrotik products, most new comers to Mikrotik hotspot are unaware of its security issues.
- Many Hotspot Operators are not Technical knowledgeable in networking
- Even I.T professionals who are new to Mikrotik Hotspot are not aware of its vulnerabilities
- Any opened wireless network is vulnerable to all kinds of attacks and it can compromise end user's sensitive information and it can also lead to legal problems between the users and hotspot operators.
- Anyone can freely use and abuse your Hotspot without you knowing it. (especially at night when you are not monitoring) 😊

## What the “IP masking” can and can’t do

- Cannot protect you from all known Passive and Active Attacks
  - Cannot stop attackers from MAC cloning and Piggybacking
-

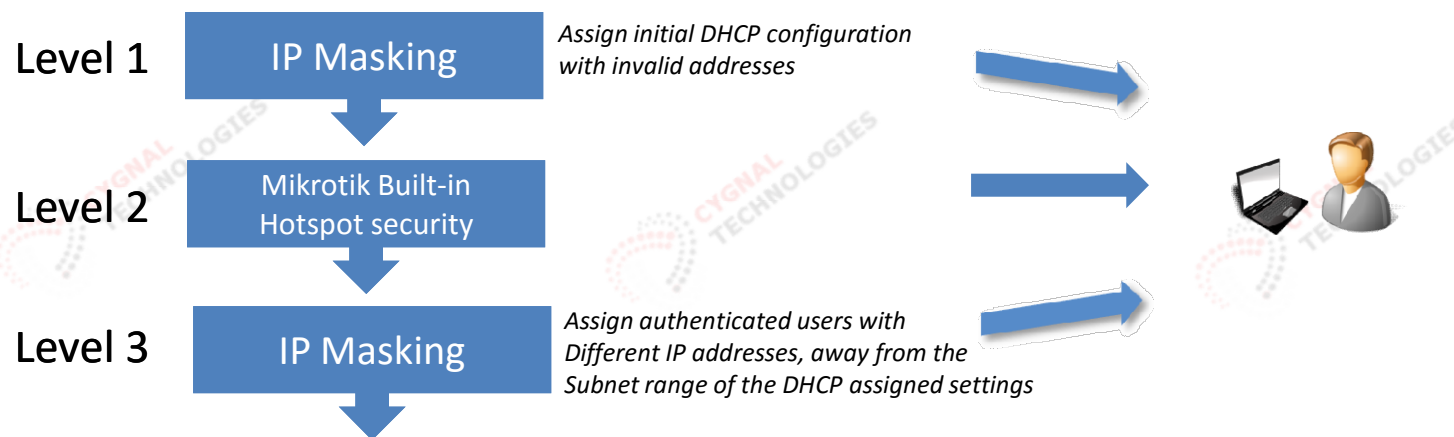
## What the “IP masking” can and can’t do

- Cannot protect you from all known Passive and Active Attacks
  - Cannot stop attackers from MAC cloning and Piggybacking
- 
- Can make harder for attackers to figure-out your network layout, therefore; piggy backing is “twice as harder” to perform.
  - Can give you extra layer of defense aside from the built-in “security”
  - Can make network professionals scratched their heads when they see how you assign IP addresses to your clients. 😊

# What the “IP masking” can and can’t do

- Cannot protect you from all known Passive and Active Attacks
- Cannot stop attackers from MAC cloning and Piggybacking

- Can make harder for attackers to figure-out your network layout therefore, piggy backing is “twice as harder” to perform.
- Can give you extra layer of defense aside from the built-in “security”
- Can make network professionals scratched their heads when they see how you assign IP addresses to your clients. 😊



## The solution

My solution is based on “*Misdirection*”, this solution is **NOT 100%** fool-proof but sufficient enough to keep “wannabee hackers”, “script kiddies”, and someone who has little knowledge of networking at bay, this could also make I.T professionals to scratch their heads when they see the IP addresses.

*An opened Wireless AP cannot be protected at all, a series of Firewall rules and Redirections is the **\*only\*** way to “prevent” unauthorized users from using the hotspot service which can be easily circumvented.*

*I called this solution as “**IP hotspot Masking**”, The idea is, we hide information as much as we could by providing the end users with false and invalid IP addresses and gateway address, hence; the “**masking**”, thus; it will create confusion and misdirection.*

## The solution

My solution is based on “*Misdirection*”, this solution is **NOT 100%** fool-proof but sufficient enough to keep “wannabee hackers”, “script kiddies”, and someone who has little knowledge of networking at bay, this could also make I.T professionals to scratch their heads when they see the IP addresses.

*An opened Wireless AP cannot be protected at all, a series of Firewall rules and Redirections is the \*only\* way to “prevent” unauthorized users from using the hotspot service which can be easily circumvented.*

*I called this solution as “**IP hotspot Masking**”, The idea is, we hide information as much as we could by providing the end users with false and invalid IP addresses and gateway address, hence; the “**masking**”, thus; it will create confusion and misdirection.*

Is this a correct format?

IP Address: **10.5.50.253**

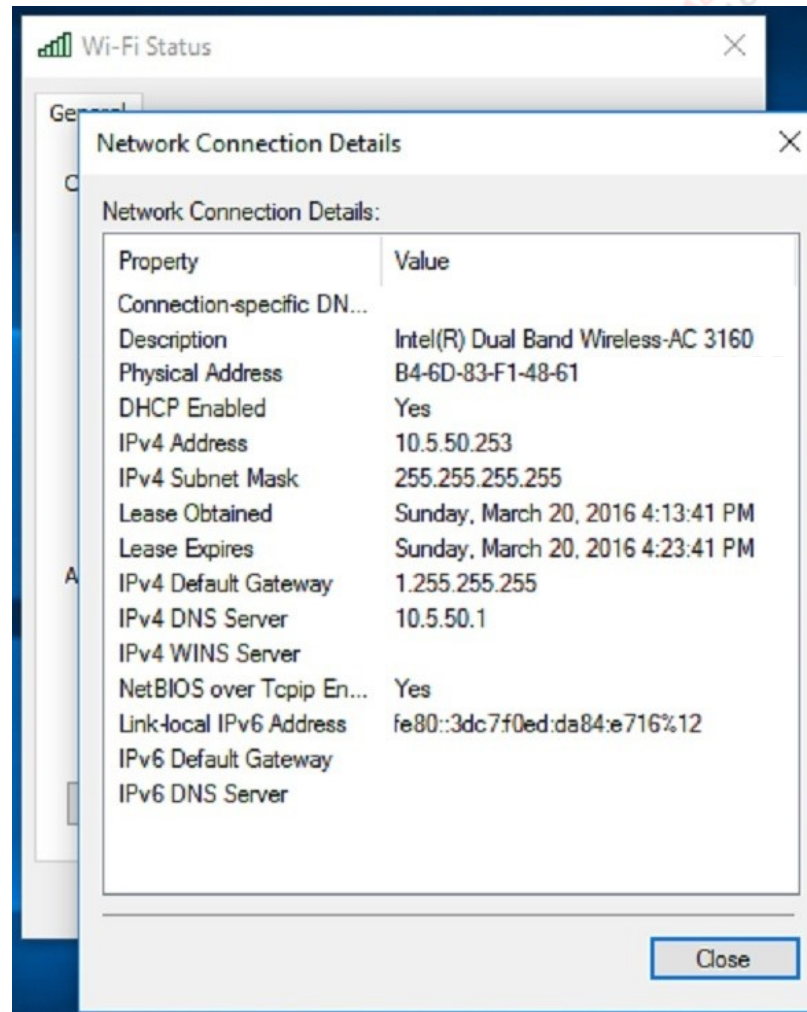
Subnet Mask: **255.255.255.255**

Gateway: **1.255.255.255**



## The solution

My solution is based on “*Misdirection*”, this solution is **NOT 100%** fool-proof but sufficient enough to keep “wannabee hackers”, “script kiddies”, and someone who has little knowledge of networking at bay, this could also make I.T professionals to scratch their heads when they see the IP addresses.



