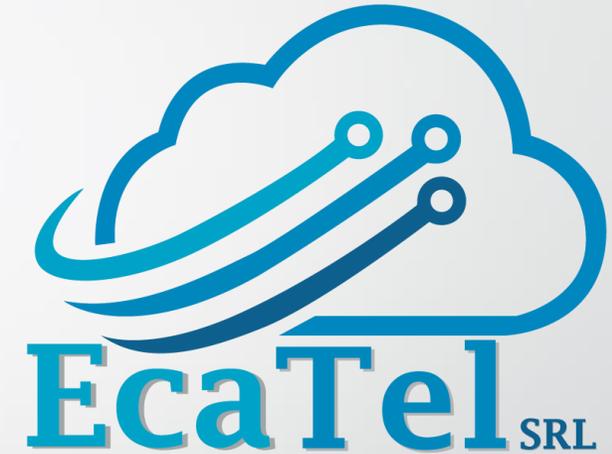


# HARDENING HOTSPOT / LAN



Ing. Jose Miguel Cabrera

**Mikrotik Trainer**

**Jefe de Proyectos**

La Paz – Bolivia

**Ecatel SRL**

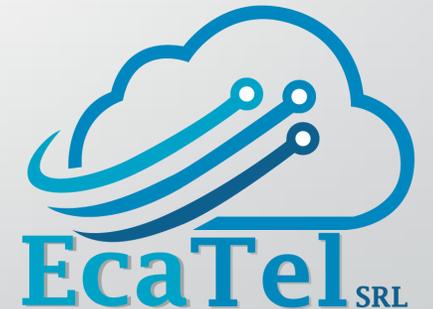
MUM 28 de Noviembre de 2016

# Acerca del disertante

- **Nombre:** Jose Miguel Cabrera Dalence
- **Profesión:** Ing. en Redes y Telecomunicaciones (UTEPSA)
- **Posgrado:** Especialista en Educación Superior Tecnológica (UAGRM)

## Experiencia:

- **Jefe de Proyectos en Ecatel SRL**
- Docente Universitario en Utepsa y UAGRM desde hace 5 años.
- Experiencia en múltiples marcas: Mikrotik, Cisco, Juniper, Check Point
- Certificaciones Mikrotik (MTCNA/**MTCIPv6E**/MTCWE/MTCRE/MTCINE/MTCUME/MTCTE/**Trainer**)
- Certificaciones Cisco (CCNP Security/CCNA/CCNA Security/VPN Specialist/Firewall Specialist)
- Certificaciones Ubiquiti (UEWA/UBWS/UBWA/UBRSS/UBRSA/Trainer)



# Acerca de Ecatel SRL

Es una empresa que se dedica a la **implementación de proyectos** integrando principalmente equipos de la marca Mikrotik, si es necesario combinados con otros marcas.

Brindamos **capacitaciones de Mikrotik**.

**Línea Gratuita**

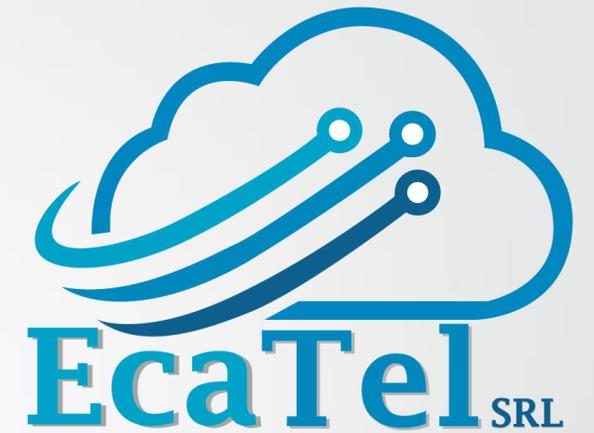
800 24 0030

info@ecatel.com.bo

Santa Cruz - Bolivia



facebook.com/EcatelSRL



# ¿QUÉ ES HARDENING ?



Hardening, significa endurecimiento, en seguridad informática es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo. Ya sea cerrando puertos, eliminando usuarios por defecto, etc.

# ¿QUÉ ES HOTSPOT ?



Proporcionan acceso a internet, puede ser gratuito o de pago.

Los hotspots se encuentran en lugares públicos, como aeropuertos, bibliotecas, centros de convenciones, cafeterías, hoteles, escuelas, etc.

# ¿QUÉ ES UNA LAN ?



**Local Area Network**, es una red que conecta dispositivos de red como: computadoras, tablets, smarthphone, etc.

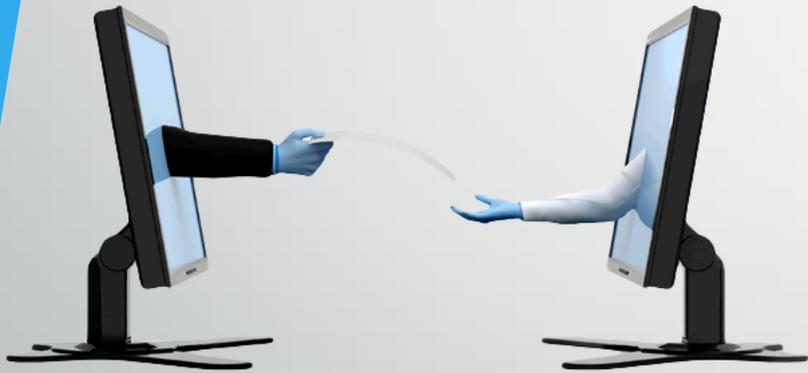
Pueden conectar entre ellas a través de cable de UTP, fibra óptica o WiFi. Deben estar geográficamente cerca.

# PROBLEMAS QUE RESOLVEREMOS



Para resolver un problema, el primer paso es identificar las posibles vulnerabilidades.

