HARDENING HOTSPOT / LAN

Ing. Jose Miguel Cabrera

Mikrotik Trainner

Jefe de Proyectos

Ecatel SRL

La Paz – Bolivia

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)

MikroTik CERTIFIED TRAINER

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)

EcaTel SRL

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.

EcaTel SRL

¿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.

EcaTel SRL

¿QUÉ ES UNA LAN ?

Local **A**rea **N**etwork, 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.

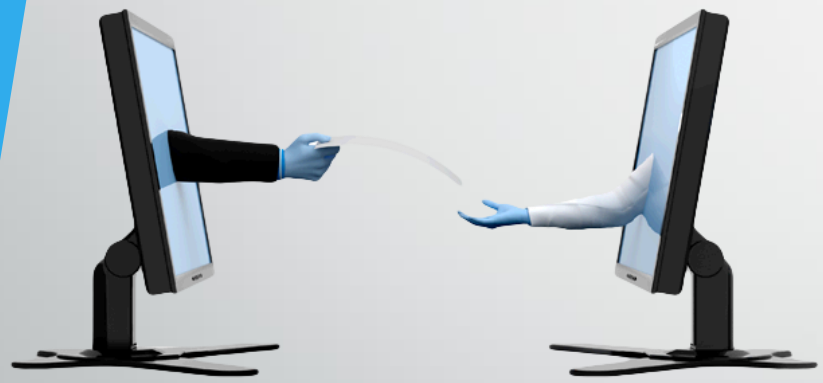
EcaTel SRL

PROBLEMAS QUE RESOLVEREMOS

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

EcaTel SRL

COMPARTIR CARPETAS



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

EcaTel SRL

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

EcaTel SRL

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 utiiza

EcaTel SRL

ATAQUES DDOS

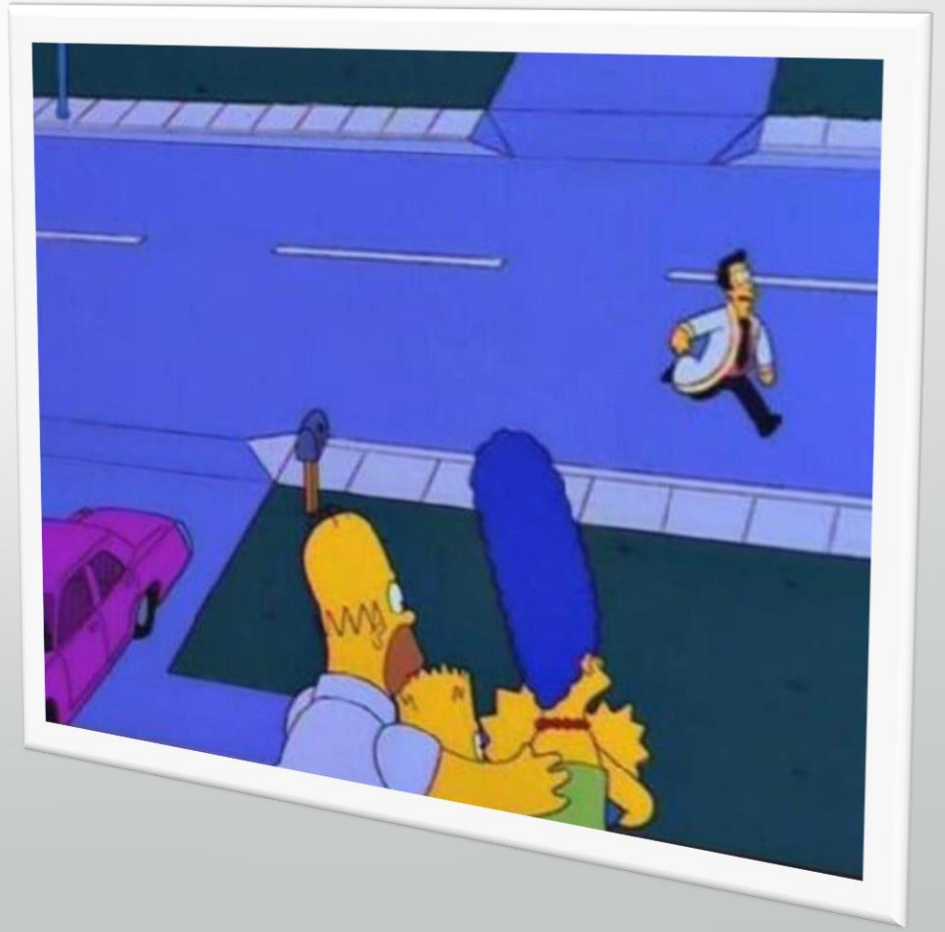
Es un ataque a un sistema o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

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.