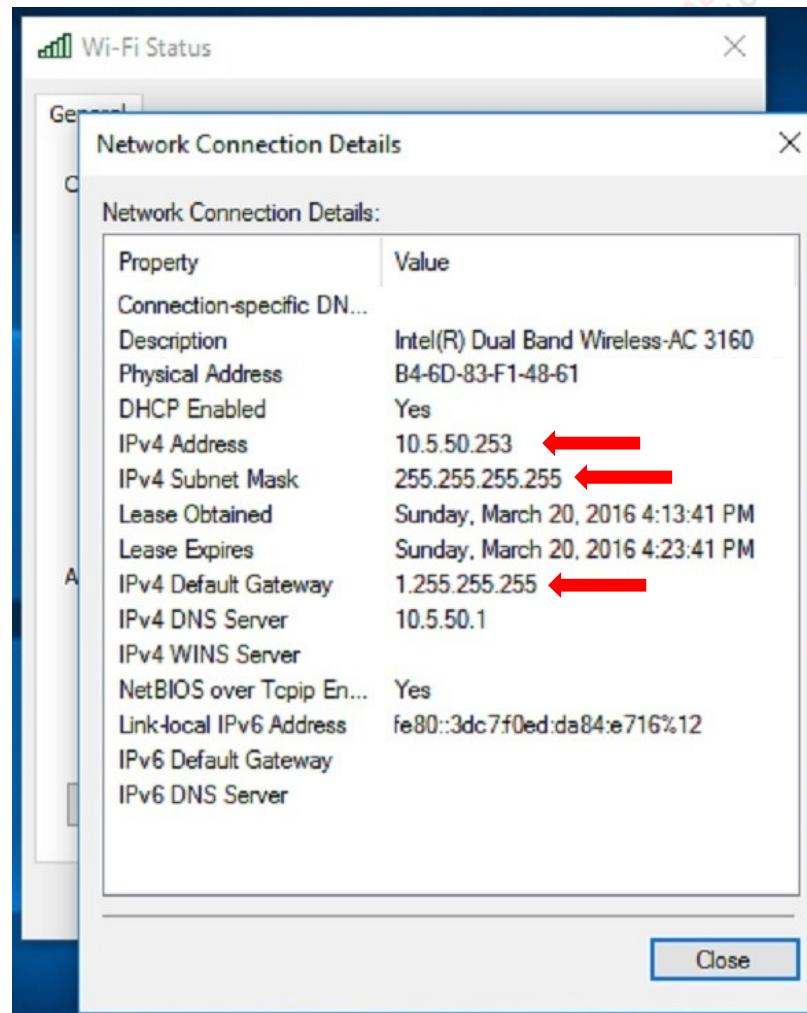
# The solution

My solution is based on “*Misdirection*”, this solution is **NOT 100%** fool-proof but sufficient enough to keep “wannabee hackers”, “script kiddies”, and someone who has little knowledge of networking at bay, this could also make I.T professionals to scratch their heads when they see the IP addresses.

Lease out an Invalid Subnet and Gateways

### Networking 101:

- Taught us that gateway and IP Address must be on the same subnet.
- Last octet of the IP Address and Gateway cannot be set to all 1's (255)



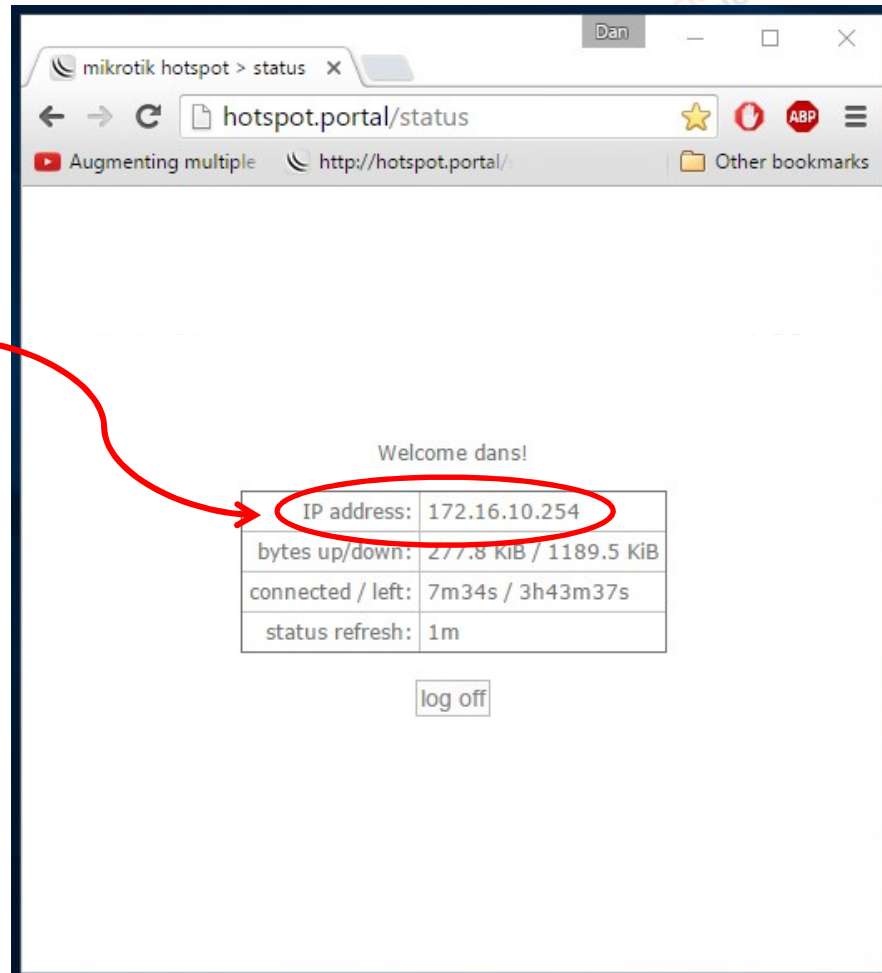
# The solution

My solution is based on “*Misdirection*”, this solution is **NOT 100%** fool-proof but sufficient enough to keep “wannabee hackers”, “script kiddies”, and someone who has little knowledge of networking at bay, this could also make I.T professionals to scratch their heads.

Give-out a “hidden routable IP addresses” to hotspot authenticated users.

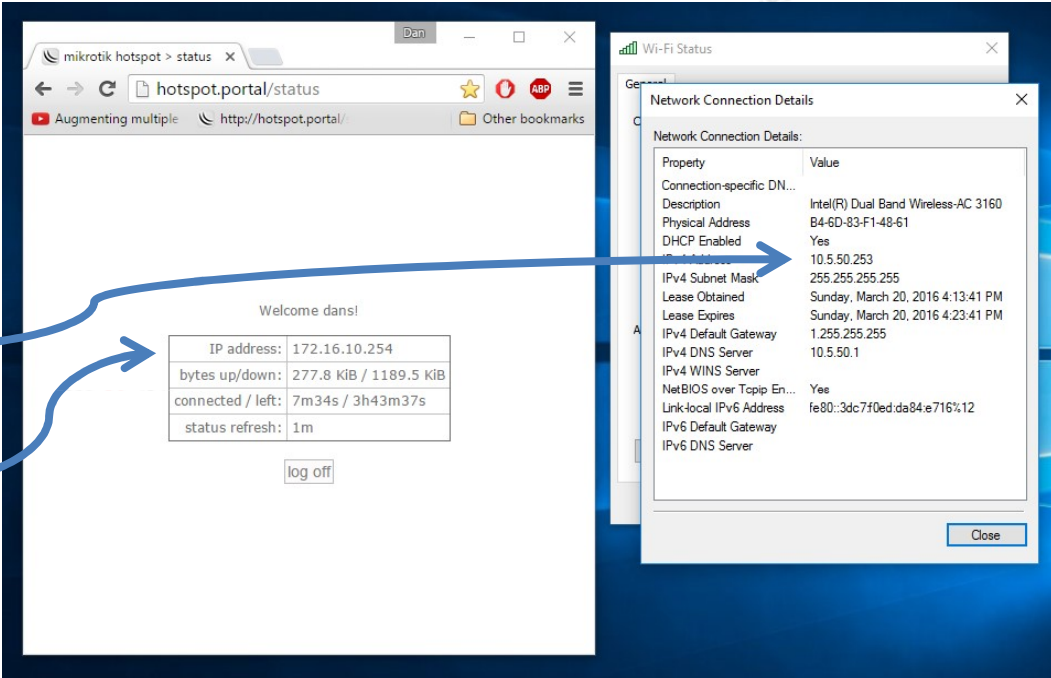
We can edit the `status.html` file and remove the IP address.

