Optimix .com.ar
Internet Engineering

Detección de fallas en redes *MikroTik*


info@optimix.com.ar


+52 55 2904 9054


optimixnetworks

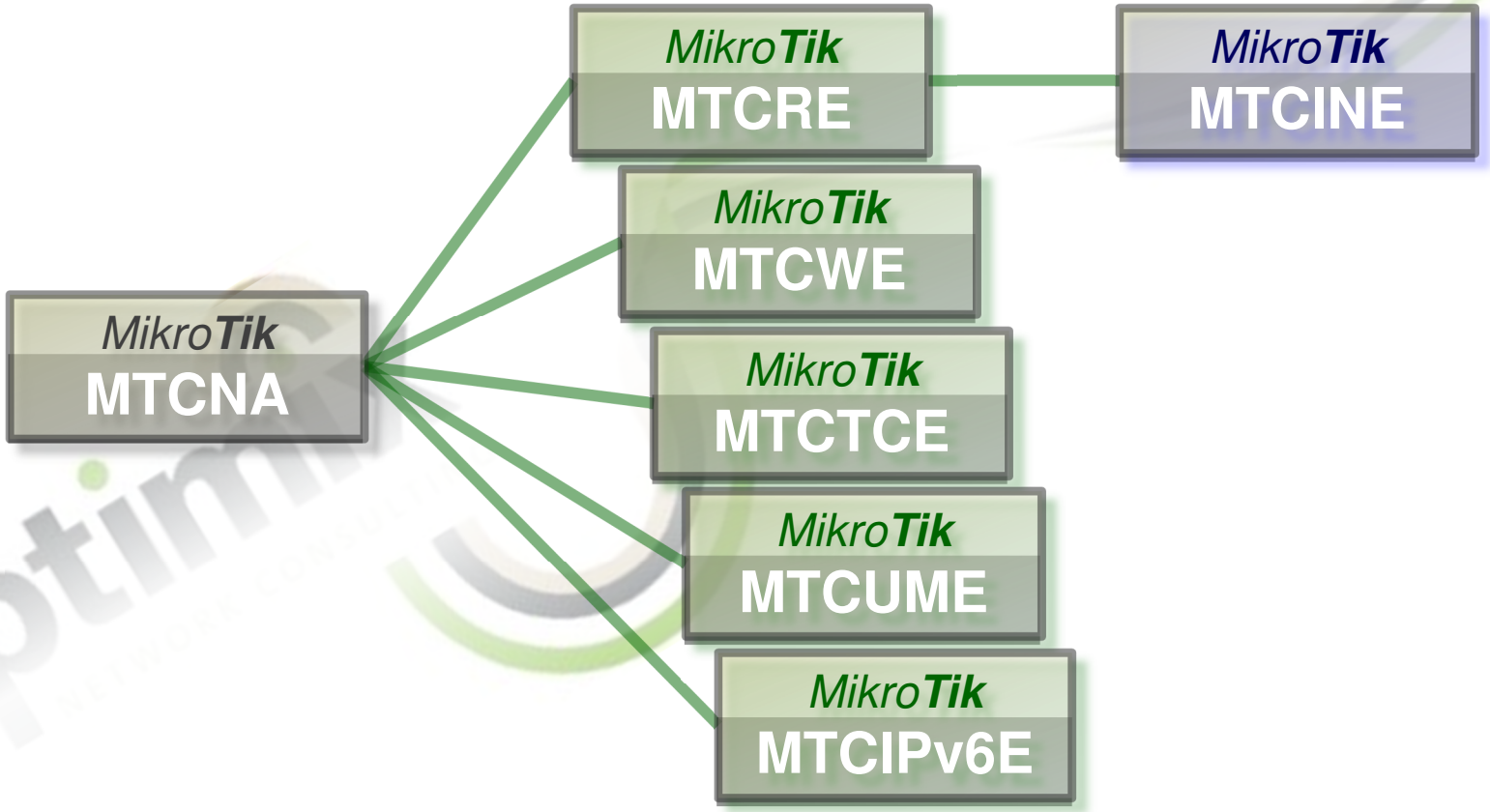
MikroTik MEXICO

Optimix para el ISP

- Guía técnica y marketing de ISPs:
  - Capacitación del personal de instalación inalámbrica y fibra óptica.
  - Capacitación del personal de atención telefónica.
  - Desarrollo y configuración de recursos de vinculación física (inalámbrica y fibra óptica), ruteo lógico integral incluyendo incumbentes (BGP).
  - Desarrollo y configuración de plataformas telefónicas de callcenter.
  - Desarrollo de solución administrativa comercial de ISPs, con facturación y suspensión de morosos.

Optimix para el Consultor

- Entrenamientos Oficiales *MikroTik*:



Objetivos de esta exposición