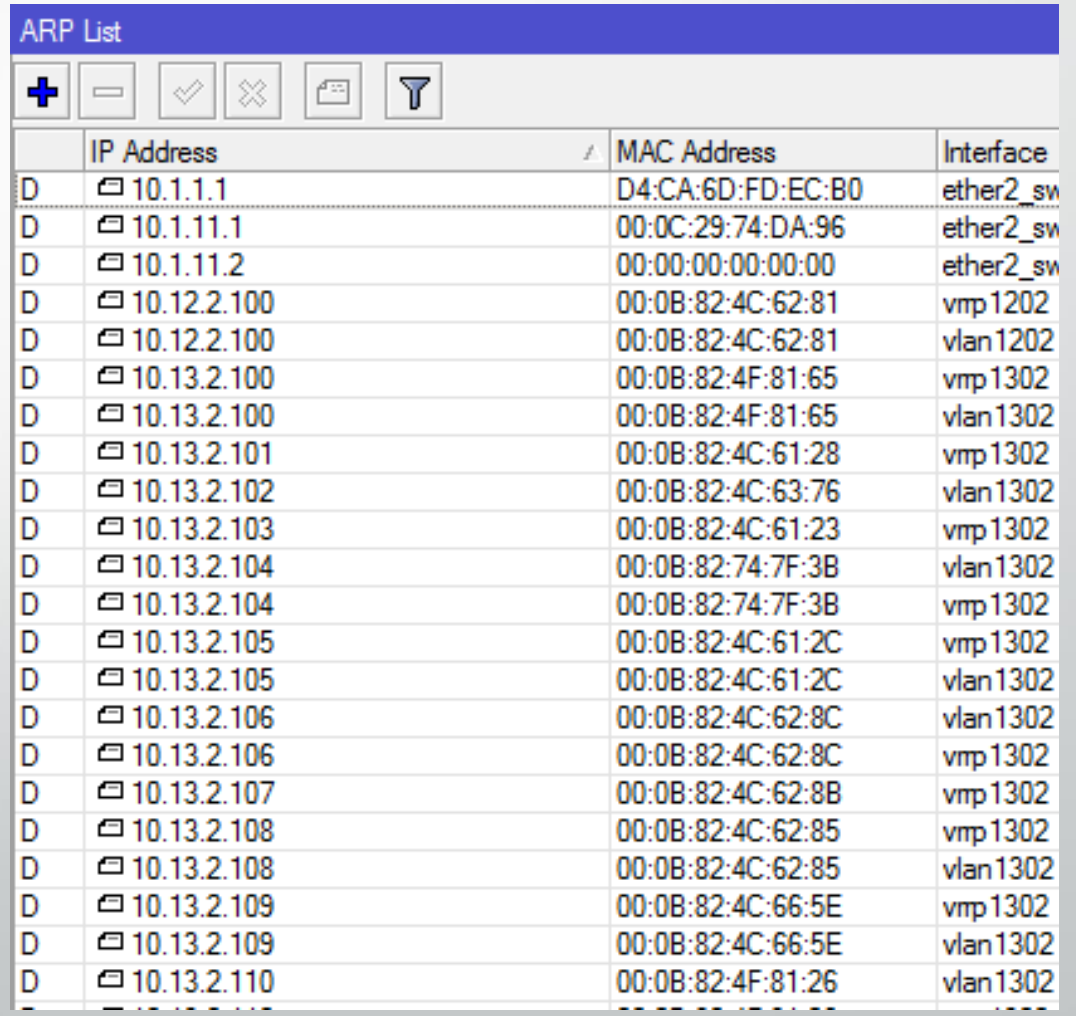
¡Calma! Que no cunda el pánico



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***

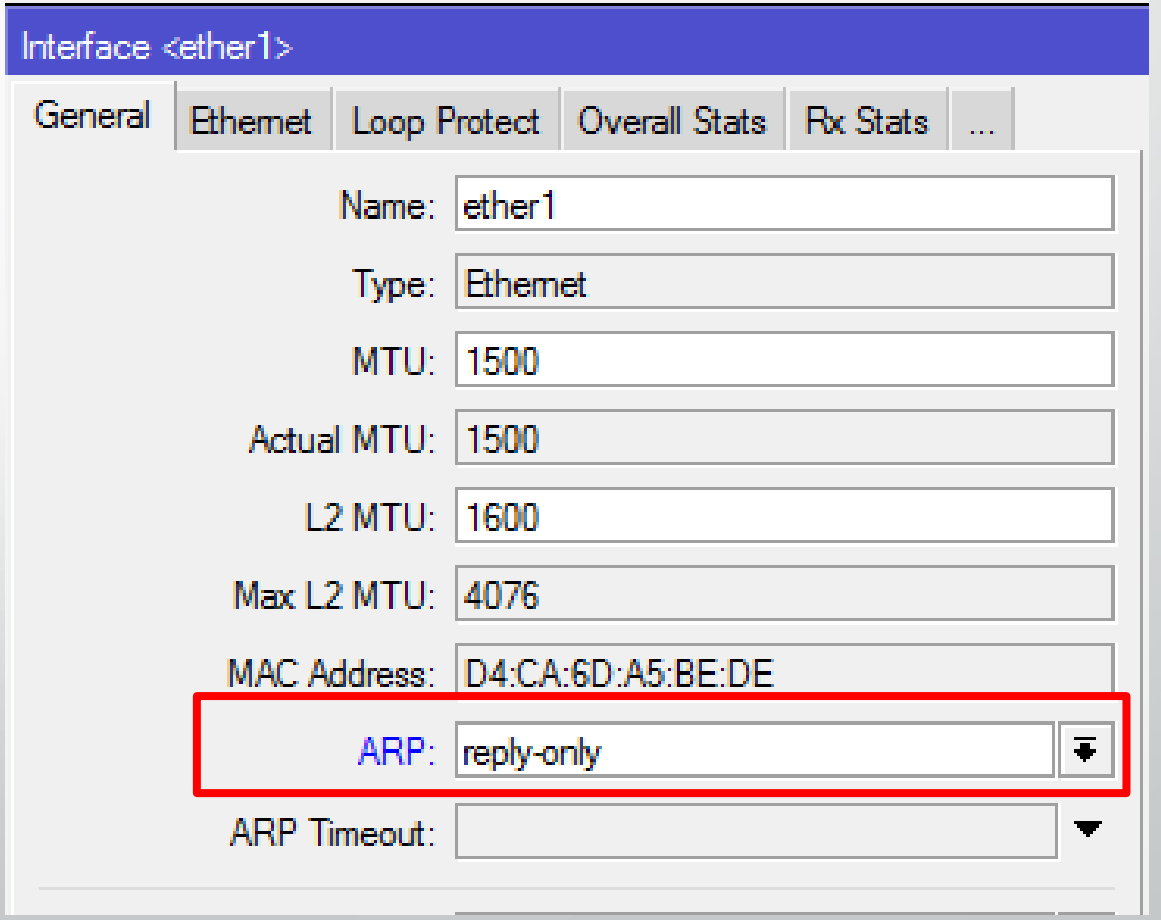


	IP Address	MAC Address	Interface
D	10.1.1.1	D4:CA:6D:FD:EC:B0	ether2_sw
D	10.1.11.1	00:0C:29:74:DA:96	ether2_sw
D	10.1.11.2	00:00:00:00:00:00	ether2_sw
D	10.12.2.100	00:0B:82:4C:62:81	vrrp1202
D	10.12.2.100	00:0B:82:4C:62:81	vlan1202
D	10.13.2.100	00:0B:82:4F:81:65	vrrp1302
D	10.13.2.100	00:0B:82:4F:81:65	vlan1302
D	10.13.2.101	00:0B:82:4C:61:28	vrrp1302
D	10.13.2.102	00:0B:82:4C:63:76	vlan1302
D	10.13.2.103	00:0B:82:4C:61:23	vrrp1302
D	10.13.2.104	00:0B:82:74:7F:3B	vlan1302
D	10.13.2.104	00:0B:82:74:7F:3B	vrrp1302
D	10.13.2.105	00:0B:82:4C:61:2C	vrrp1302
D	10.13.2.105	00:0B:82:4C:61:2C	vlan1302
D	10.13.2.106	00:0B:82:4C:62:8C	vlan1302
D	10.13.2.106	00:0B:82:4C:62:8C	vrrp1302
D	10.13.2.107	00:0B:82:4C:62:8B	vrrp1302
D	10.13.2.108	00:0B:82:4C:62:85	vrrp1302
D	10.13.2.108	00:0B:82:4C:62:85	vlan1302
D	10.13.2.109	00:0B:82:4C:66:5E	vrrp1302
D	10.13.2.109	00:0B:82:4C:66:5E	vlan1302
D	10.13.2.110	00:0B:82:4F:81:26	vlan1302