The IP address is a dead-give away of the network layout and the possible gateway address.



# The solution

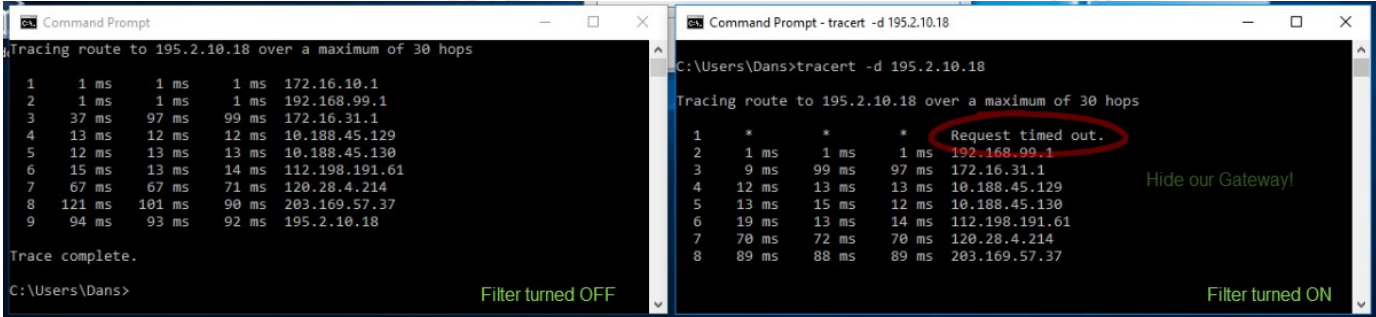
My solution is based on “Misdirection”, this solution is **NOT 100%** fool-proof but sufficient enough to keep “wannabee hackers”, “script kiddies”, and someone who has little knowledge of networking at bay, this could also make I.T professionals to scratch their heads.



Lease out an Invalid Subnet and Gateways

Give-out a “hidden routable IP addresses” to hotspot authenticated users.

Property	Value
Connection-specific DN...	
Description	Intel(R) Dual Band Wireless-AC 3160
Physical Address	B4-6D-83-F1-48-61
DHCP Enabled	Yes
IP Address	10.5.50.253
IPv4 Subnet Mask	255.255.255.255
Lease Obtained	Sunday, March 20, 2016 4:13:41 PM
Lease Expires	Sunday, March 20, 2016 4:23:41 PM
IPv4 Default Gateway	1.255.255.255
IPv4 DNS Server	10.5.50.1
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	fe80::3dc710ed.da84e716%12
IPv6 Default Gateway	
IPv6 DNS Server	



Remove any footprint of router/ gateway addresses

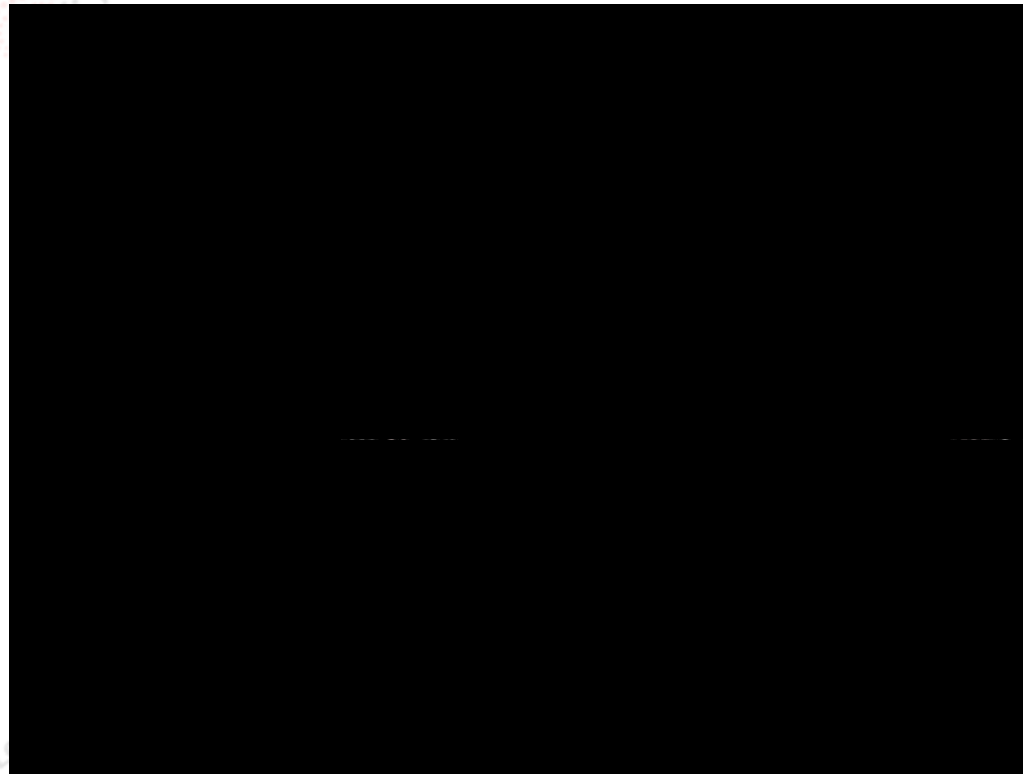
```

C:\Users\Dans>tracert -d 195.2.10.18
Tracing route to 195.2.10.18 over a maximum of 30 hops:
 0  0 ms  0 ms  0 ms  192.168.99.1
 1  1 ms  1 ms  1 ms  172.16.10.1
 2  1 ms  1 ms  1 ms  192.168.99.1
 3  37 ms  97 ms  99 ms  172.16.31.1
 4  13 ms  12 ms  12 ms  10.188.45.129
 5  12 ms  13 ms  13 ms  10.188.45.130
 6  15 ms  13 ms  14 ms  112.198.191.61
 7  67 ms  67 ms  71 ms  120.28.4.214
 8  121 ms  101 ms  90 ms  203.169.57.37
 9  94 ms  93 ms  92 ms  195.2.10.18
Trace complete.
C:\Users\Dans>
Filter turned OFF
    
```

```

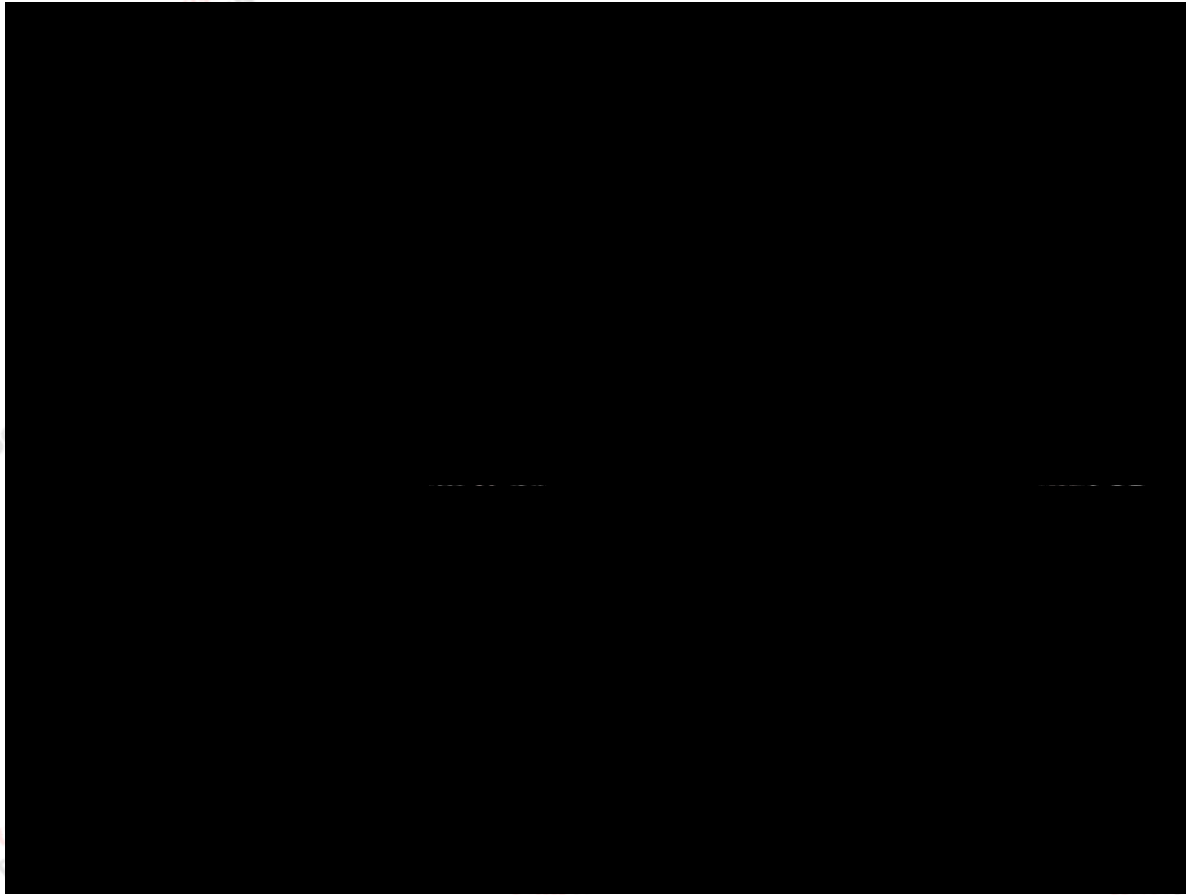
C:\Users\Dans>tracert -d 195.2.10.18
Tracing route to 195.2.10.18 over a maximum of 30 hops:
 0  * * * 192.168.99.1
 1  1 ms  1 ms  1 ms  172.16.31.1
 2  9 ms  99 ms  97 ms  172.16.31.1
 3  12 ms  13 ms  13 ms  10.188.45.129
 4  13 ms  15 ms  12 ms  10.188.45.130
 5  19 ms  13 ms  14 ms  112.198.191.61
 6  70 ms  72 ms  70 ms  120.28.4.214
 7  89 ms  88 ms  89 ms  203.169.57.37
 8  * * * Request timed out.
Trace complete.
C:\Users\Dans>
Filter turned ON
    
```