# COMPARTIR CARPETAS



Los usuarios pueden infectar de virus a la PC de su colega. Si están usando la red WiFi pueden saturarla

# ROBO DE SESION / IDENTIDAD



Al estar en el mismo segmento de red, pueden realizar ataques de MitM (Hombre en el medio) y robar credenciales de sistemas inseguros Ejemplo: http, telnet

# ESCALAMIENTO DE PRIVILEGIOS



Muchos permisos en la red se basan en la dirección IP del cliente.

Tan fácil como esperar que el administrador salga y colocarse la IP que él utiliza

# ATAQUES DDOS



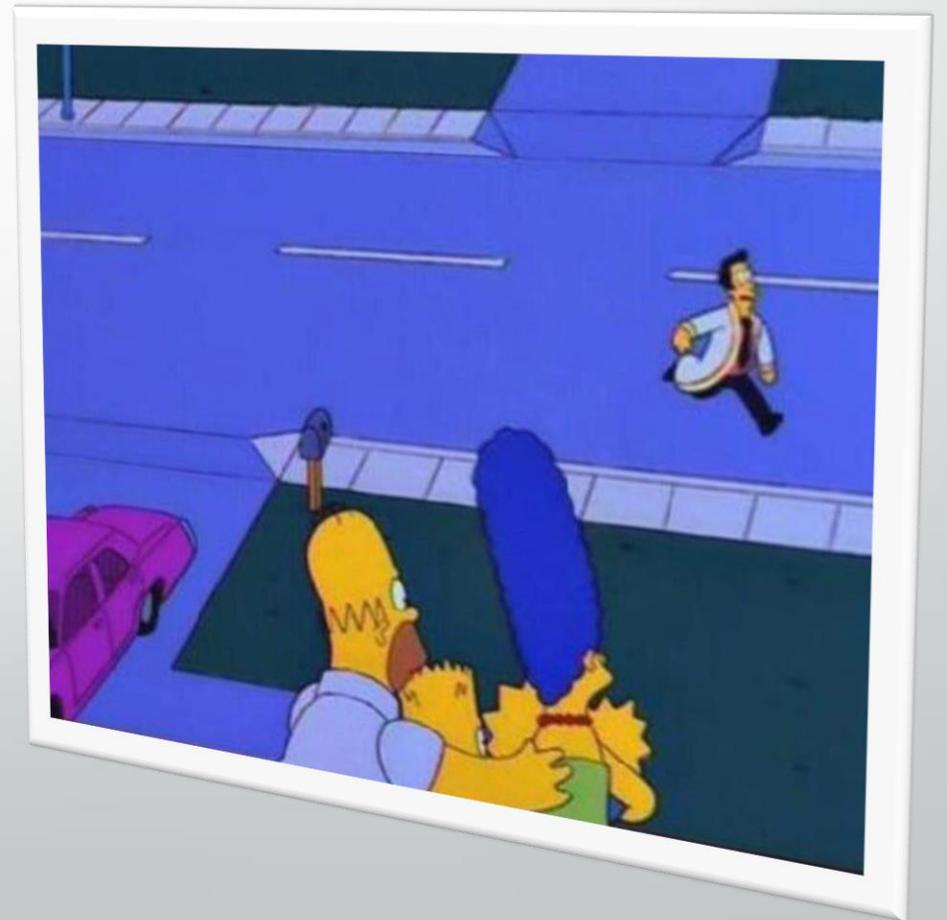
Es un ataque a un sistema o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

Aunque no se roba información, igualmente causa pérdidas económicas.

# ¿QUE HACEMOS?

Podemos ignorar el problema, como lo hace la mayoría, salir corriendo despavoridos de miedo.