EcaTel SRL

ARP – REPLY ONLY

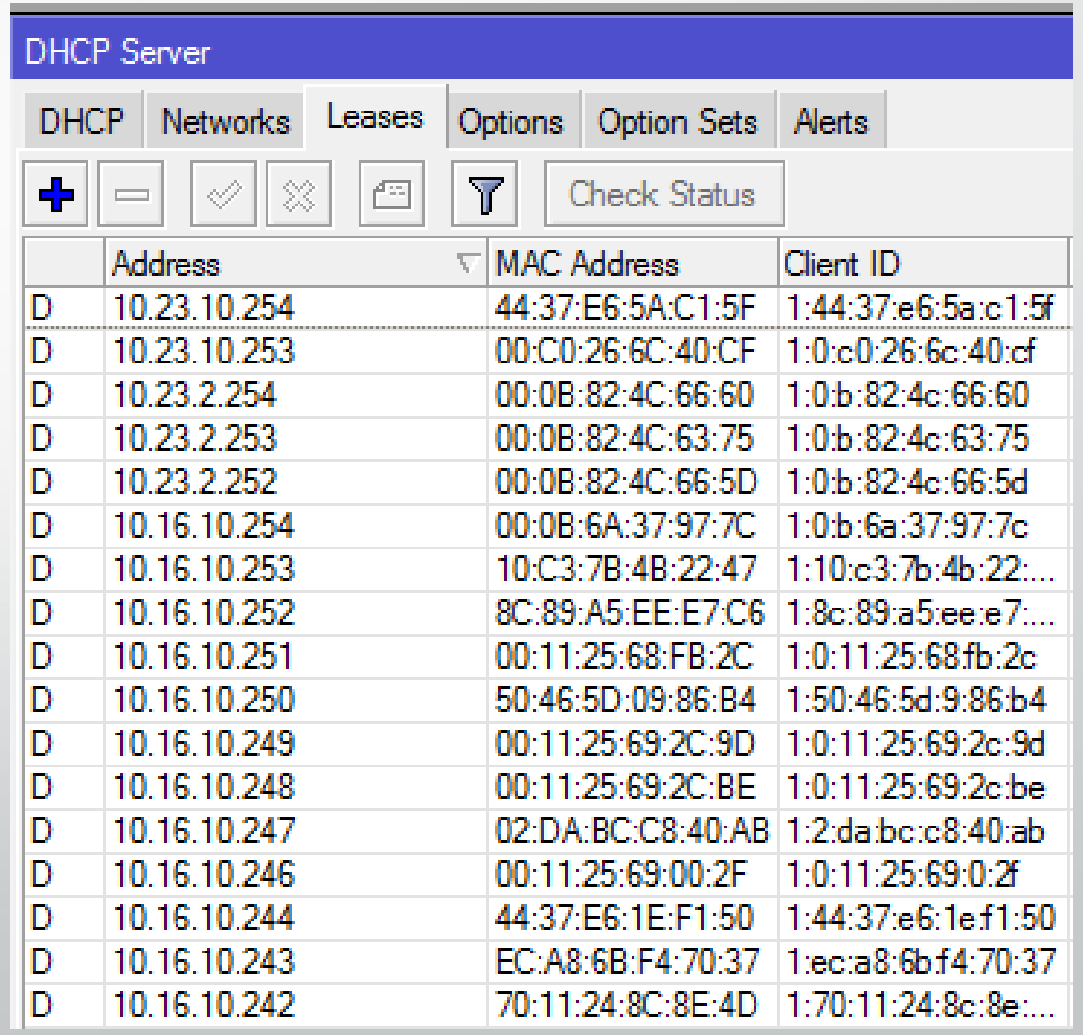
Activando en el router el modo "reply-only" para el ARP, un administrador deberá *llenar la tabla ARP* de manera ***MANUAL***



EcaTel SRL

CONCEPTO – DHCP SERVER

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



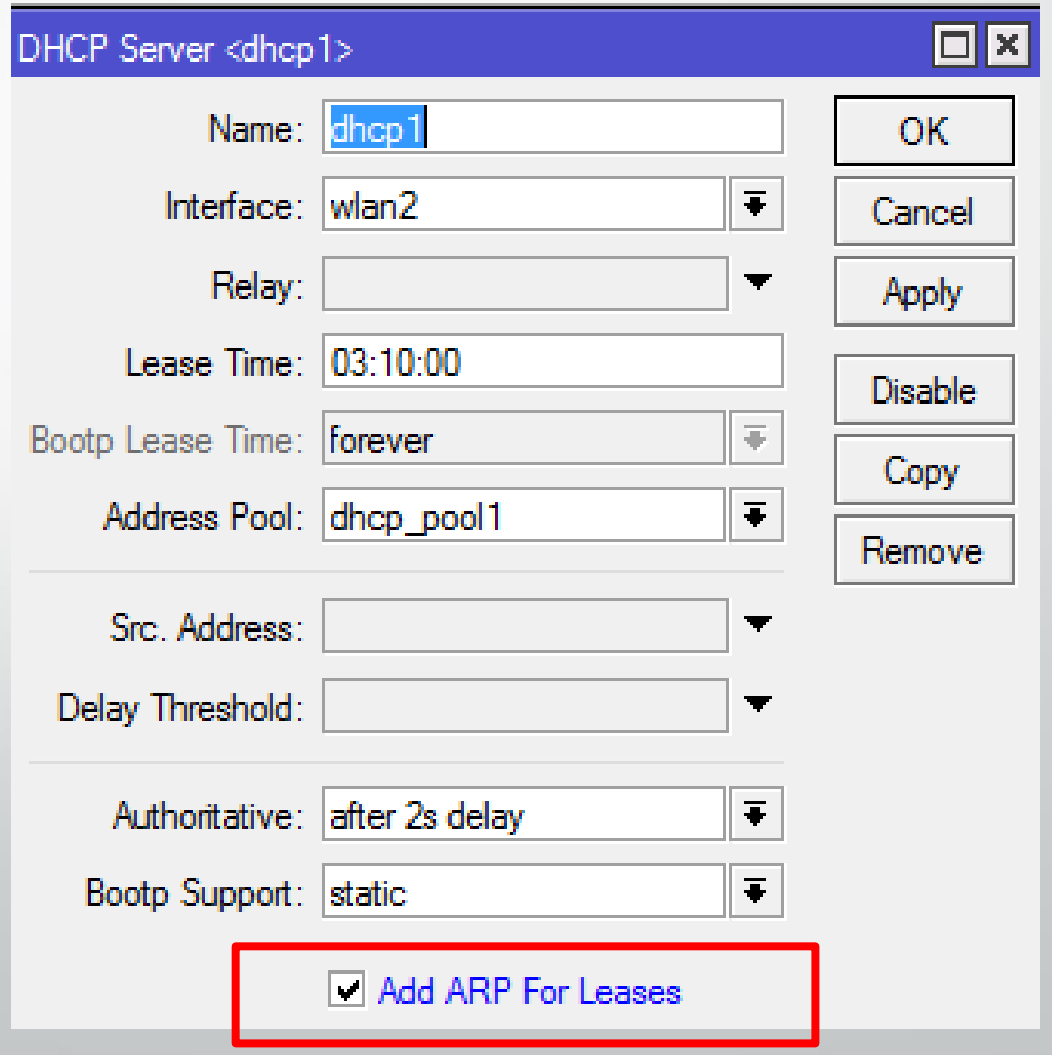
	Address	MAC Address	Client ID
D	10.23.10.254	44:37:E6:5A:C1:5F	1:44:37:e6:5a:c1:5f
D	10.23.10.253	00:C0:26:6C:40:CF	1:0:c0:26:6c:40:cf
D	10.23.2.254	00:0B:82:4C:66:60	1:0:b:82:4c:66:60
D	10.23.2.253	00:0B:82:4C:63:75	1:0:b:82:4c:63:75
D	10.23.2.252	00:0B:82:4C:66:5D	1:0:b:82:4c:66:5d
D	10.16.10.254	00:0B:6A:37:97:7C	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:...