# IP Hotspot Masking





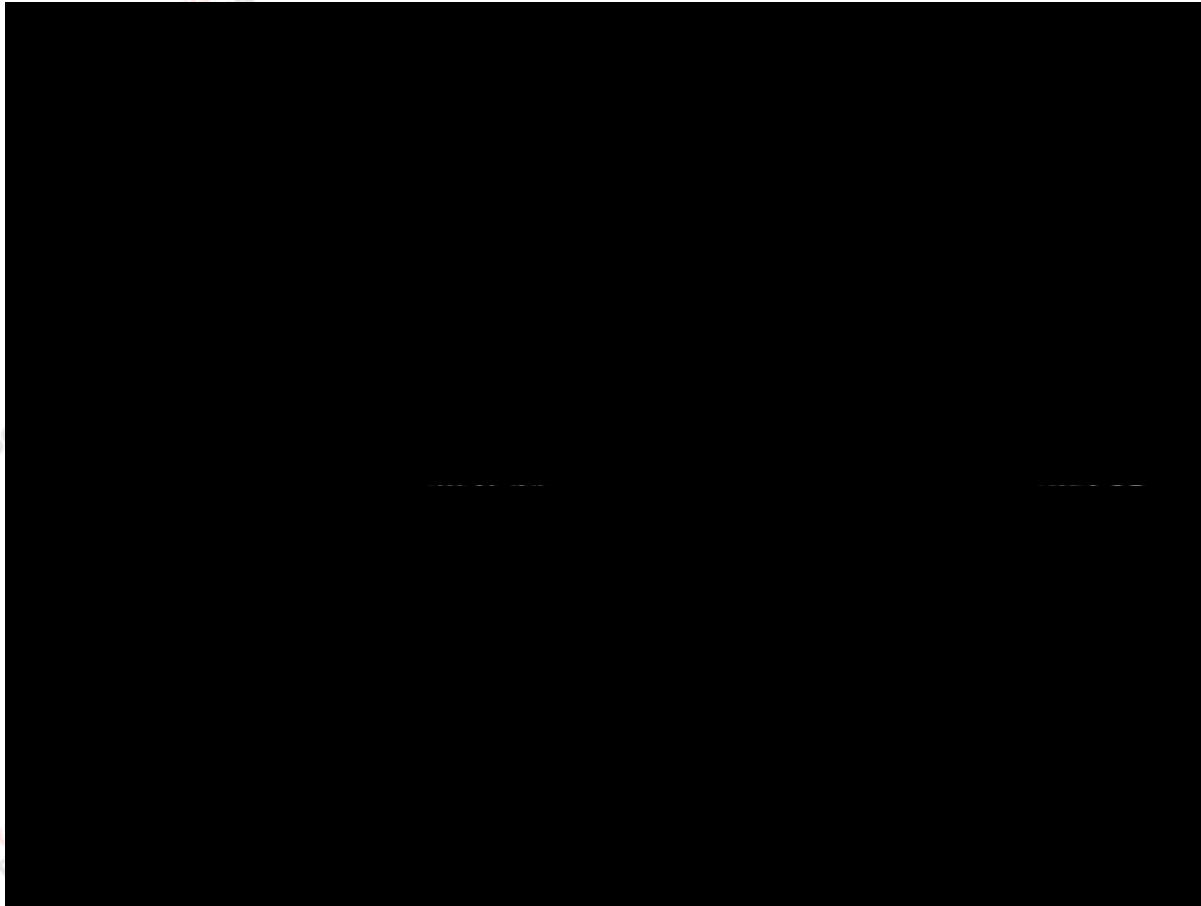
Leave no trace!







# More hiding



# IP Masking Configuration

The title "IP Masking Configuration" is centered on the page. The word "Masking" is followed by a black icon of a wrench and a pencil crossed at their handles. The word "Configuration" follows the icon.

# Configuration (Interface and IP Addresses)

RESET the RouterBoard without  
default configuration

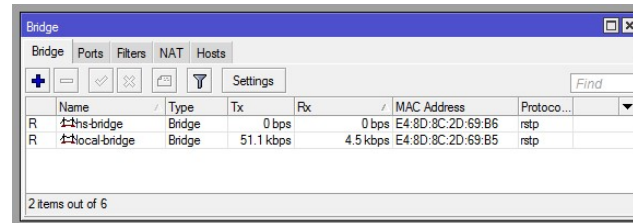


# Configuration (Interface and IP Addresses)

RESET the RouterBoard without default configuration



Create a bridge interface

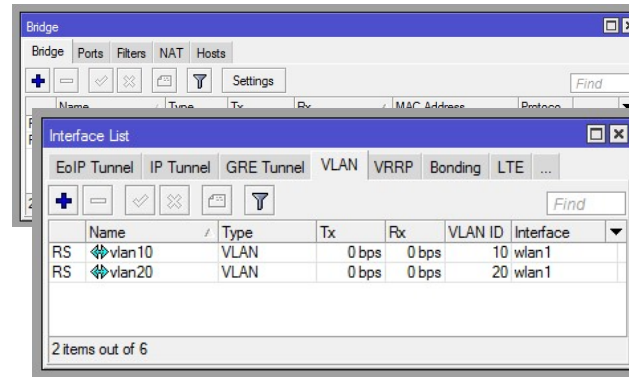
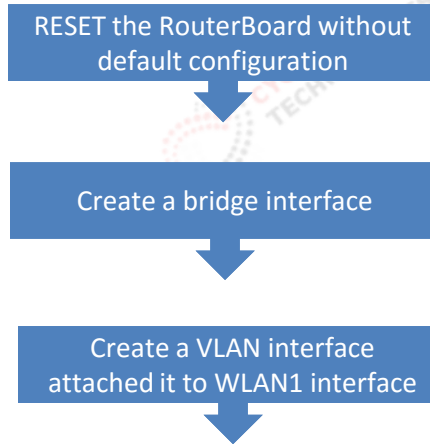
Name	Type	Tx	Rx	MAC Address	Protoco...
lan-bridge	Bridge	0 bps	0 bps	E4:8D:8C:2D:69:B6	rstp
local-bridge	Bridge	51.1 kbps	4.5 kbps	E4:8D:8C:2D:69:B5	rstp