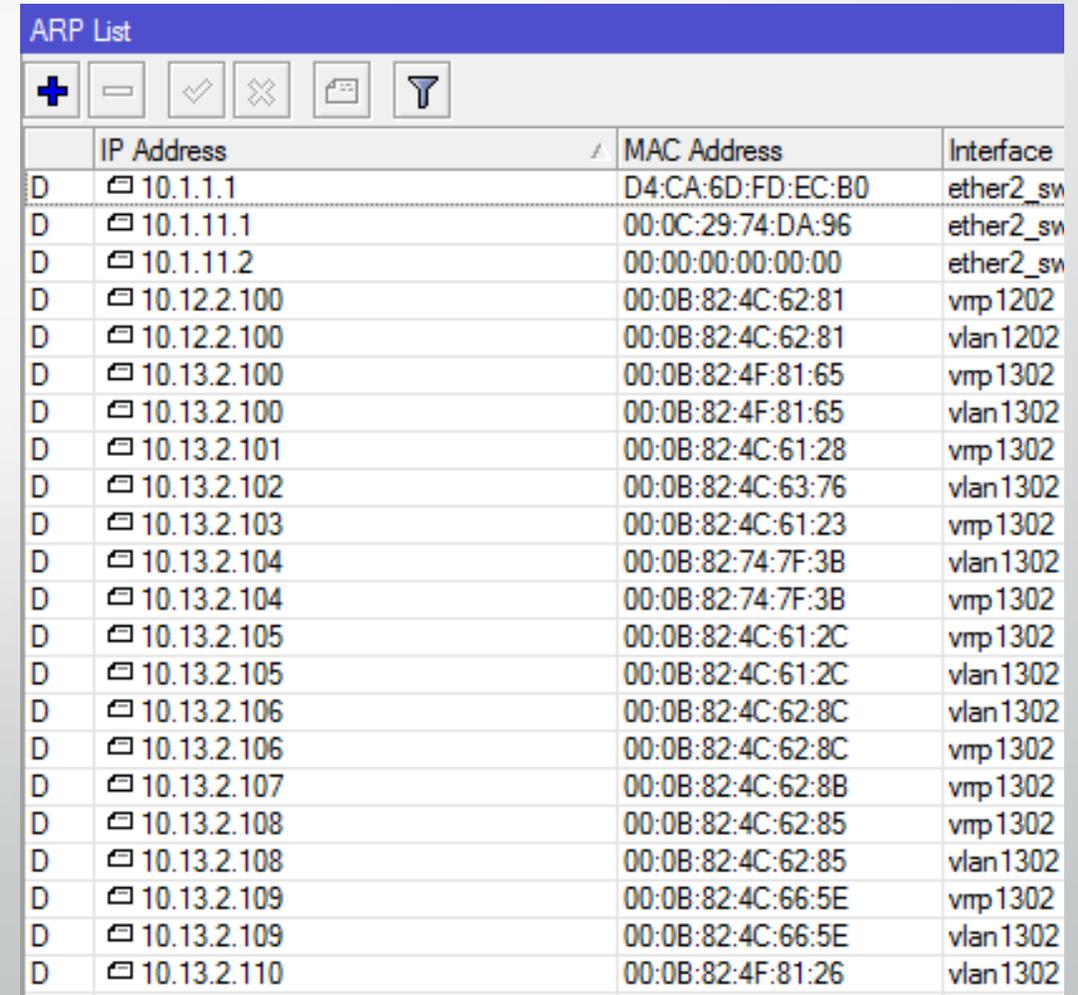
***¡Calma! Que no cunda el pánico***



# CONCEPTO - PROTOCOLO ARP

Es un protocolo de la capa de enlace(2) del modelo OSI, responsable de encontrar la dirección de hardware (MAC) que corresponde a una determinada dirección IP.

La tabla ARP muestra esta información. *Por defecto* se llena de manera **DINAMICA**



The screenshot shows a window titled "ARP List" with a table of network entries. The table has four columns: a status column with 'D' in a box, an IP Address column, a MAC Address column, and an Interface column. The entries are sorted by IP address. The interface names include ether2\_sw, vmp 1202, vmp 1302, and vlan 1202, vlan 1302.

	IP Address	MAC Address	Interface
D	10.1.1.1	D4:CA:6D:FD:EC:B0	ether2_sw
D	10.1.11.1	00:0C:29:74:DA:96	ether2_sw
D	10.1.11.2	00:00:00:00:00:00	ether2_sw
D	10.12.2.100	00:0B:82:4C:62:81	vmp 1202
D	10.12.2.100	00:0B:82:4C:62:81	vlan 1202
D	10.13.2.100	00:0B:82:4F:81:65	vmp 1302
D	10.13.2.100	00:0B:82:4F:81:65	vlan 1302
D	10.13.2.101	00:0B:82:4C:61:28	vmp 1302
D	10.13.2.102	00:0B:82:4C:63:76	vlan 1302
D	10.13.2.103	00:0B:82:4C:61:23	vmp 1302
D	10.13.2.104	00:0B:82:74:7F:3B	vlan 1302
D	10.13.2.104	00:0B:82:74:7F:3B	vmp 1302
D	10.13.2.105	00:0B:82:4C:61:2C	vmp 1302
D	10.13.2.105	00:0B:82:4C:61:2C	vlan 1302
D	10.13.2.106	00:0B:82:4C:62:8C	vlan 1302
D	10.13.2.106	00:0B:82:4C:62:8C	vmp 1302
D	10.13.2.107	00:0B:82:4C:62:8B	vmp 1302
D	10.13.2.108	00:0B:82:4C:62:85	vmp 1302
D	10.13.2.108	00:0B:82:4C:62:85	vlan 1302
D	10.13.2.109	00:0B:82:4C:66:5E	vmp 1302
D	10.13.2.109	00:0B:82:4C:66:5E	vlan 1302
D	10.13.2.110	00:0B:82:4F:81:26	vlan 1302

# ARP – REPLY ONLY

Activando en el router el modo “reply-only” para el ARP, un administrador deberá *llenar la tabla ARP* de manera **MANUAL**

Interface <ether1>

General | Ethernet | Loop Protect | Overall Stats | Rx Stats | ...