- Analizar distintas fallas que suelen presentarse en la red, y cómo apoyarse en las herramientas *Mikro**Tik*** RouterOS para diagnosticarlas.
- Proponer algunas técnicas para generar alarmas al administrador de la red, y advertirle las fallas mediante *Mikro**Tik*** RouterOS.

Entrenador – Ing. Jorge Filippo

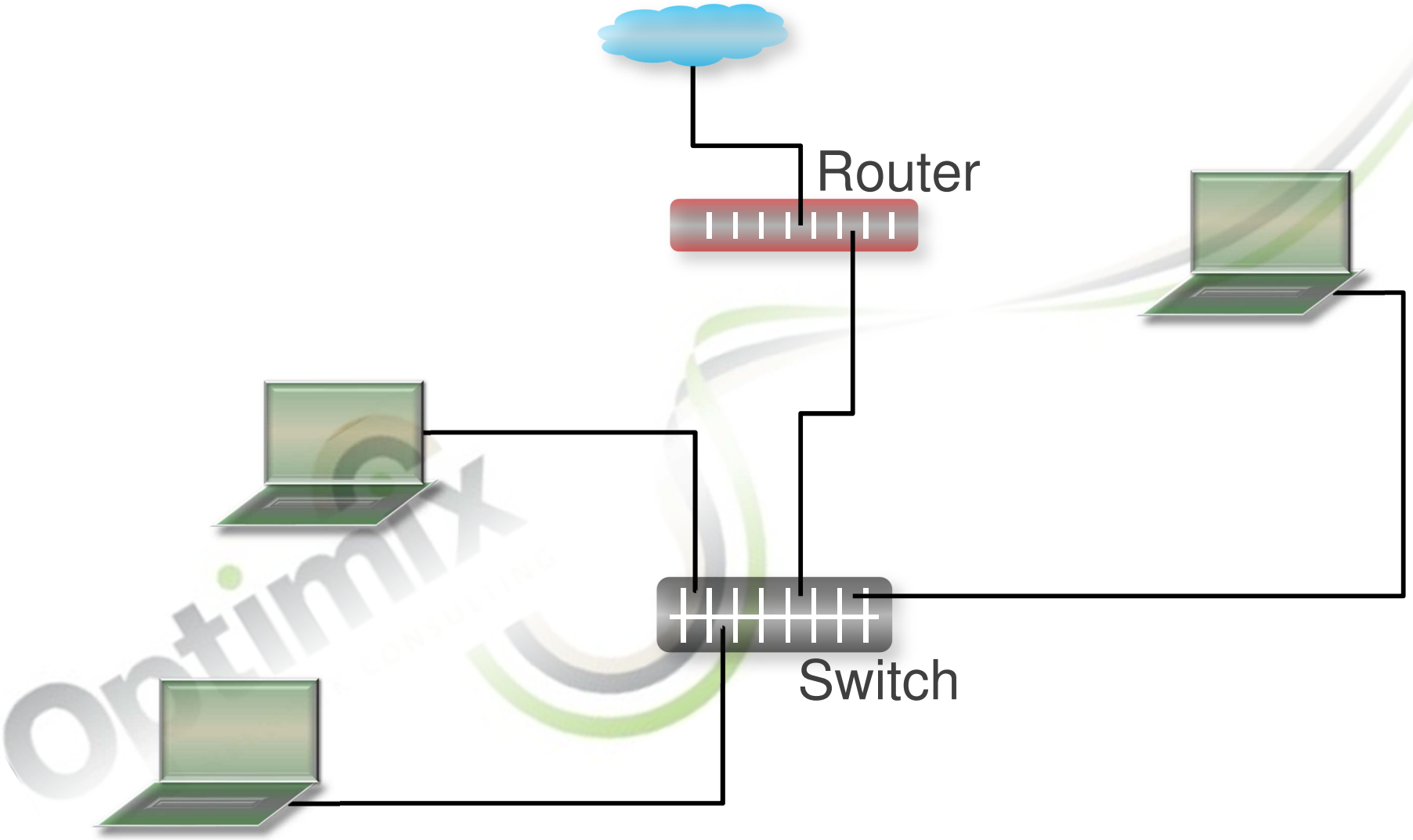
- Ingeniero en Electrónica (grado de 6 años, Universidad Tecnológica Nacional, Buenos Aires, 2005).
- Miembro I06485 del Consejo de Ingenieros COPITEC Argentina.
- Postgrado en Dirección de Empresas (Universidad Tecnológica Nacional, Buenos Aires, 2006).
- Entrenador Oficial 2011 MikroTik MTCNA, WE, RE, TCE, UME, INE.
- Entrenador Oficial 2012 Ubiquiti, 1ra, 2da y 3ra generación, UBWA y UEWA.
- Certificado Asterisk Issabel ICA 2017, Huawei HCNA 2018, DigiFort VideoVigilancia 2018, Cambium Networks ePMP 2017.
- Líder Estratégico de las principales redes mixtas latinoamericanas:
  - Red Dorsal Sonora – Red interestatal de gobierno gestionada desde Hermosillo, con ruteo bidireccional BGP en MikroTik, transportada por fibras punto a punto e inalámbricos.
  - GPON Berazategui – Red municipal, gestionada desde el Palacio Municipal, con más de 600 puntos con ruteo bidireccional MikroTik transportados por GPON.
  - VideoVigilancia Avellaneda – Red municipal MikroTik+Ubiquiti+DigiFort, gestionada desde el Centro de Monitoreo ciudadano, con más de 750 cámaras inalámbricas.
  - Redes WISP – Miles de usuarios, en múltiples ciudades, con MikroTik, Ubiquiti, Cambium Networks, Mimosa, Huawei, Furukawa, Cisco, Arista.