EcaTel SRL

ARP REPLY ONLY + DHCP SERVER

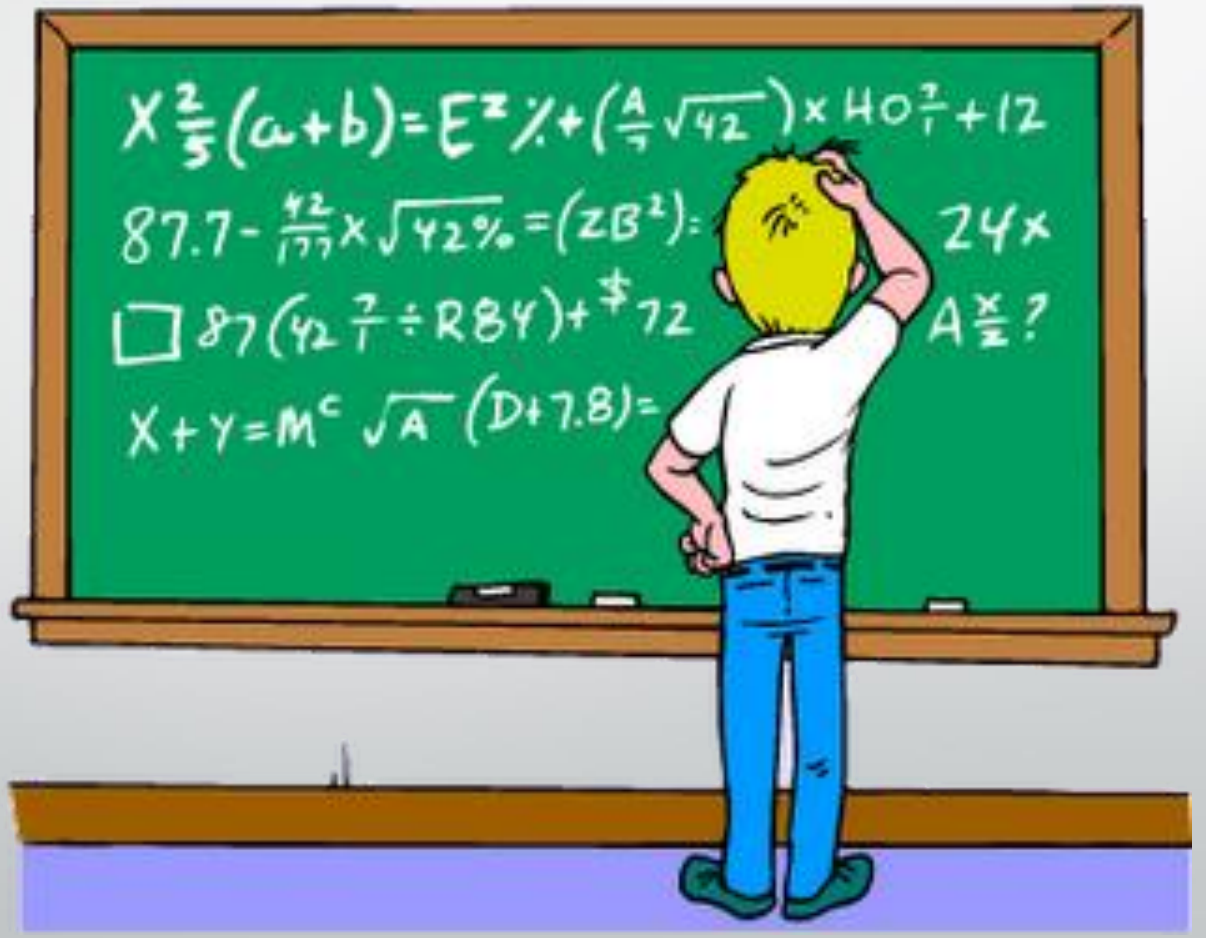
Colocando el ARP en modo REPLY ONLY, además de utilizar DHCP y marcar la opción ADD ARP FOR LEASES

Tenemos la solución al cambio de direcciones IP.



EcaTel SRL

¿SE ENTENDIO?



SHOW TIME!

DEMOSTRACION

AISLAMIENTO DEL USUARIO

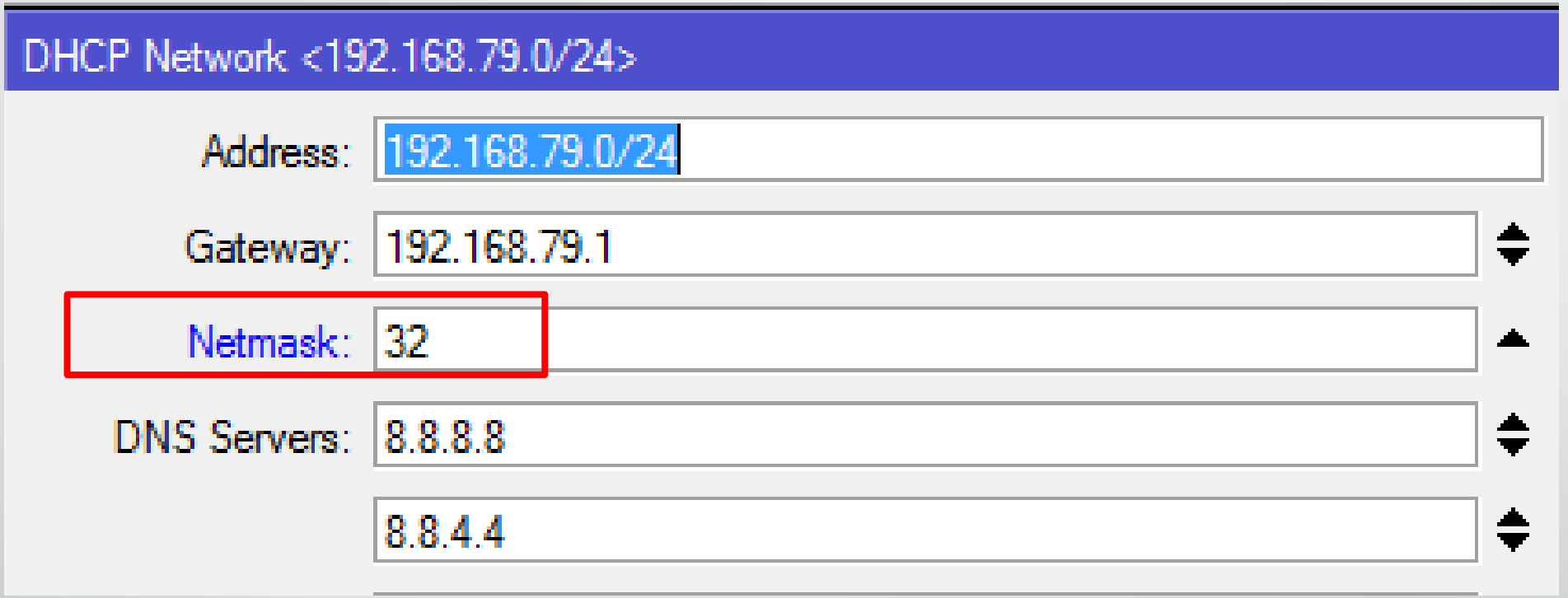
No deseamos que un usuario se comunique con otro.