Name: ether1

Type: Ethernet

MTU: 1500

Actual MTU: 1500

L2 MTU: 1600

Max L2 MTU: 4076

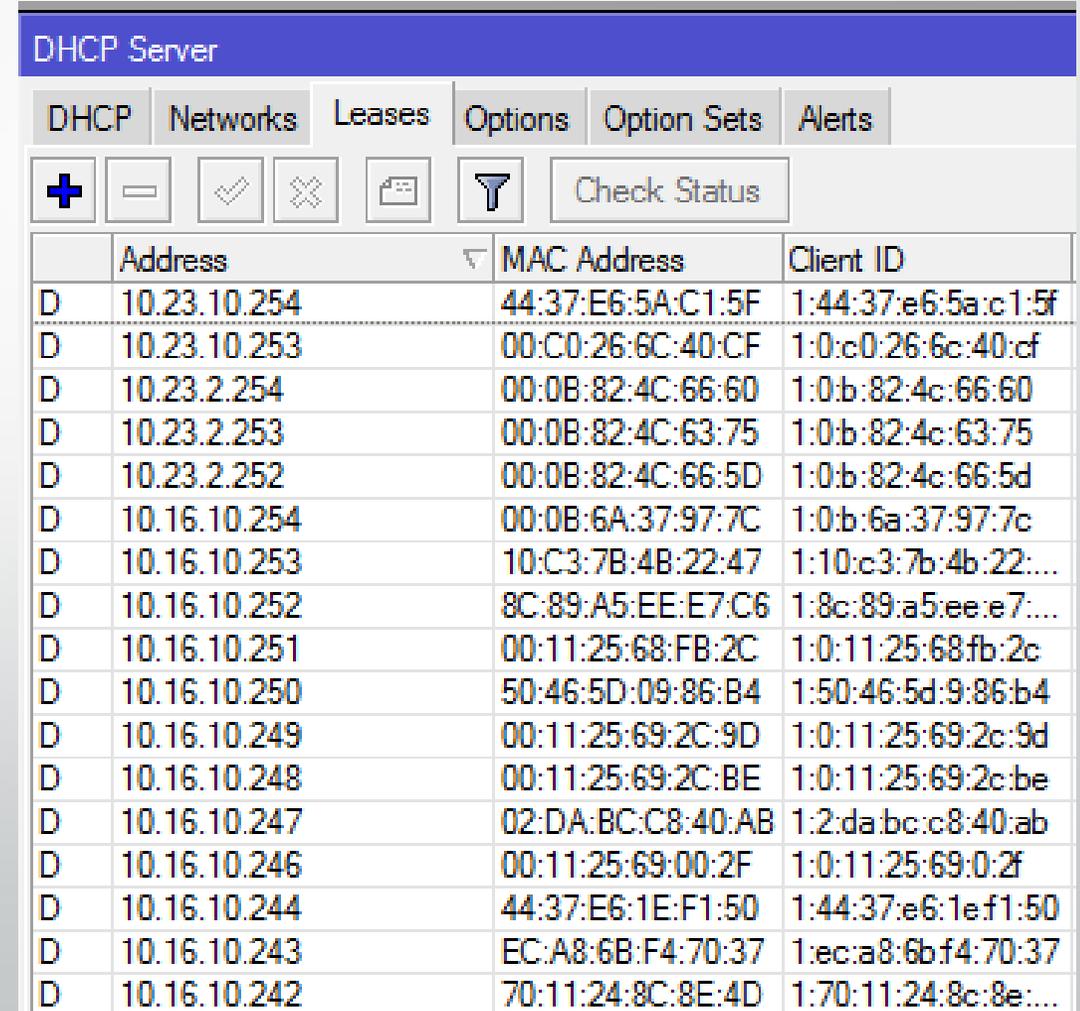
MAC Address: D4:CA:6D:A5:BE:DE

ARP: reply-only

ARP Timeout:

# CONCEPTO – DHCP SERVER

Es un servidor que posee una lista de direcciones IP (pool) para asignar a los clientes, además provee información como: Gateway, DNS, NTP, etc.



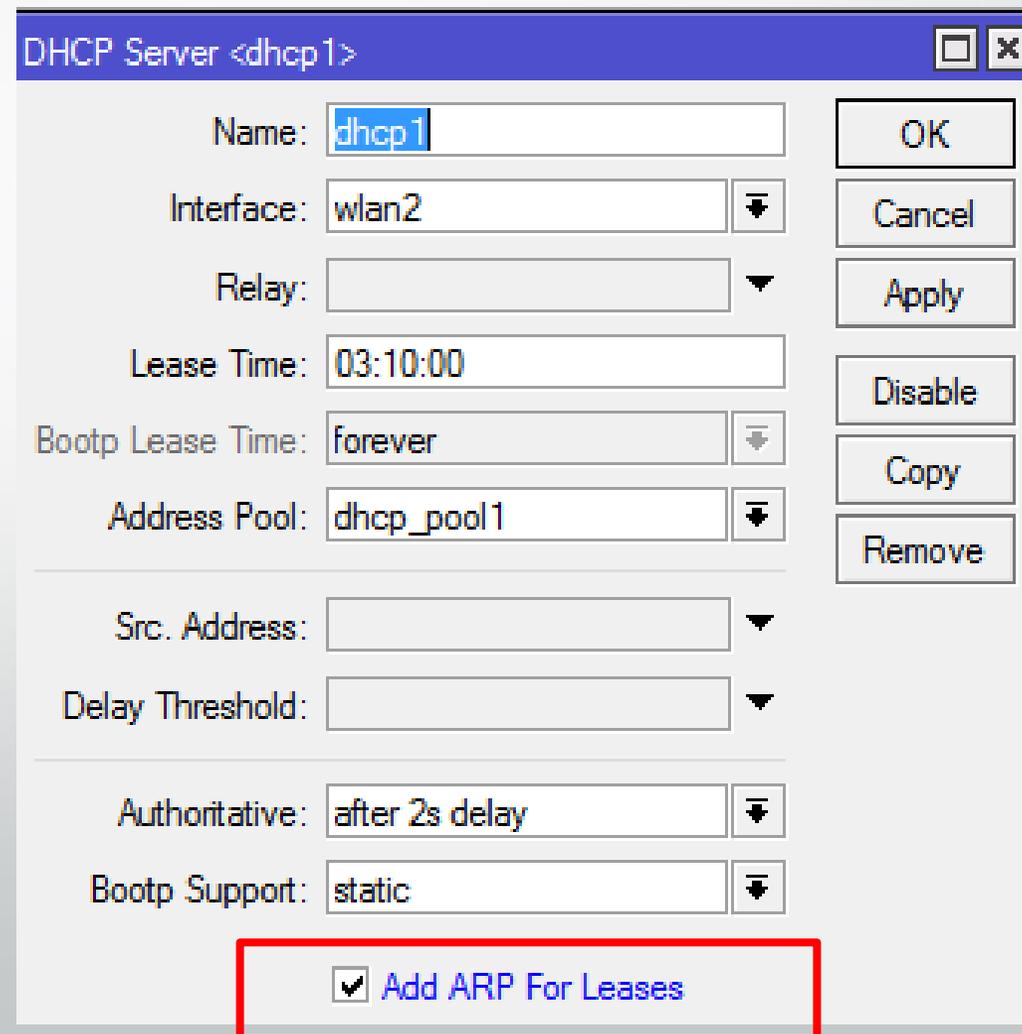
The screenshot shows a web-based interface for a DHCP Server. At the top, there is a blue header with the text "DHCP Server". Below the header, there are several tabs: "DHCP", "Networks", "Leases", "Options", "Option Sets", and "Alerts". The "Leases" tab is currently selected. Below the tabs, there is a toolbar with icons for adding (+), removing (-), checking (checkmark), deleting (X), and a filter icon, along with a "Check Status" button. The main area displays a table with the following columns: "Address", "MAC Address", and "Client ID". The table contains 16 rows of data, each representing a DHCP lease.