Optimix .com.ar
Internet Engineering

Recorriendo fallas!

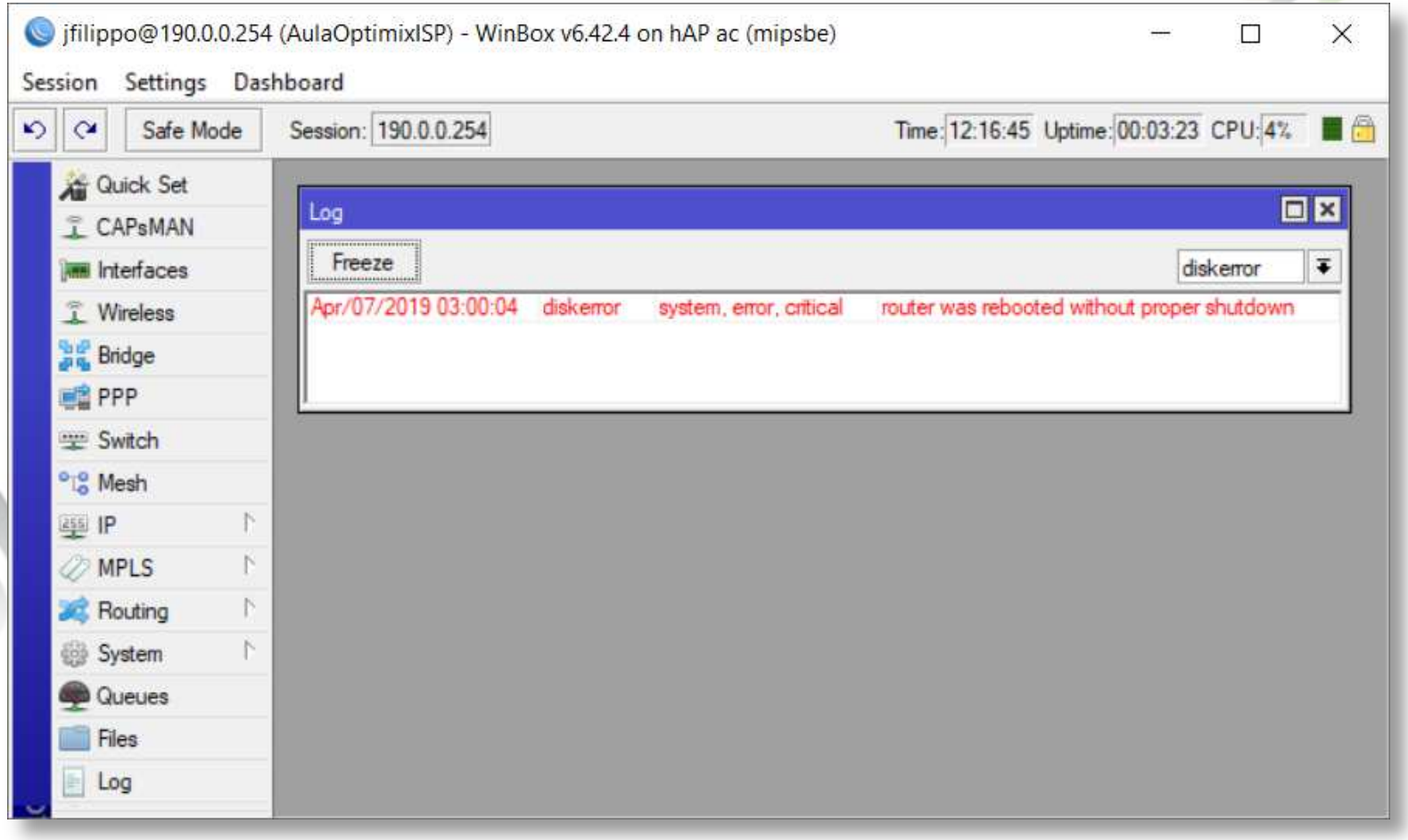
Distintas fallas o agresiones en recursos generales de red, y cómo detectarlas