Los pondremos fácilmente en un segmento /32

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

EcaTel SRL

AISLAMIENTO DEL USUARIO

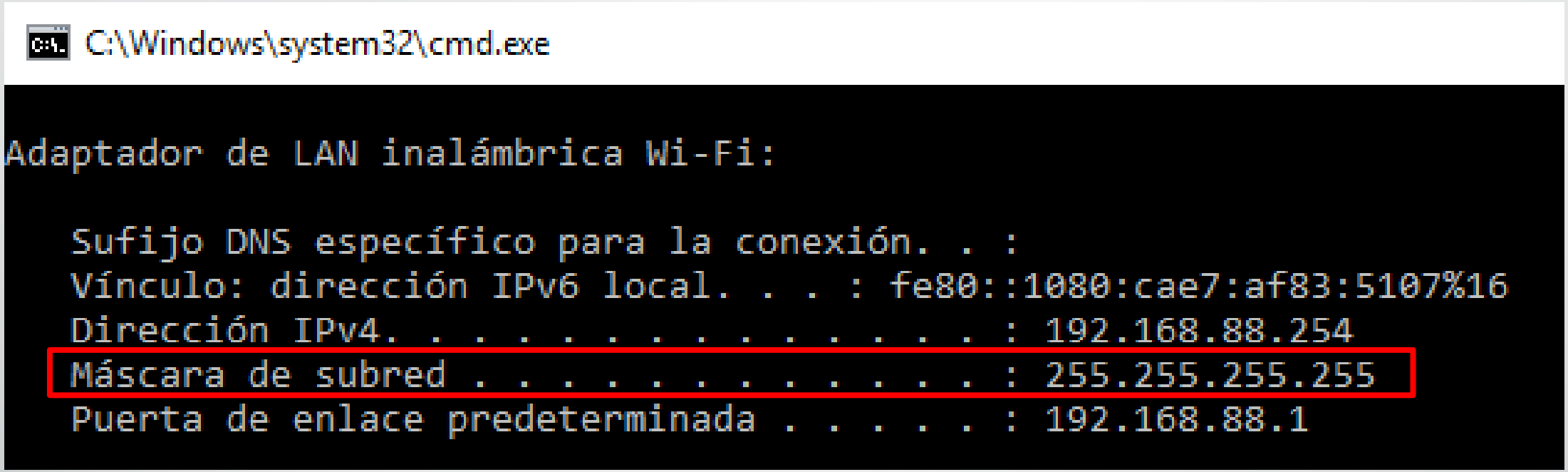


Adicionamos en

IP -> DHCP-SERVER -> NETWORK

EcaTel SRL

AISLAMIENTO DEL USUARIO



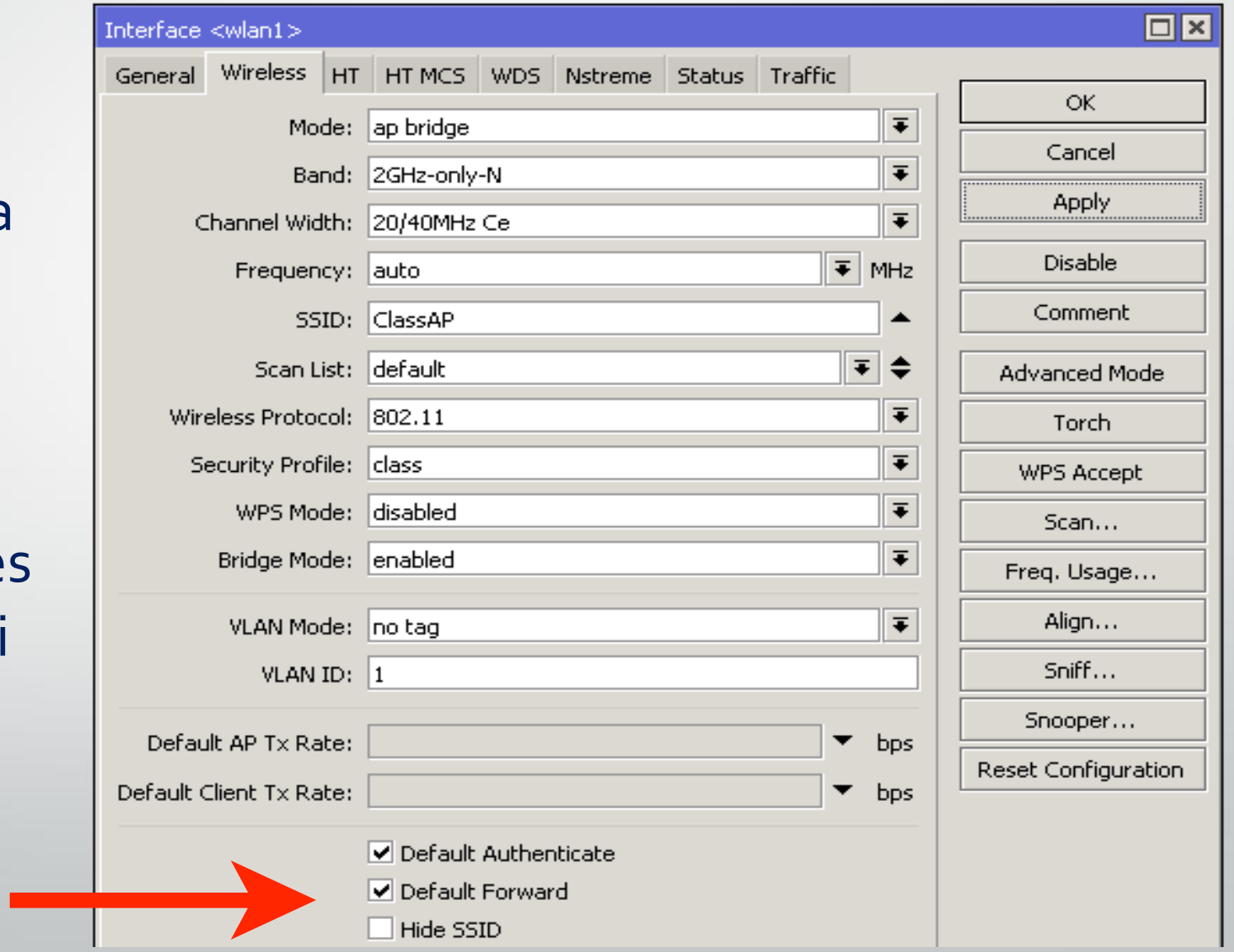
El resultado esperado sería este.

¿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.