2 items out of 6

*2 Bridge interface for the LAN and Hotspot*



# Configuration (Interface and IP Addresses)

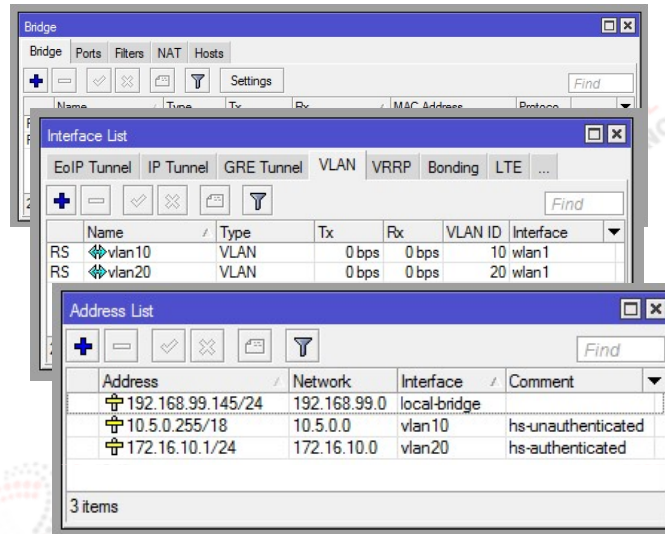
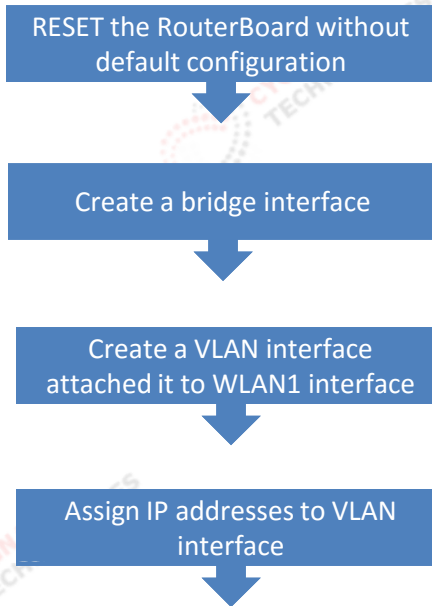


*2 Bridge interface for the LAN and Hotspot*

*The VLAN will only act as a dummy interface to hold the IP addresses for hs-unauthenticated and hs-authenticated*



# Configuration (Interface and IP Addresses)

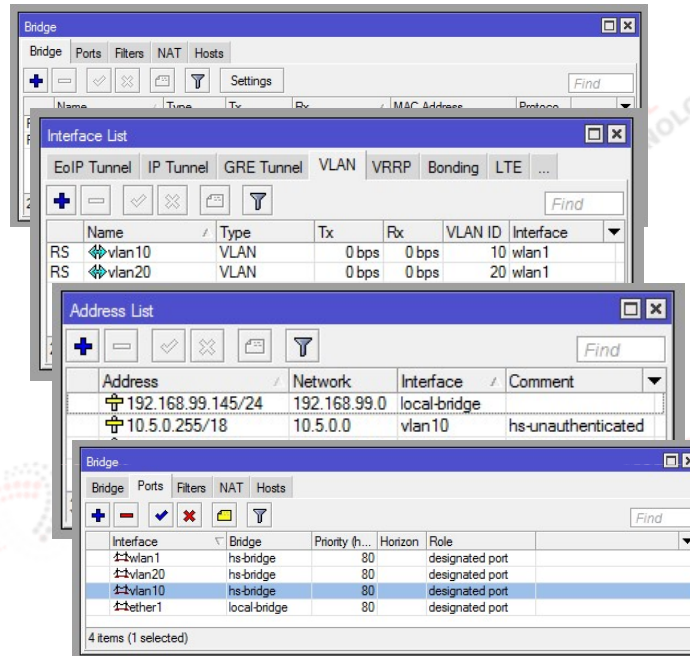
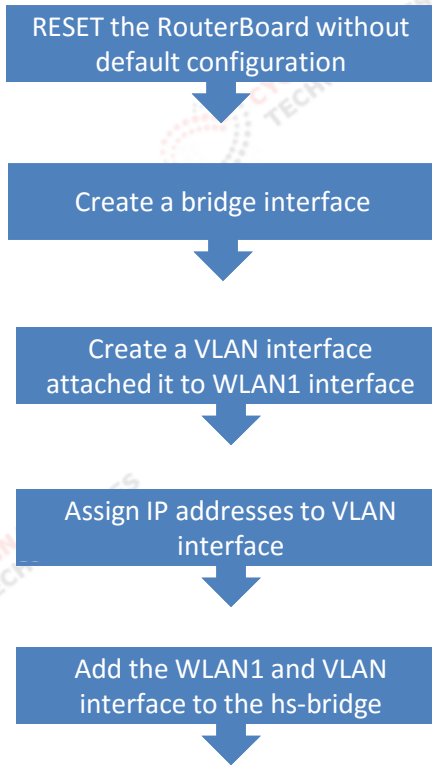


*2 Bridge interface for the LAN and Hotspot*

*The VLAN will only act as a dummy interface to hold the IP addresses for hs-unauthenticated and hs-authenticated*

*Assign your own IP for the LAN and VLAN, **DO NOT** assign any IP to hs-bridge.*

# Configuration (Interface and IP Addresses)

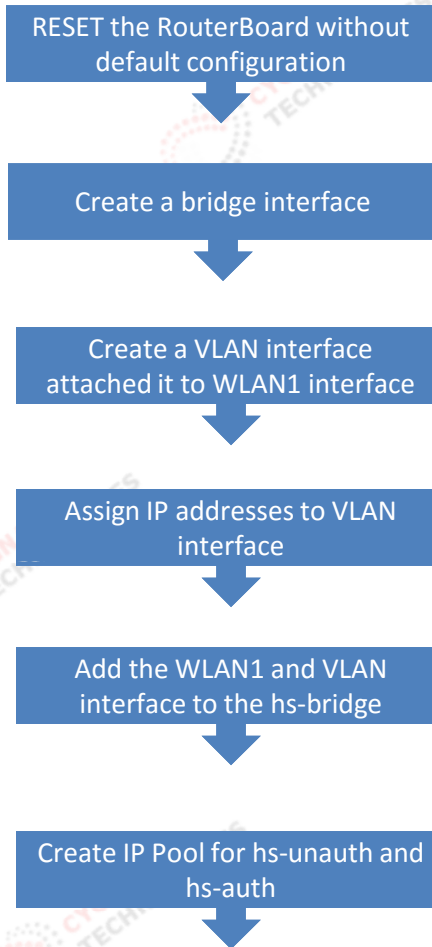
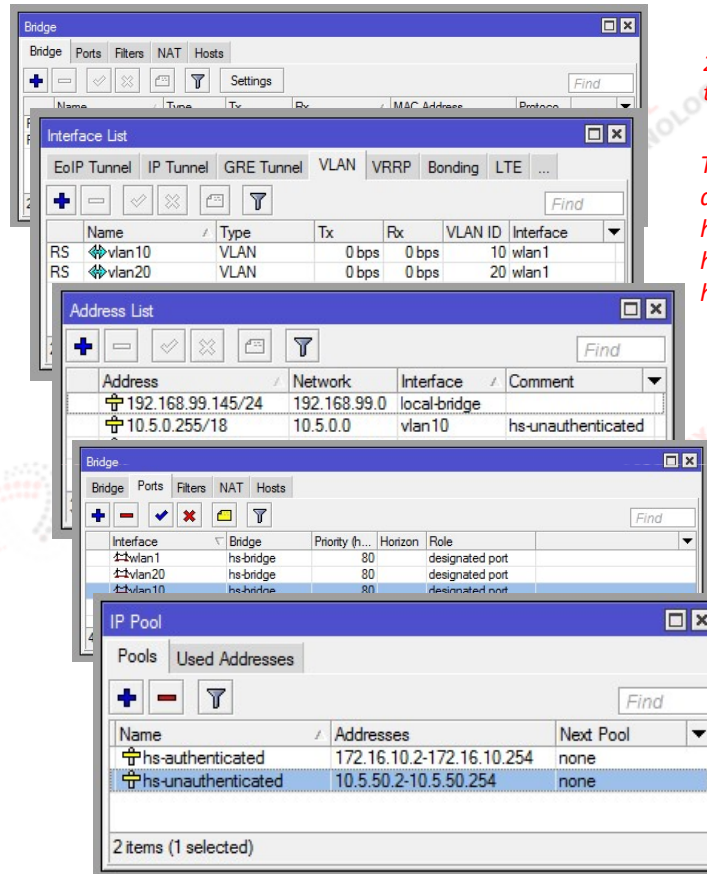