1) Internet se corta *de a ratos*

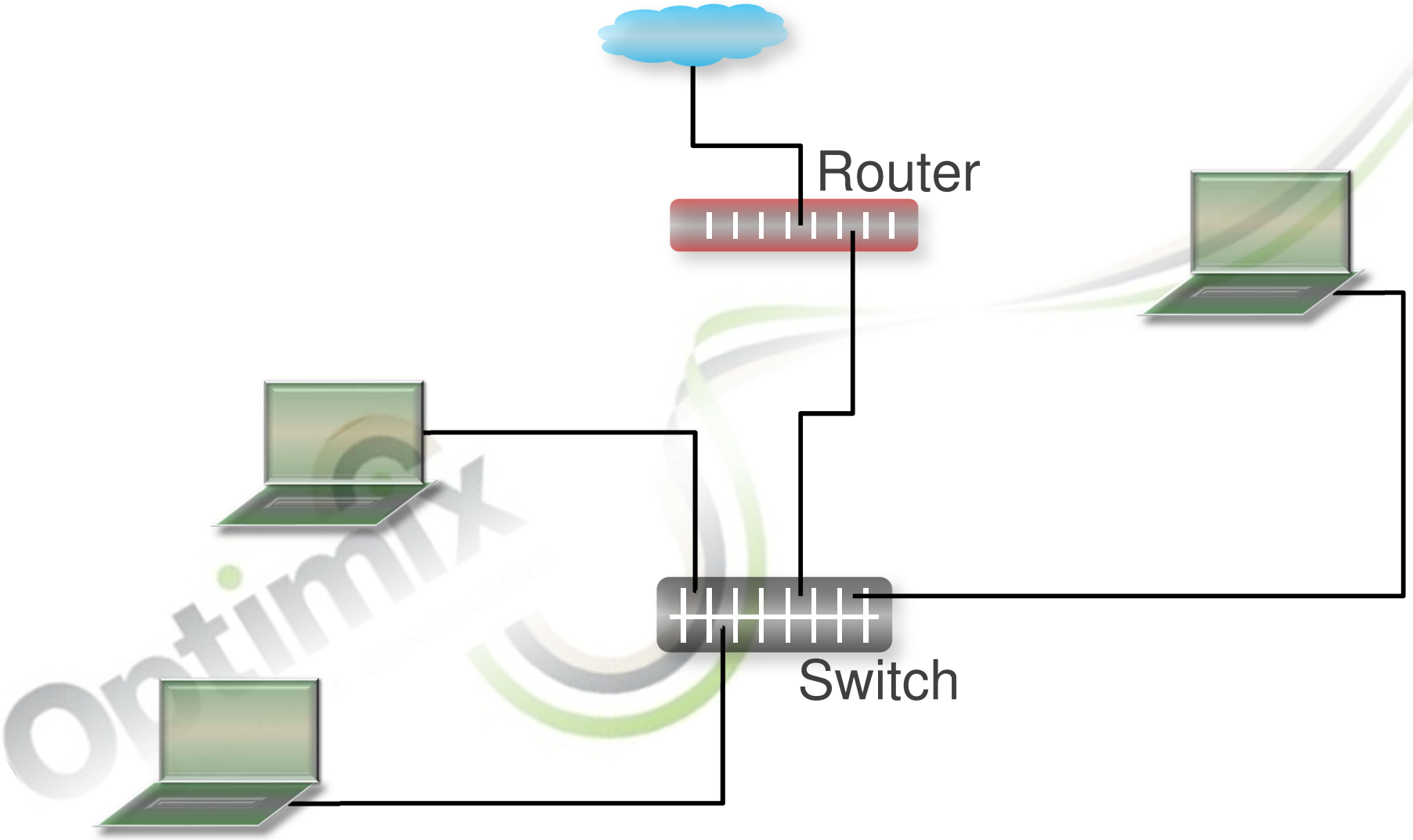


Logs

- En el menú ***Log***, tenemos los eventos que se produjeron en la red:



2) Internet se corta *para algunos*



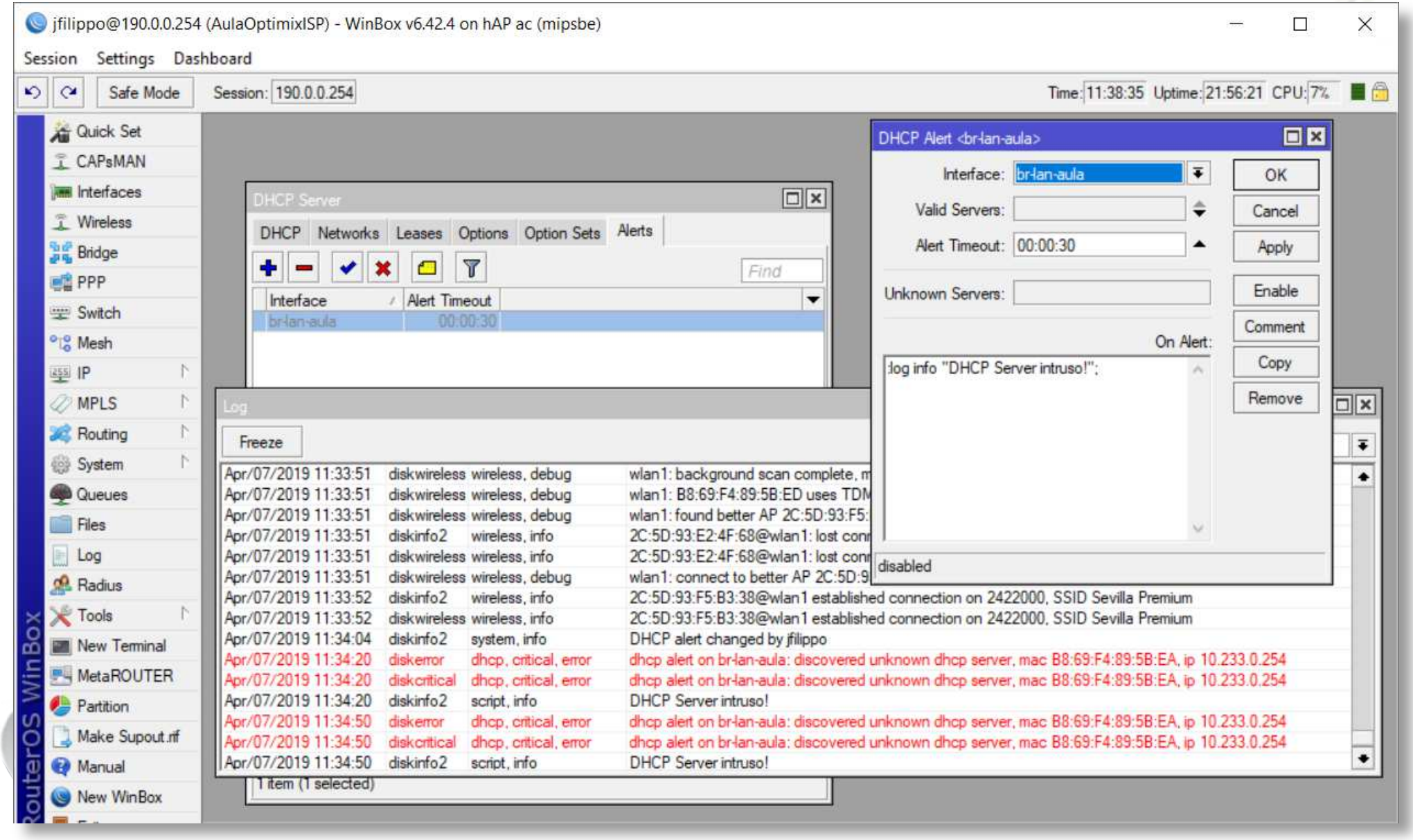
2) Internet se corta *para algunos*

- Tenemos una red con DHCP, y los usuarios están navegando.
- El técnico local nos llama, y nos informa que varias PCs se quedaron sin Internet.
- Ingresamos al router de borde, y vemos tráfico en la LAN coherente con la WAN.
- En la tabla ARP del router, vemos varias direcciones MAC registradas, y todo parece normal.