	Address	MAC Address	Client ID
D	10.23.10.254	44:37:E6:5A:C1:5F	1:44:37:e6:5a:c1:5f
D	10.23.10.253	00:C0:26:6C:40:CF	1:0:c0:26:6c:40:cf
D	10.23.2.254	00:0B:82:4C:66:60	1:0:b:82:4c:66:60
D	10.23.2.253	00:0B:82:4C:63:75	1:0:b:82:4c:63:75
D	10.23.2.252	00:0B:82:4C:66:5D	1:0:b:82:4c:66:5d
D	10.16.10.254	00:0B:6A:37:97:7C	1:0:b:6a:37:97:7c
D	10.16.10.253	10:C3:7B:4B:22:47	1:10:c3:7b:4b:22:...
D	10.16.10.252	8C:89:A5:EE:E7:C6	1:8c:89:a5:ee:e7:...
D	10.16.10.251	00:11:25:68:FB:2C	1:0:11:25:68:fb:2c
D	10.16.10.250	50:46:5D:09:86:B4	1:50:46:5d:9:86:b4
D	10.16.10.249	00:11:25:69:2C:9D	1:0:11:25:69:2c:9d
D	10.16.10.248	00:11:25:69:2C:BE	1:0:11:25:69:2c:be
D	10.16.10.247	02:DA:BC:C8:40:AB	1:2:da:bc:c8:40:ab
D	10.16.10.246	00:11:25:69:00:2F	1:0:11:25:69:0:2f
D	10.16.10.244	44:37:E6:1E:F1:50	1:44:37:e6:1e:f1:50
D	10.16.10.243	EC:A8:6B:F4:70:37	1:ec:a8:6b:f4:70:37
D	10.16.10.242	70:11:24:8C:8E:4D	1:70:11:24:8c:8e:...

# ARP REPLY ONLY + DHCP SERVER

Colocando el ARP en modo REPLY ONLY, además de utilizar DHCP y marcar la opción ADD ARP FOR LEASES

Tenemos la solución al cambio de direcciones IP.



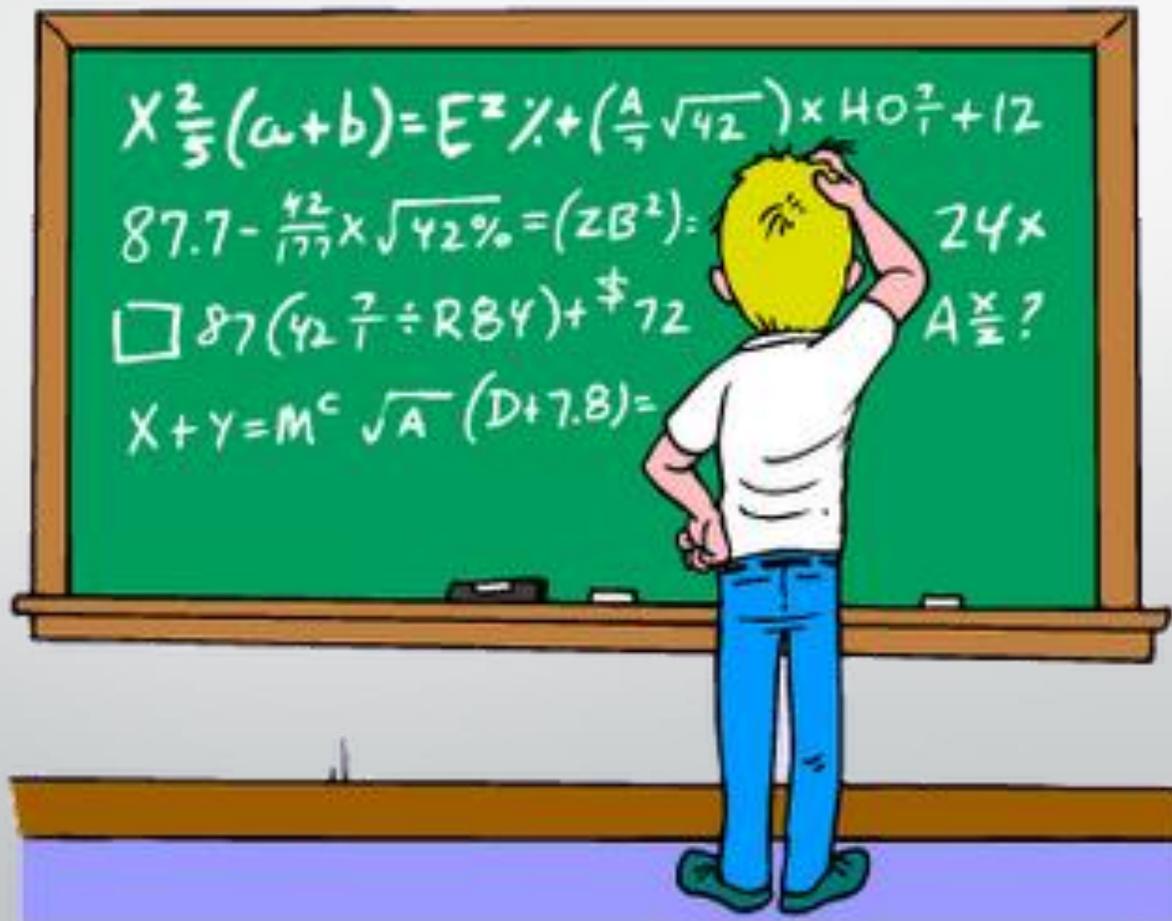
The screenshot shows a configuration window titled "DHCP Server <dhcp1>". The window contains several fields and buttons:

- Name: dhcp1
- Interface: wlan2
- Relay: (empty)
- Lease Time: 03:10:00
- Bootp Lease Time: forever
- Address Pool: dhcp\_pool1
- Src. Address: (empty)
- Delay Threshold: (empty)
- Authoritative: after 2s delay
- Bootp Support: static

Buttons on the right side include: OK, Cancel, Apply, Disable, Copy, and Remove.