*2 Bridge interface for the LAN and Hotspot*

*The VLAN will only act as a dummy interface to hold the IP addresses for hs-unauthenticated and hs-authenticated*

*Assign your own IP for the LAN and VLAN, DO NOT assign any IP to hs-bridge.*

# Configuration (Interface and IP Addresses)

The screenshots show the following configurations:

- Bridge:** Shows a bridge interface named 'hs-bridge' with ports 'wlan1', 'vlan20', and 'vlan10'.
- Interface List:** Shows VLAN interfaces 'vlan10' and 'vlan20' attached to 'wlan1'.
- Address List:** Shows IP addresses assigned to the bridge and VLAN10:
 

Address	Network	Interface	Comment
192.168.99.145/24	192.168.99.0	local-bridge	
10.5.0.255/18	10.5.0.0	vlan10	hs-unauthenticated
- Bridge (Ports):** Shows 'wlan1', 'vlan20', and 'vlan10' as designated ports of the 'hs-bridge'.
- IP Pool:** Shows two pools: 'hs-authenticated' (172.16.10.2-172.16.10.254) and 'hs-unauthenticated' (10.5.50.2-10.5.50.254).

*2 Bridge interface for the LAN and Hotspot*

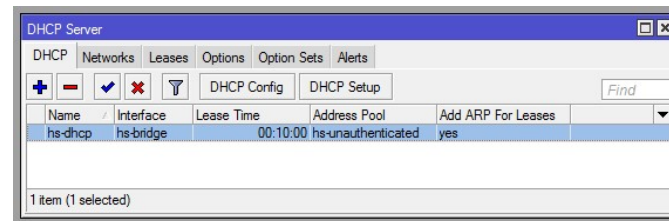
*The VLAN will only act as a dummy interface to hold the IP addresses for hs-unauthenticated and hs-authenticated*

*Assign your own IP for the LAN and VLAN, DO NOT assign any IP to hs-bridge.*



# Configuration (DHCP and DNS Settings)

Create a DHCP server BINDED to the hs-bridge interface



Name	Interface	Lease Time	Address Pool	Add ARP For Leases
hs-dhcp	hs-bridge	00:10:00	hs-unauthenticated	yes

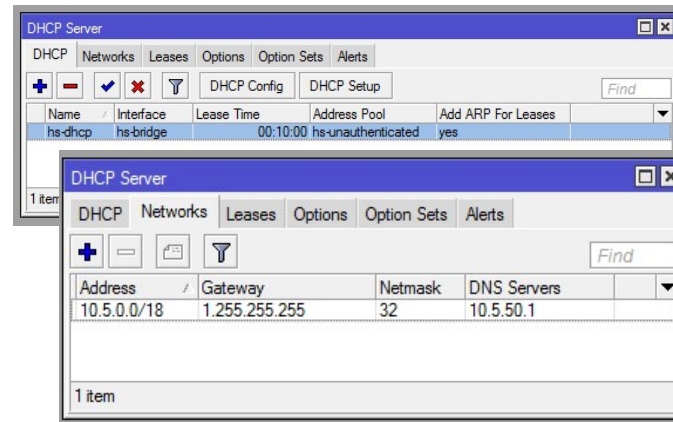
Select the hs-unauthenticated IP Pool the hs-unauthenticated pool will be handed out to all hotspot clients.

# Configuration (DHCP and DNS Settings)

Create a DHCP server BINDED to the hs-bridge interface



Set the Network Settings for DHCP



Select the hs-unauthenticated IP Pool the hs-unauthenticated pool will be handed out to all hotspot clients.

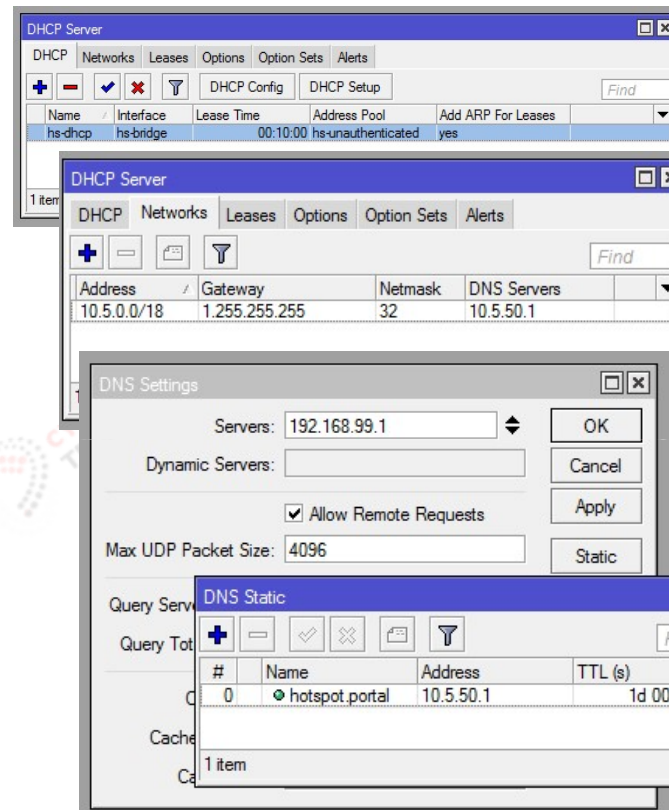
With the gateway, you can put anything here. Better to put something invalid, please note of the Netmask to set to 32

# Configuration (DHCP and DNS Settings)

Create a DHCP server BINDED to the hs-bridge interface

Set the Network Settings for DHCP

Set the DNS to allow request and create a static DNS entry



The image shows four overlapping screenshots from Mikrotik WinBox:

- DHCP Server:** Shows a table with one entry:
 

Name	Interface	Lease Time	Address Pool	Add ARP For Leases
hs-dhcp	hs-bridge	00:10:00	hs-unauthenticated	yes
- DHCP Setup:** Shows network settings:
 

Address	Gateway	Netmask	DNS Servers
10.5.0.0/18	1.255.255.255	32	10.5.50.1
- DNS Settings:** Shows 'Servers' set to 192.168.99.1, 'Allow Remote Requests' checked, and 'Max UDP Packet Size' set to 4096.
- DNS Static:** Shows a table with one static entry:
 

#	Name	Address	TTL (s)
0	hotspot.portal	10.5.50.1	1d 00:00:00

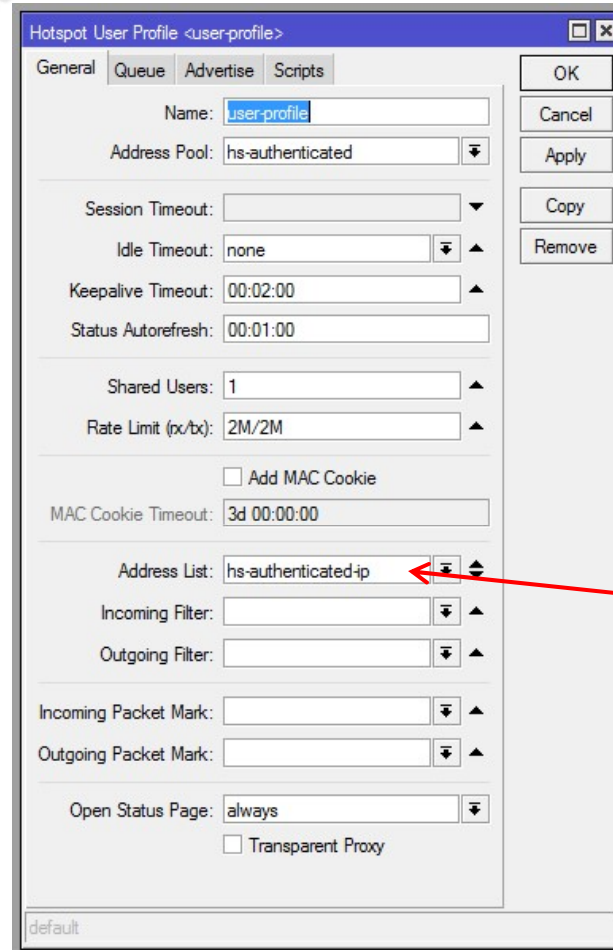
Select the hs-unauthenticated IP Pool the hs-unauthenticated pool will be handed out to all hotspot clients.