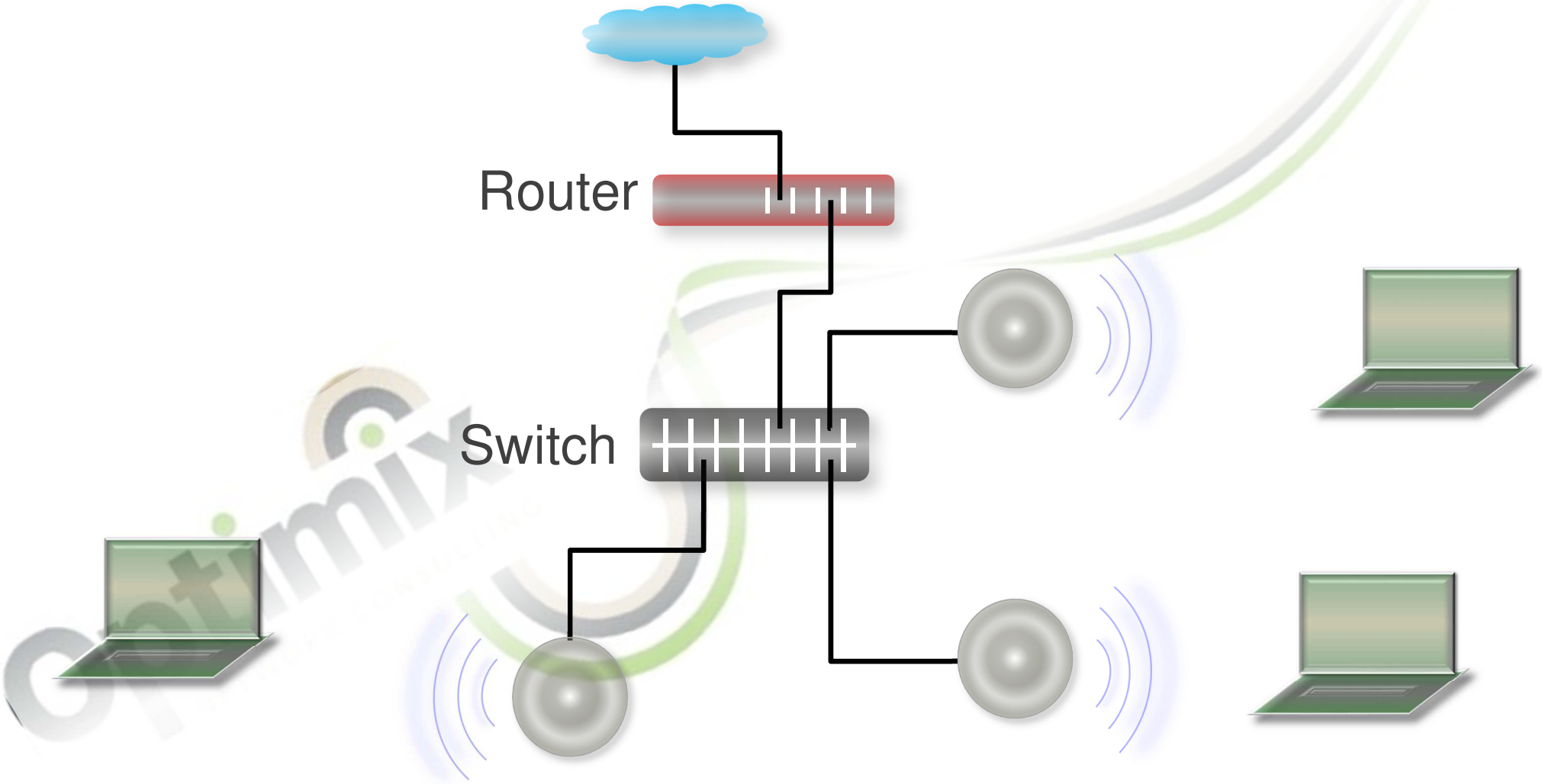
DHCP Server intruso, ***Alerts***

- Un servidor DHCP intruso, les brinda IP a algunas PCs, que se quedan sin Internet.
- Típicos intrusos son routers WiFi conectados mediante su puerto LAN, o DVRs con funciones de router que entregan DHCP.
- La detección se puede lograr publicando un ***DHCP Client*** en el mismo puerto en el que publicamos el ***DHCP Server***.
- La otra opción es utilizar los ***Alerts*** del ***DHCP***, que nos permiten disparar scripts.