At the bottom, there is a checkbox labeled "Add ARP For Leases" which is checked and highlighted with a red box.

# ¿SE ENTENDIO?



***SHOW TIME!***

***DEMOSTRACION***



# AISLAMIENTO DEL USUARIO



**No** deseamos que un usuario se comunique con otro.

Los pondremos fácilmente en un segmento /32

No, no es error. Un segmento **SOLO** para él

# AISLAMIENTO DEL USUARIO

DHCP Network <192.168.79.0/24>

Address: 192.168.79.0/24

Gateway: 192.168.79.1

Netmask: 32

DNS Servers: 8.8.8.8

8.8.4.4

Adicionamos en

**IP -> DHCP-SERVER -> NETWORK**

# AISLAMIENTO DEL USUARIO

C:\Windows\system32\cmd.exe

```
Adaptador de LAN inalámbrica Wi-Fi:
```

```
Sufijo DNS específico para la conexión. . . :  
Vínculo: dirección IPv6 local. . . . : fe80::1080:cae7:af83:5107%16  
Dirección IPv4. . . . . : 192.168.88.254  
Máscara de subred . . . . . : 255.255.255.255  
Puerta de enlace predeterminada . . . . . : 192.168.88.1
```

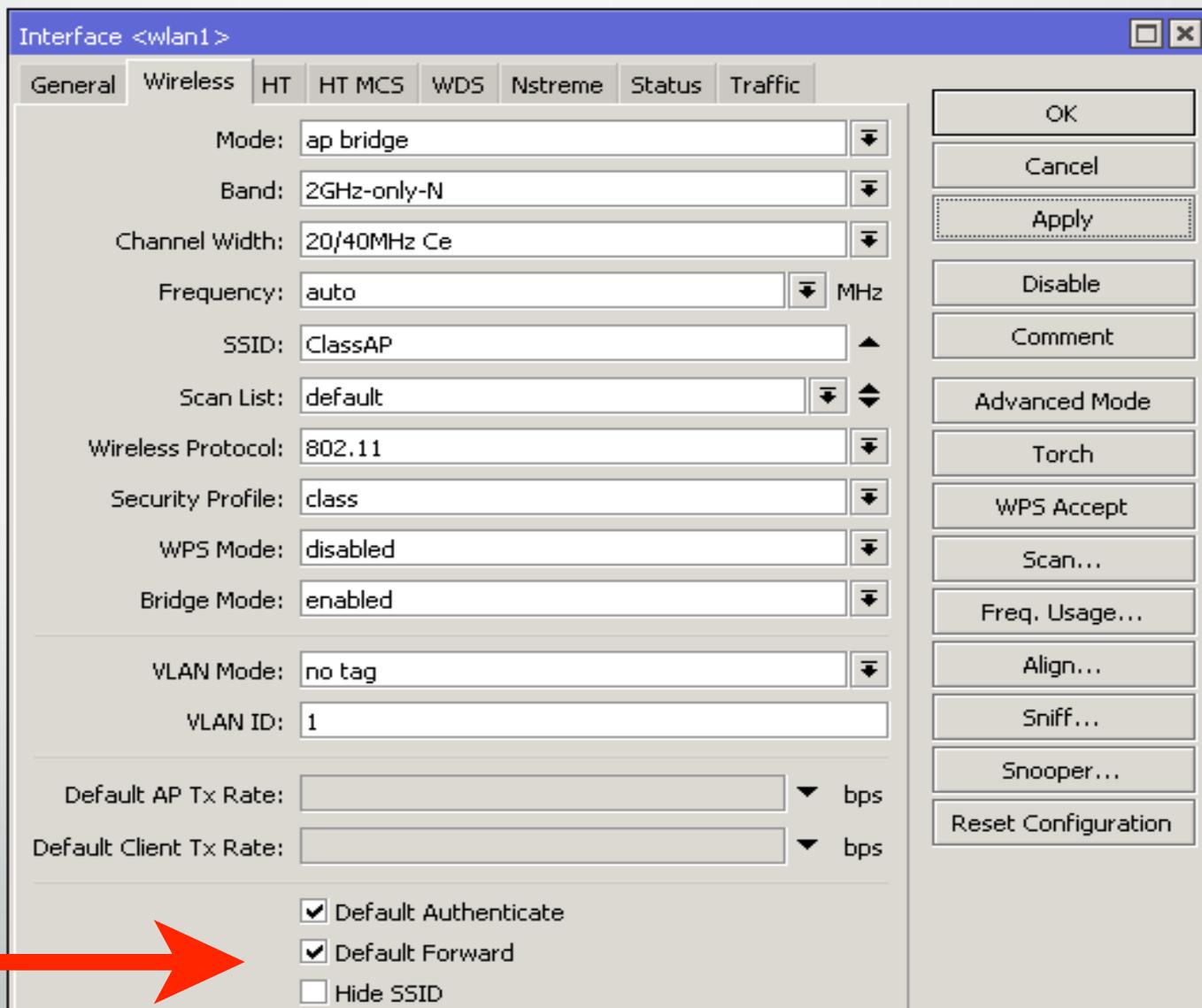
El resultado esperado sería este.

¿Por qué quiero un /32? Todo el tráfico del usuario obligatoriamente pasará por el router a nivel de capa 3, por lo que se podrán aplicar reglas de Firewall para bloquear lo que no deseamos.

# AISLAMIENTO DEL USUARIO

En la tarjeta inalámbrica desactive la casilla "Default Forward"

Esto evita que los clientes usen la red WiFi como si fuera un switch.