With the gateway, you can put anything here. Better to put something invalid, please note of the Netmask to set to 32

The static DNS entry hotspot.portal is what will appear in the URL bar

# Configuration (Hotspot Server Settings)

Create a User Profile

Hotspot User Profile <user-profile>

General Queue Advertise Scripts

Name: user-profile

Address Pool: hs-authenticated

Session Timeout: [dropdown]

Idle Timeout: none

Keepalive Timeout: 00:02:00

Status Autorefresh: 00:01:00

Shared Users: 1

Rate Limit (rx/bx): 2M/2M

Add MAC Cookie

MAC Cookie Timeout: 3d 00:00:00

Address List: hs-authenticated-ip

Incoming Filter: [dropdown]

Outgoing Filter: [dropdown]

Incoming Packet Mark: [dropdown]

Outgoing Packet Mark: [dropdown]

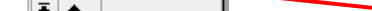
Open Status Page: always

Transparent Proxy

OK Cancel Apply Copy Remove

At the user Profile, use the hs-authenticated pool, this pool will be assigned to users who passed the authentication, If you use usermanager, you can insert it at the IP-POOL field

Insert the hs-authenticated-ip at the address list, it will be used for NAT purpose.



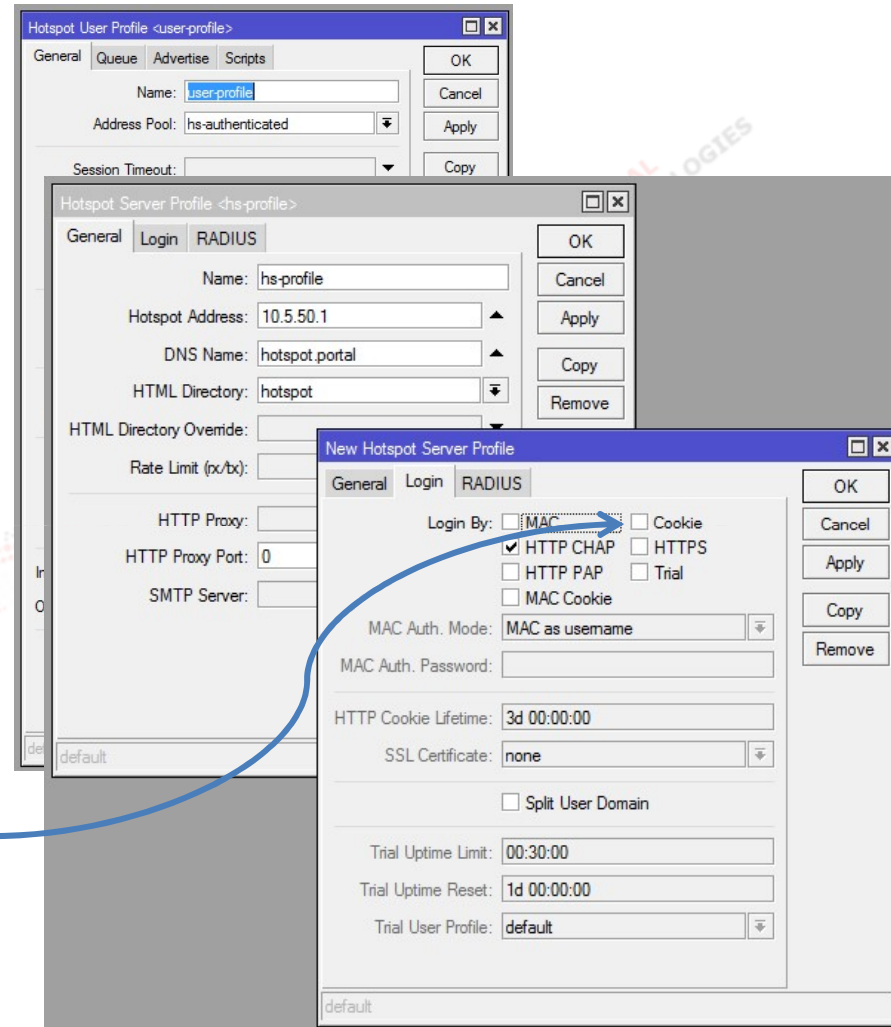
# Configuration (Hotspot Server Settings)

Create a User Profile

Create Hotspot Server Profile

*Cookie is used to allow mobile/tablet users to be logged-in automatically without entering the username and password, when the cookie is checked, mobile users do not need to re-login again until the cookie lifetime expires.*

*I recommend to unchecked it, as it can pose a problem, let the mobile users to be logged-out automatically when idle in a certain amount of time.*



# Configuration (Hotspot Server Settings)

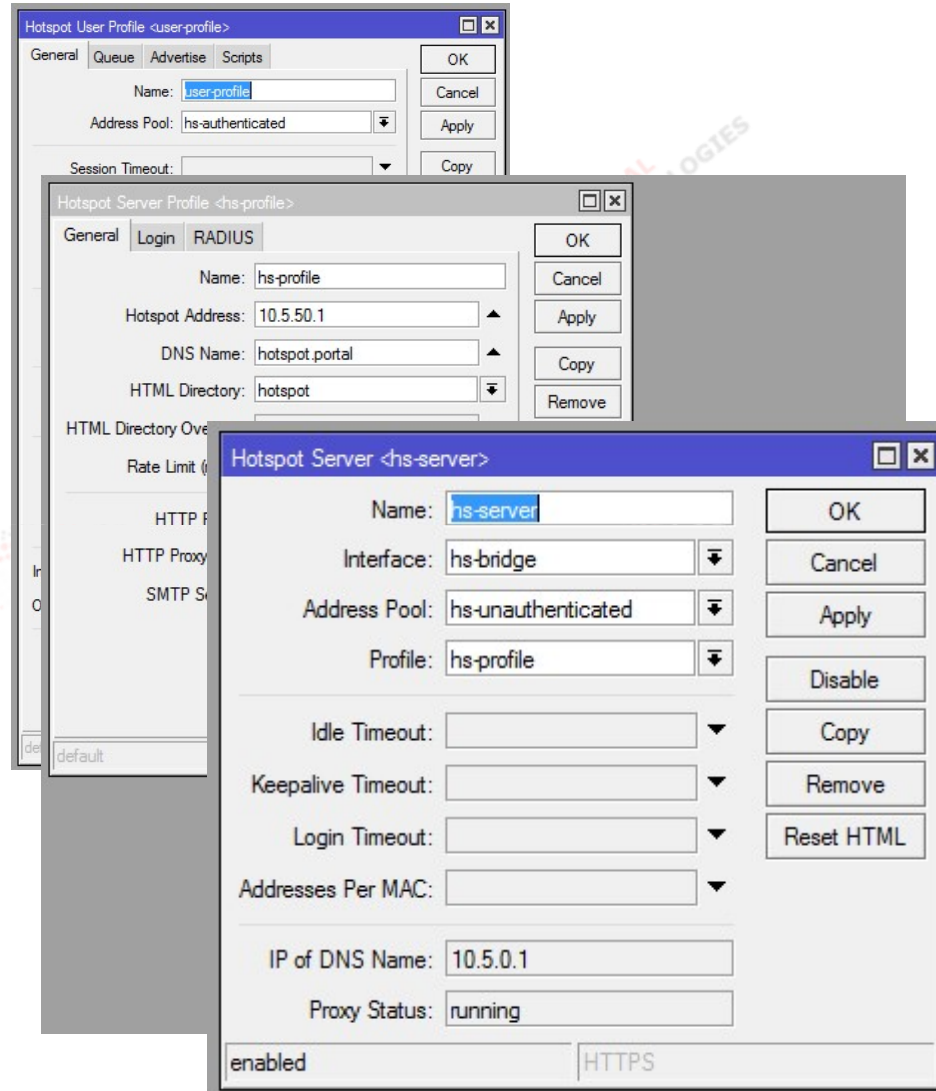
Create a User Profile



Create Hotspot Server Profile



Enable Hotspot Server

The image shows three overlapping configuration windows from a network management interface:

- Hotspot User Profile <user-profile>**: Shows the 'General' tab with fields for Name (user-profile), Address Pool (hs-authenticated), and Session Timeout.
- Hotspot Server Profile <hs-profile>**: Shows the 'RADIUS' tab with fields for Name (hs-profile), Hotspot Address (10.5.50.1), DNS Name (hotspot.portal), and HTML Directory (hotspot).
- Hotspot Server <hs-server>**: Shows configuration for the server, including Name (hs-server), Interface (hs-bridge), Address Pool (hs-unauthenticated), Profile (hs-profile), Idle Timeout, Keepalive Timeout, Login Timeout, Addresses Per MAC, IP of DNS Name (10.5.0.1), Proxy Status (running), and a checkbox for 'enabled'.