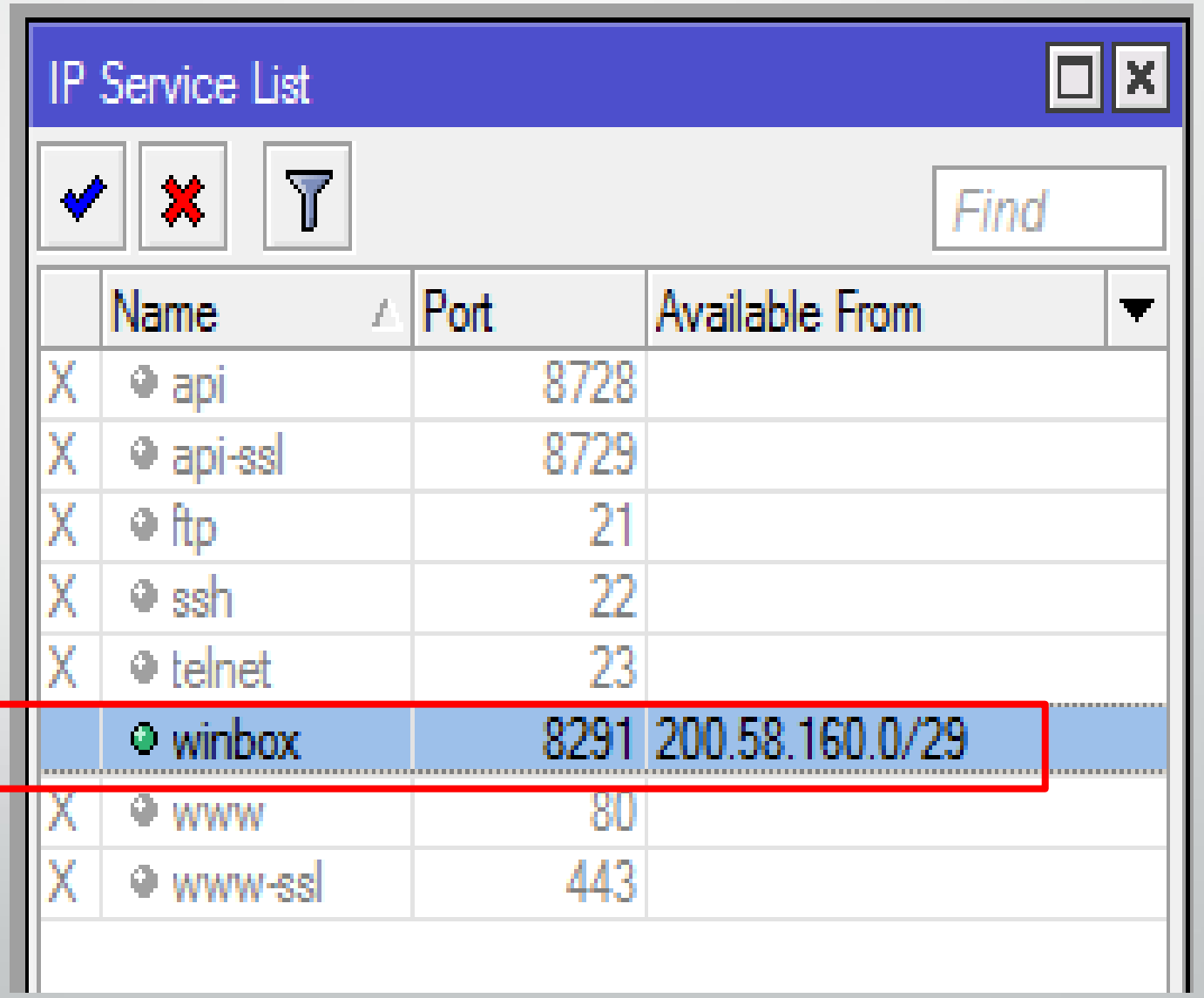


SEGURIDAD PARA EL ROUTER

EcaTel SRL

DESHABILITAR SERVICIOS INNECESARIOS

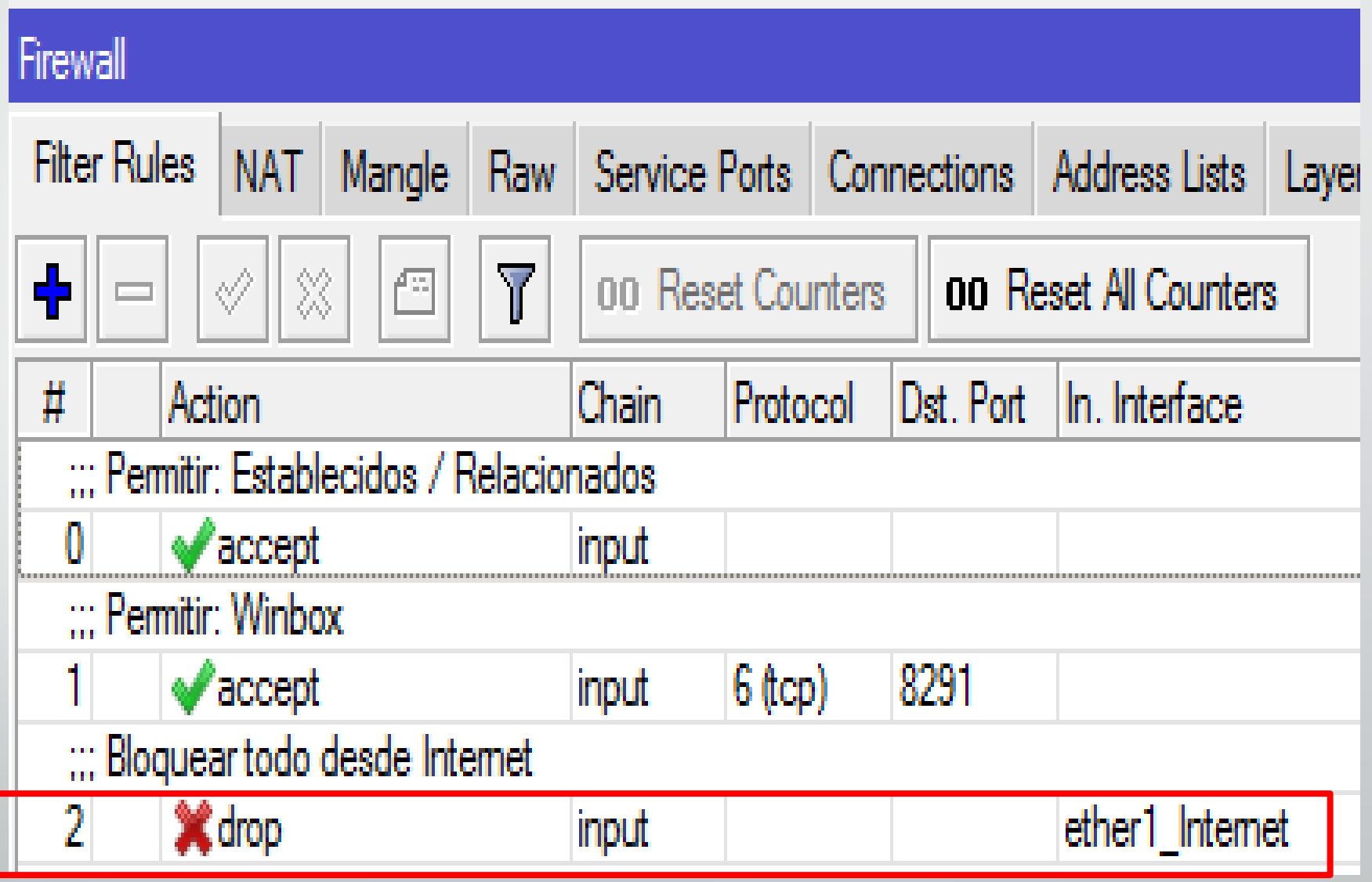