Interface <wlan1>

General Wireless HT HT MCS WDS Nstreme Status Traffic

Mode: ap bridge

Band: 2GHz-only-N

Channel Width: 20/40MHz Ce

Frequency: auto MHz

SSID: ClassAP

Scan List: default

Wireless Protocol: 802.11

Security Profile: class

WPS Mode: disabled

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

Scan...

Freq. Usage...

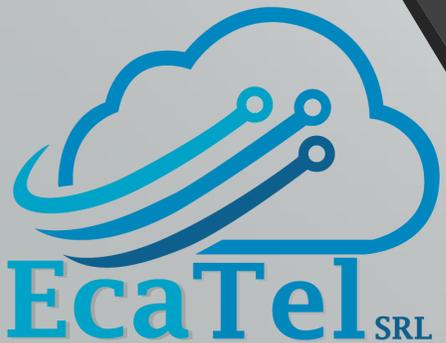
Align...

Sniff...

Snooper...

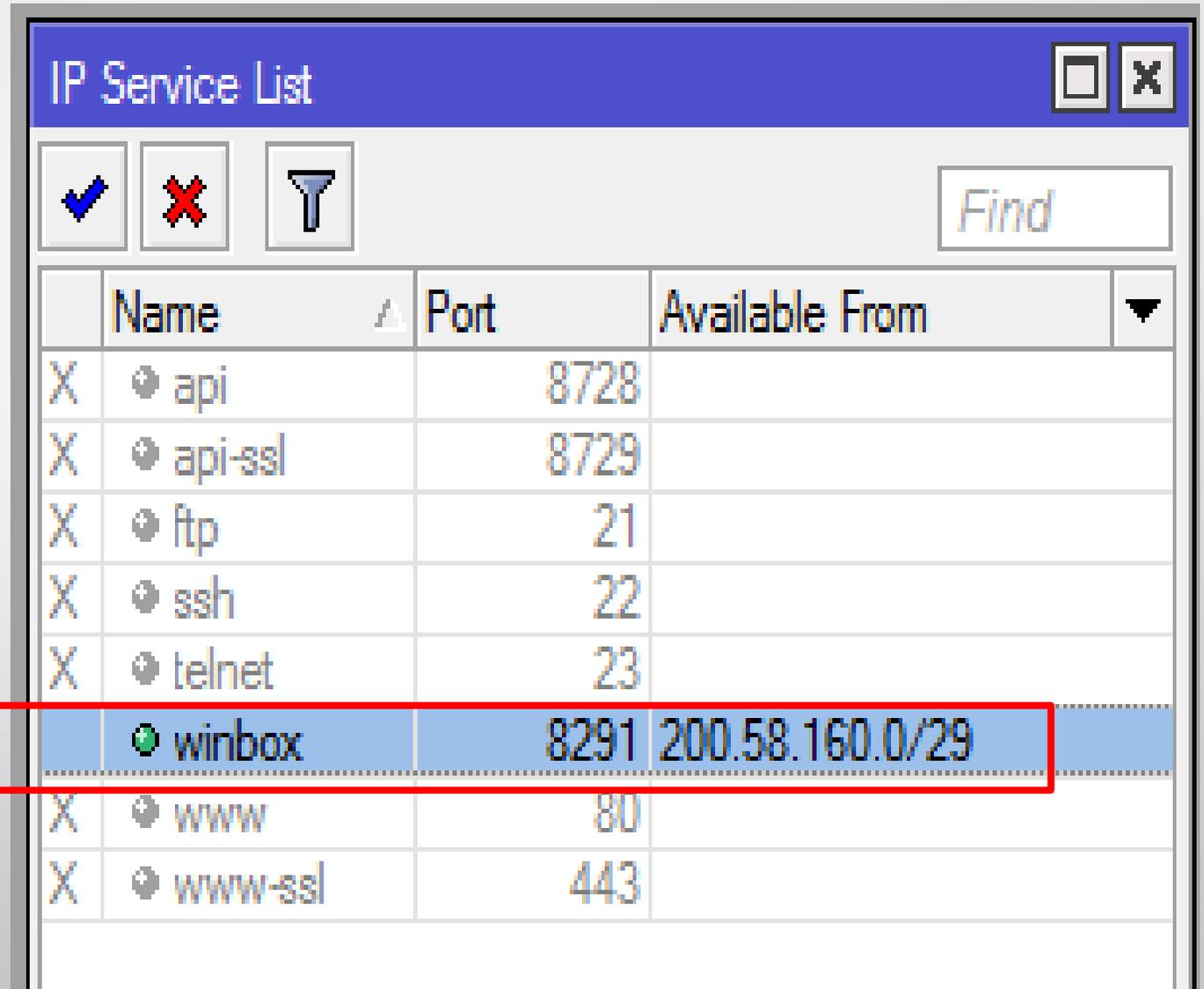
Reset Configuration

# SEGURIDAD PARA EL ROUTER



# DESHABILITAR SERVICIOS INNECESARIOS

IP -> SERVICES



The screenshot shows a window titled "IP Service List" with a table of services. The table has columns for Name, Port, and Available From. The 'winbox' service is highlighted with a red box.

	Name	Port	Available From
X	api	8728	
X	api-ssl	8729	
X	ftp	21	
X	ssh	22	
X	telnet	23	
	winbox	8291	200.58.160.0/29
X	www	80	
X	www-ssl	443	

# REGLAS BÁSICAS EN CHAIN INPUT

IP -> FIREWALL

Firewall						
Filter Rules						
NAT						
Mangle						
Raw						
Service Ports						
Connections						
Address Lists						
Layer						
+ - ✓ ✗ [icon] [icon] 00 Reset Counters 00 Reset All Counters						
#	Action	Chain	Protocol	Dst. Port	In. Interface	
::: Permitir: Establecidos / Relacionados						
0	✓ accept	input				
::: Permitir: Winbox						
1	✓ accept	input	6 (tcp)	8291		
::: Bloquear todo desde Internet						
2	✗ drop	input			ether1_Internet	