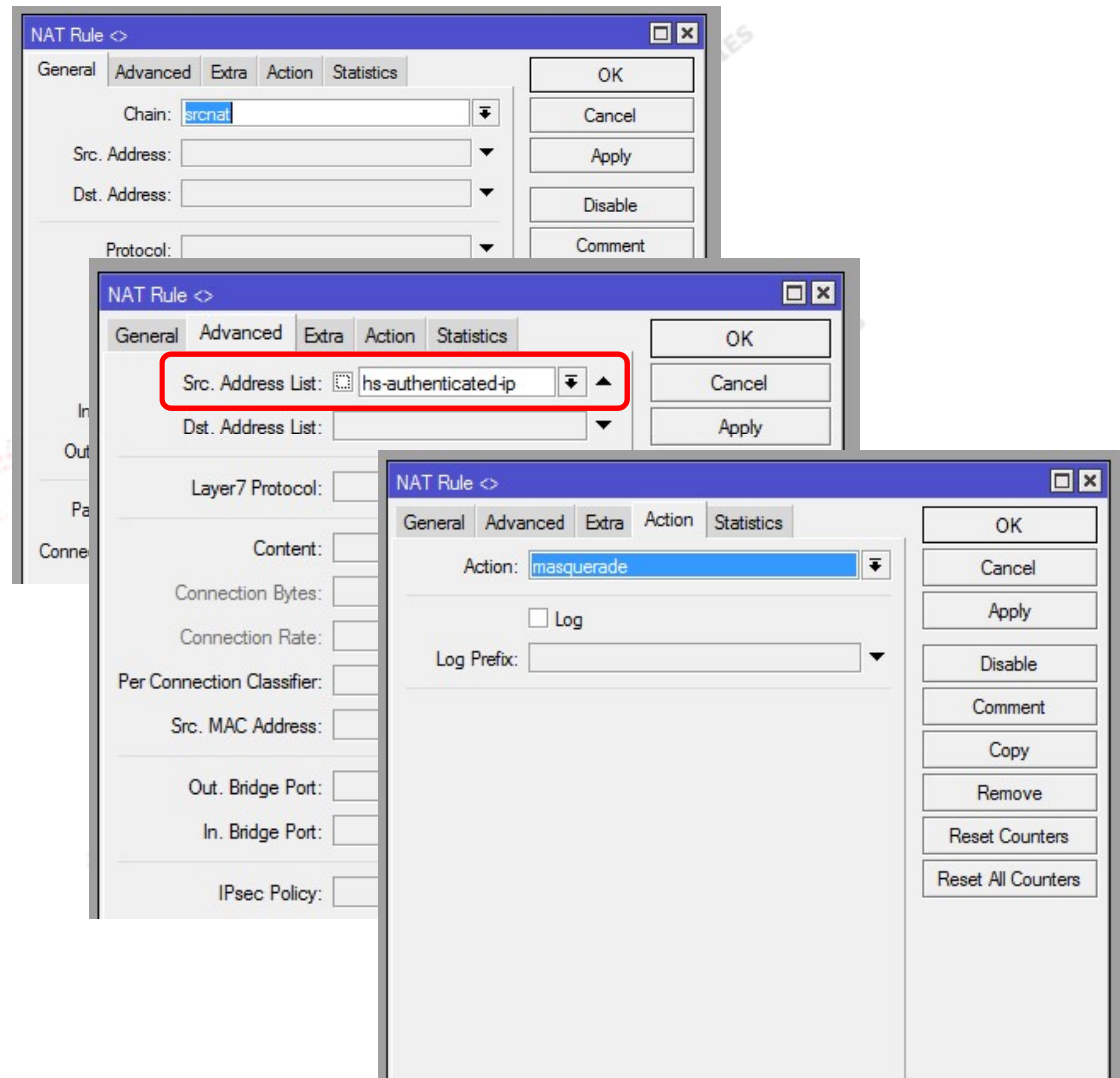
# Configuration (NAT settings)

Set the chain to SRCNAT

Use the SRC Address list to limit the authenticated user's IP to be NATTED

*The Mikrotik Hotspot Wizard setup uses the entire subnet to be natted (eg. 10.5.0.0/24), this can pose a problem.*

Use the MASQUERADE action



The image displays three sequential screenshots of the Mikrotik NAT Rule configuration interface:

- Top Screenshot:** The 'Chain' dropdown menu is set to 'srcnat'.
- Middle Screenshot:** The 'Src. Address List' dropdown menu is set to 'hs-authenticated-ip', which is highlighted with a red rectangular box.
- Bottom Screenshot:** The 'Action' dropdown menu is set to 'masquerade'.

## Further Security Measures

Service	Public Hotspot	Private Companies
Hotspot	Unsecured	NOT recommended for accessing company data
	Level of Security: Extremely Poor	Level of Security: Extremely Poor
VPN over opened wireless	NOT recommended	Highly Recommended with L2 security
	Level of Security: Practically useless if used with an open AP	Level of Security: Highly secure with L2 encryptions, can result to slow access due to high VPN overhead and lower payload size (ranging from 1300-1450)
PPPoE over wireless	Recommended for a permanent subscribers	Can be used with L2 Security
	Level of Security: Almost useless if used with an open AP, prone to rouge PPPoE server and ARP poisoning.	I do not know, who would use PPPoE on an encrypted Layer 2? (except if you want to have a control for the user account usage.)
802.1x with Radius AAA	Possible to use but not recommended	Recommended
	Level of Security: High but requires external server, not applicable for Public Hotspot	Level of Security: High but requires external server.



# Additional Hotspot Security

What to do...	What it does...
Disable Default Forward	Similar to AP Isolation (prevents wireless user from seeing each other at Layer-2 )
Set hotspot interface to ARP-REPLY only	It prevents user from poisoning the Router's ARP Table
Set DHCP to "Add ARP Address"	Let the router to add client's ARP to its table, (must be used with ARP-REPLY only)
Use a bigger IP pool like /23 or /22 and do not always use the first and last host address for the router	Typically, router always end in xxx.xxx.xxx.1 or xxx.xxx.xxx.254, this make it easier for anyone to attack the router.
Use the Netmask 32 at the DHCP server setting	It will assign the end user with 255.255.255.255 subnet mask.
Use my "IP hotspot Masking"	This will give another layer of defense by confusing the users of your network layout
Make use of HTTPS for hotspot login page	This will provide your end user a secured login process
DO NOT ACCESS your Userman page at your hotspot interface.	Limit your administrative webfig within your internal network, if you really need to access it from the hotspot interface, create a virtual AP with security and bind it to you local network interface.
Use HTTPS on all RouterOS web services and disable local web port 80, including other services SSH, TELNET, API.	Do not let these services to run on all interface especially the hotspot interface, limit it within your internal network
User RADIUS AAA for your authentication	RADIUS can provide you Authorization, Accounting and Access, a complete RADIUS package allows you to manage all kinds of services like your hotspot, VPN, dial-up, 802.1x etc..etc.. It also provide you a billing system.

# Mikrotik User Meeting

April 13 2016  
Manila, Philippines



-- END --