IP -> SERVICES



EcaTel SRL

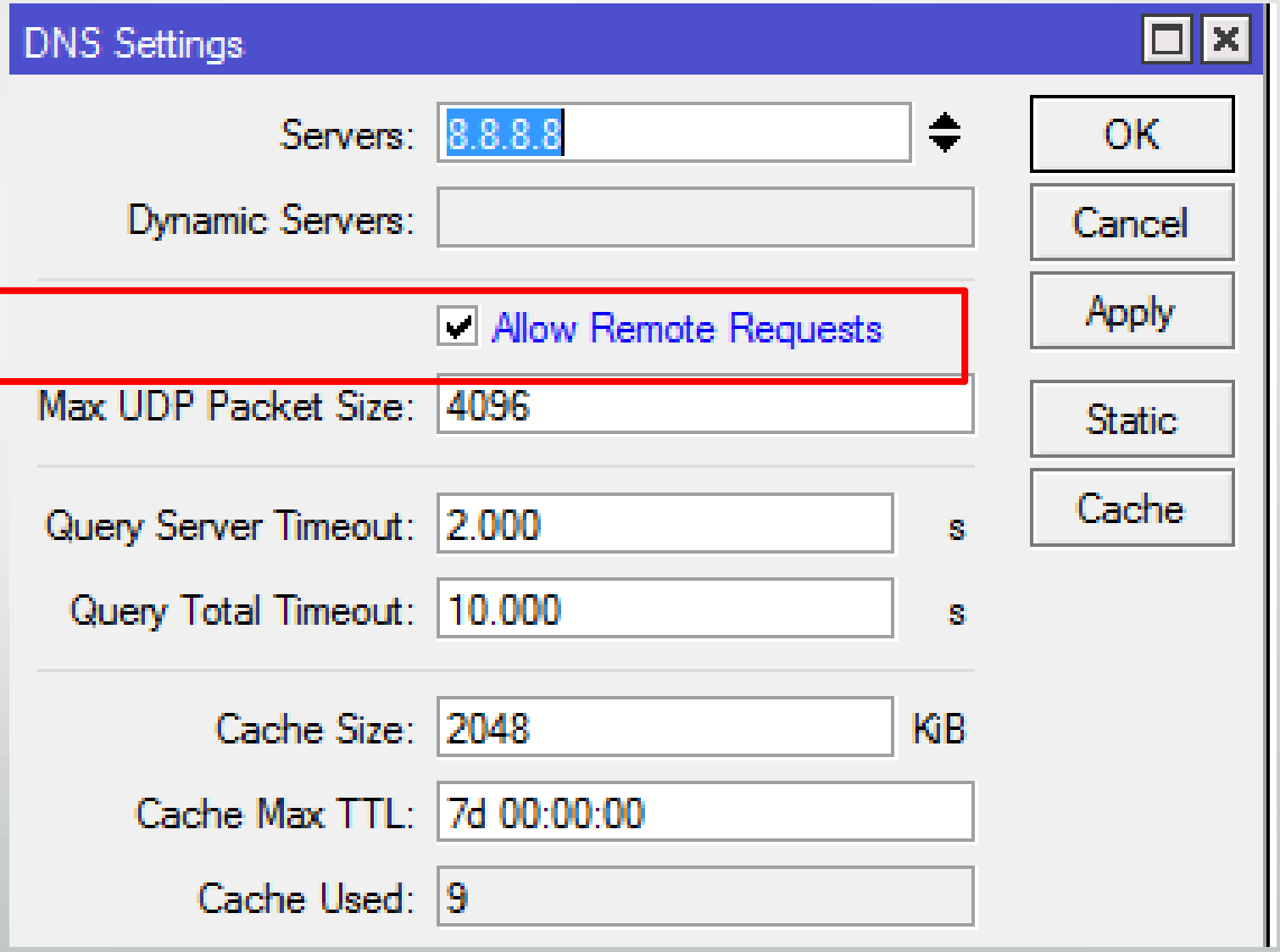
REGLAS BÁSICAS EN CHAIN INPUT

IP -> FIREWALL



DNS – ¡PRECAUCION!