# DNS – ¡PRECAUCION!

IP -> DNS

DNS Settings

Servers:  ⇅

Dynamic Servers:

Allow Remote Requests

Max UDP Packet Size:

Query Server Timeout:  s

Query Total Timeout:  s

Cache Size:  KB

Cache Max TTL:

Cache Used:

OK

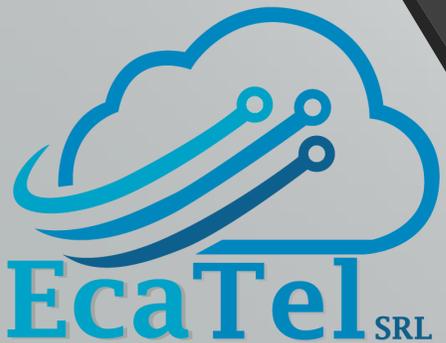
Cancel

Apply

Static

Cache

# HEALTH (Salud) DEL ROUTER



# INFORMACION BÁSICA DEL EQUIPO

## System -> Health

System Health		<input type="checkbox"/>	<input type="checkbox"/>
Voltage:	24.0 V	<input type="button" value="OK"/>	
Temperature:	15 C	<input type="button" value="Cancel"/>	
CPU Temperature:	31 C	<input type="button" value="Apply"/>	
Current:	631 mA		
Power Consumption:	15.1 W		

# ESTADO DEL CPU DEL EQUIPO

soporte@[REDACTED] - WinBox v6.37.2 on RB2011UiAS-2HnD (mipsbe) - □ X

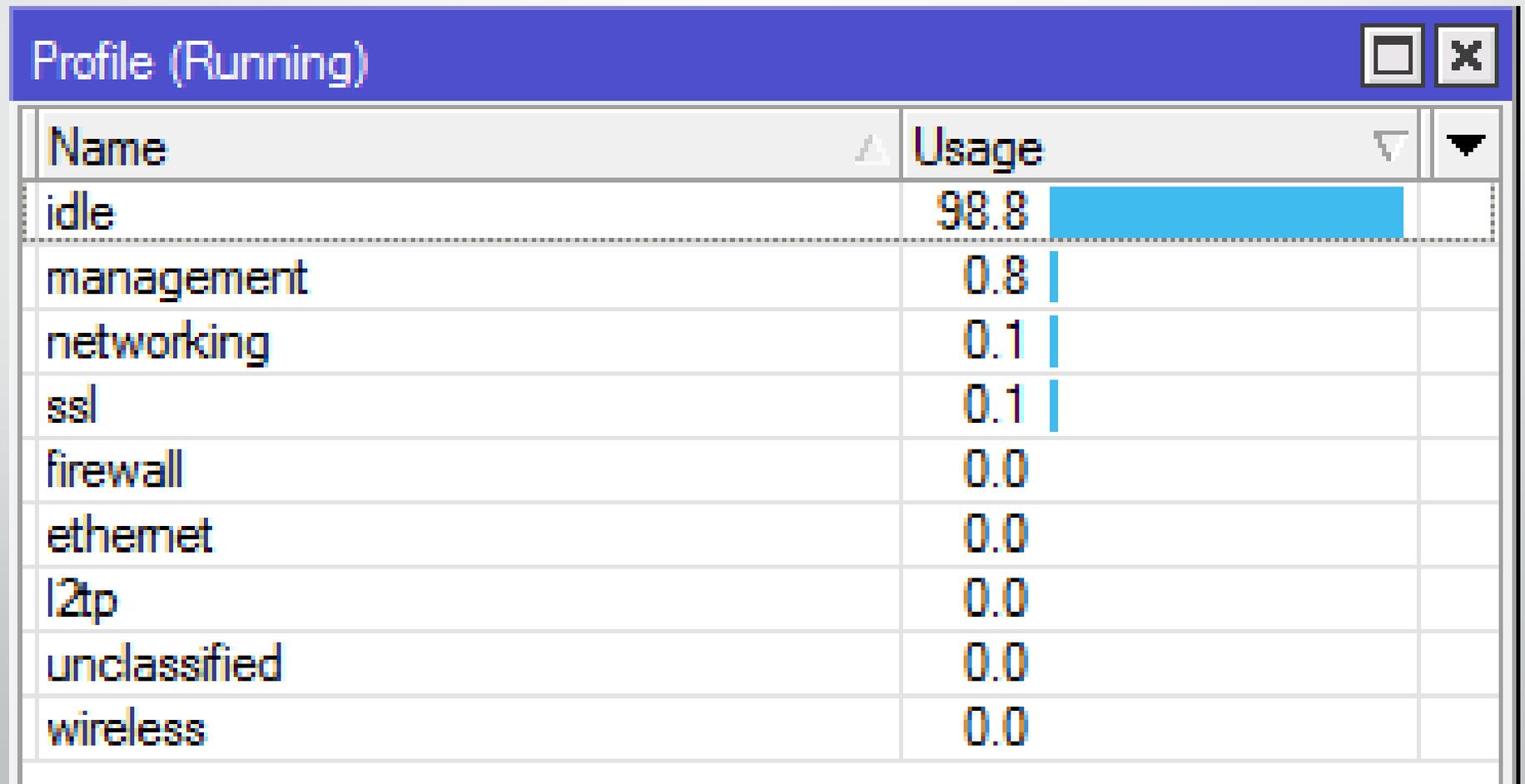
Session Settings Dashboard

  Safe Mode Session:  Uptime: 3d 15:41:20 Memory: 101.0 MiB **CPU: 1%** Date: Nov/28/2016 Time: 09:59:29 

 Firewall

# ¿COMO SE CONSUME EL CPU?

Tool -> Profile



Name	Usage
idle	98.8
management	0.8
networking	0.1
ssl	0.1
firewall	0.0
ethemet	0.0
l2tp	0.0
unclassified	0.0
wireless	0.0

***SHOW TIME!***

***DEMOSTRACION***