IP -> DNS



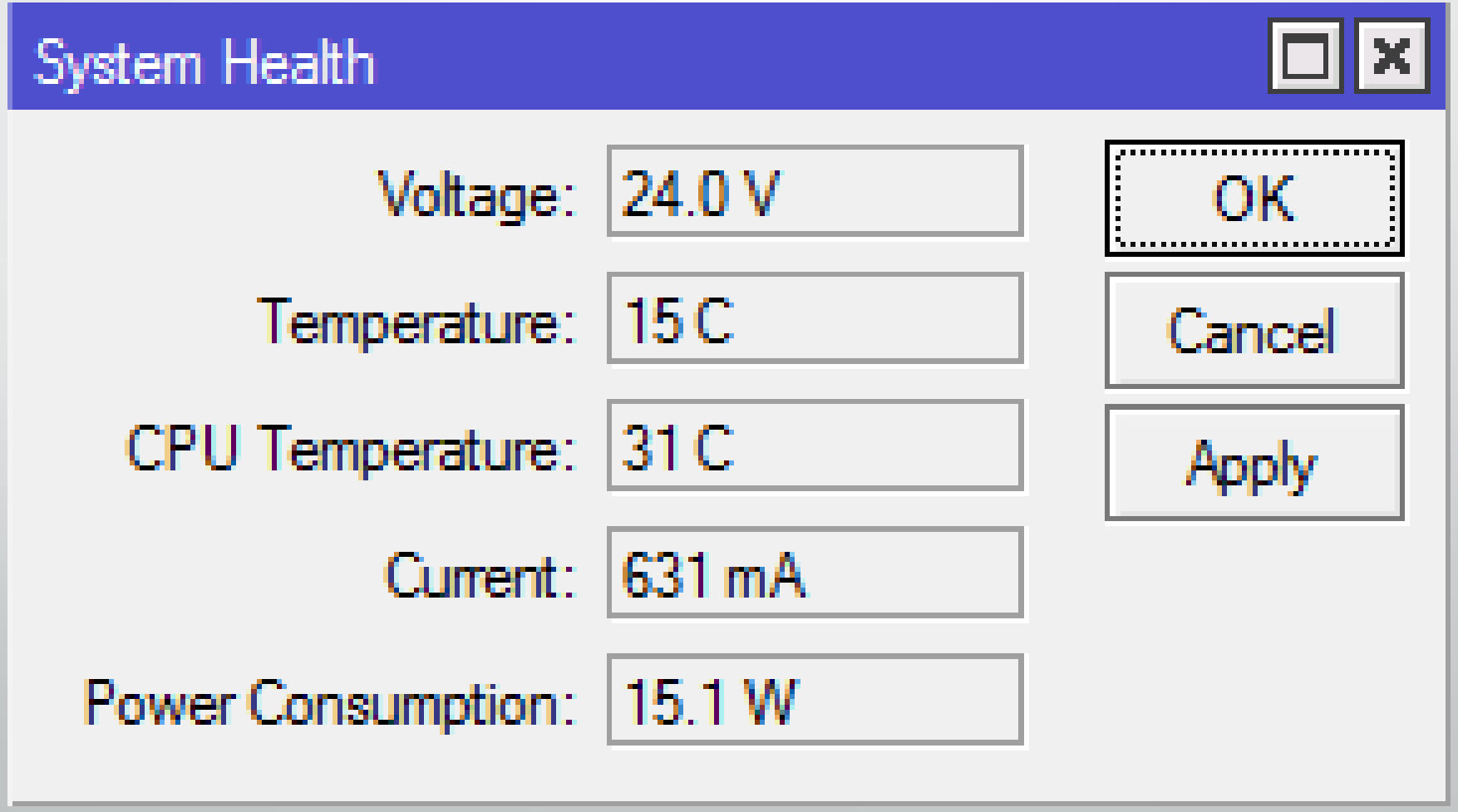
EcaTel SRL

HEALTH (Salud)
DEL ROUTER

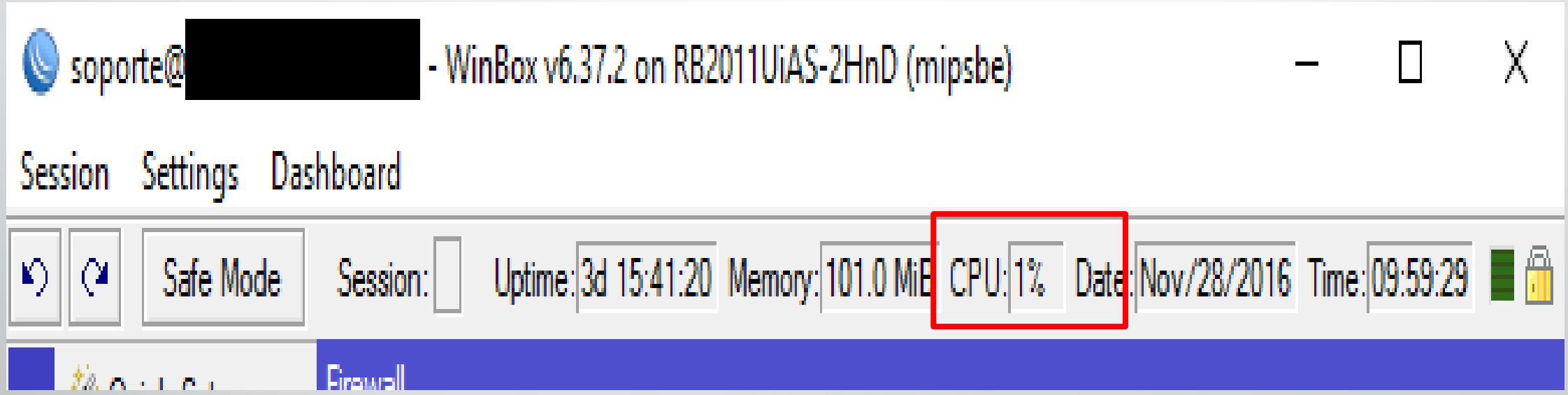
EcaTel SRL

INFORMACION BÁSICA DEL EQUIPO

System -> Health

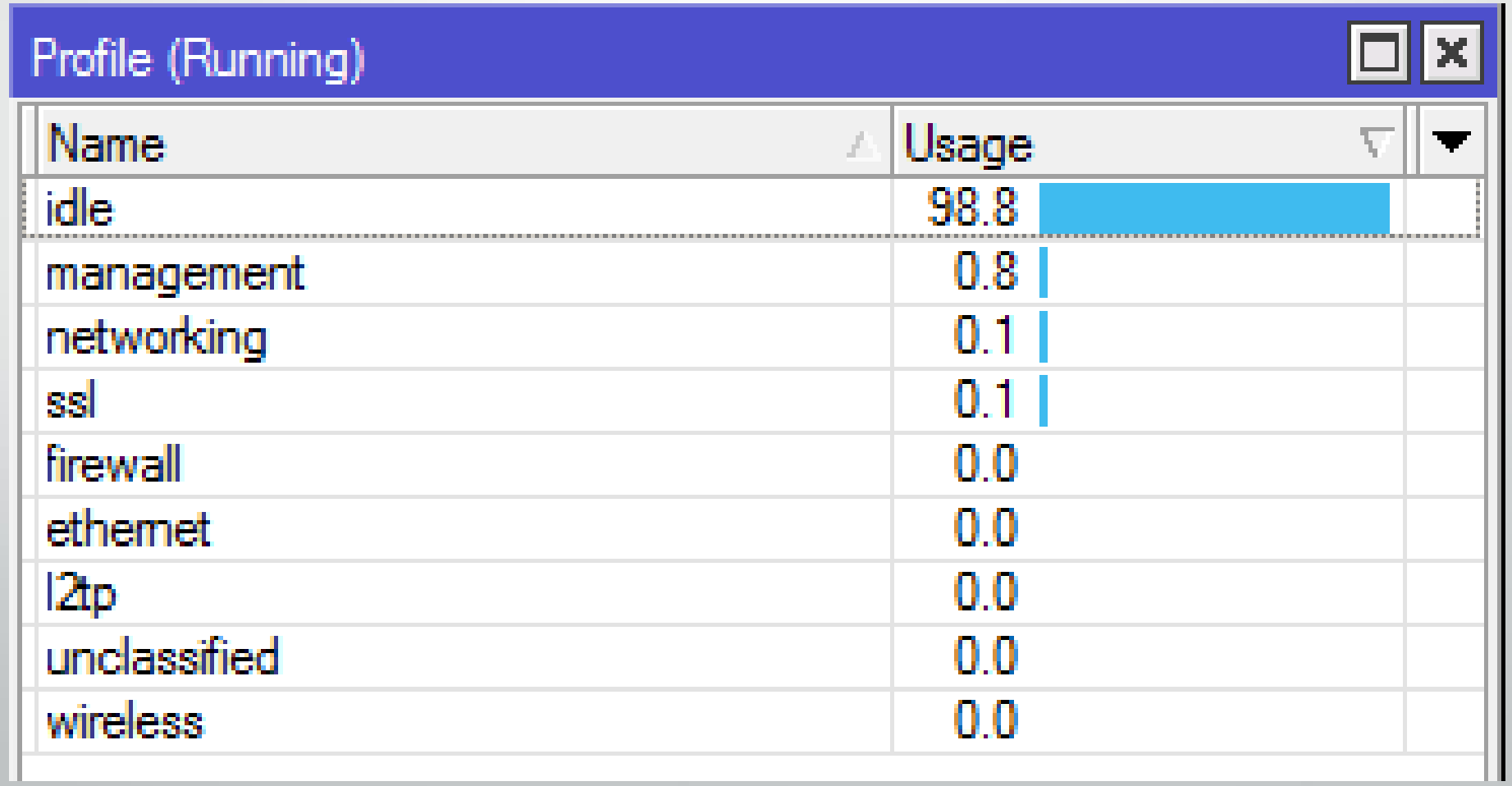


ESTADO DEL CPU DEL EQUIPO



¿COMO SE CONSUME EL CPU?

Tool -> Profile



SHOW TIME!

DEMOSTRACION