DHCP Server intruso, ***Alerts***



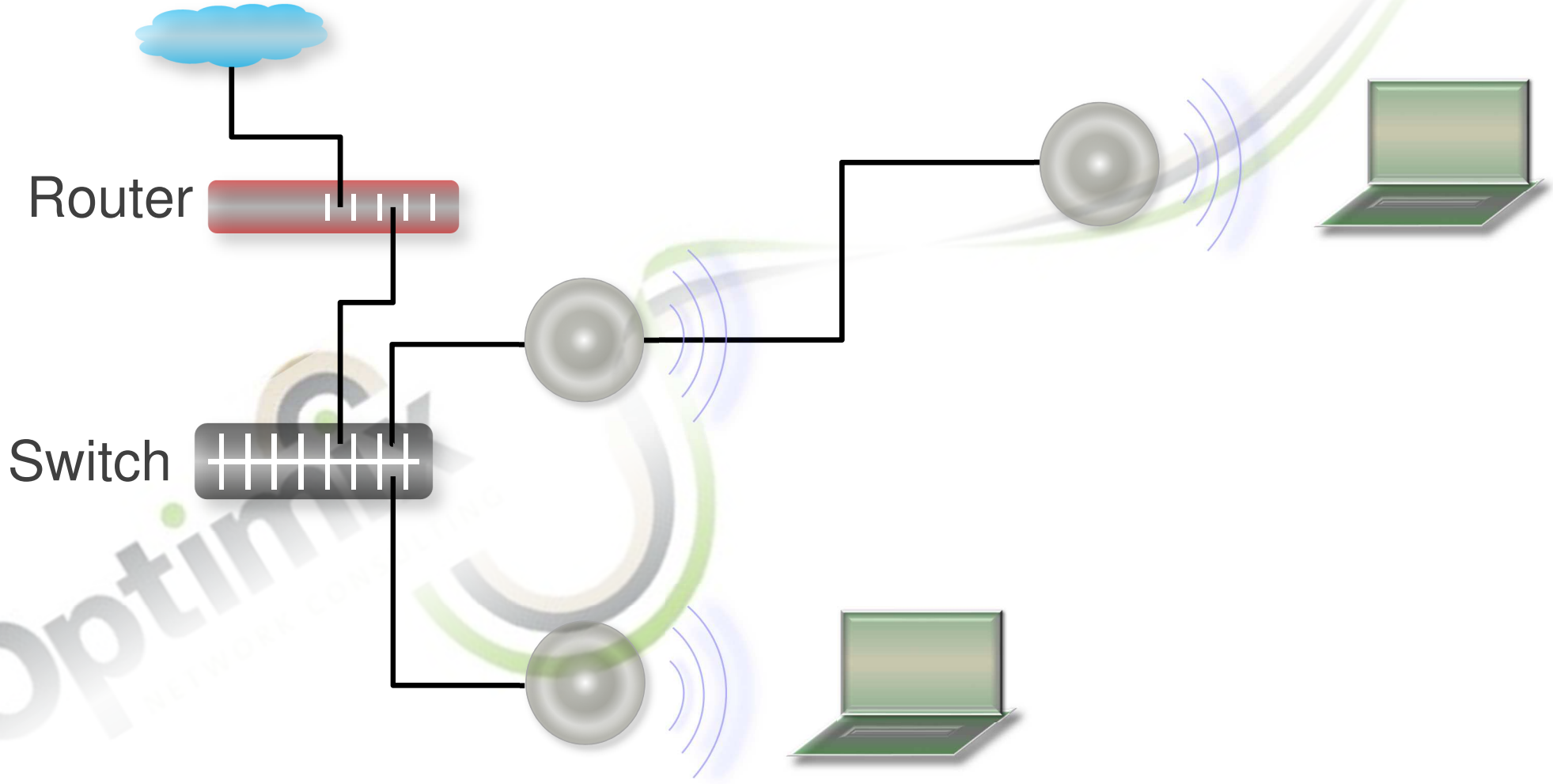
3) El *WiFi* se corta *para algunos*



3) El *WiFi* se corta *para algunos*

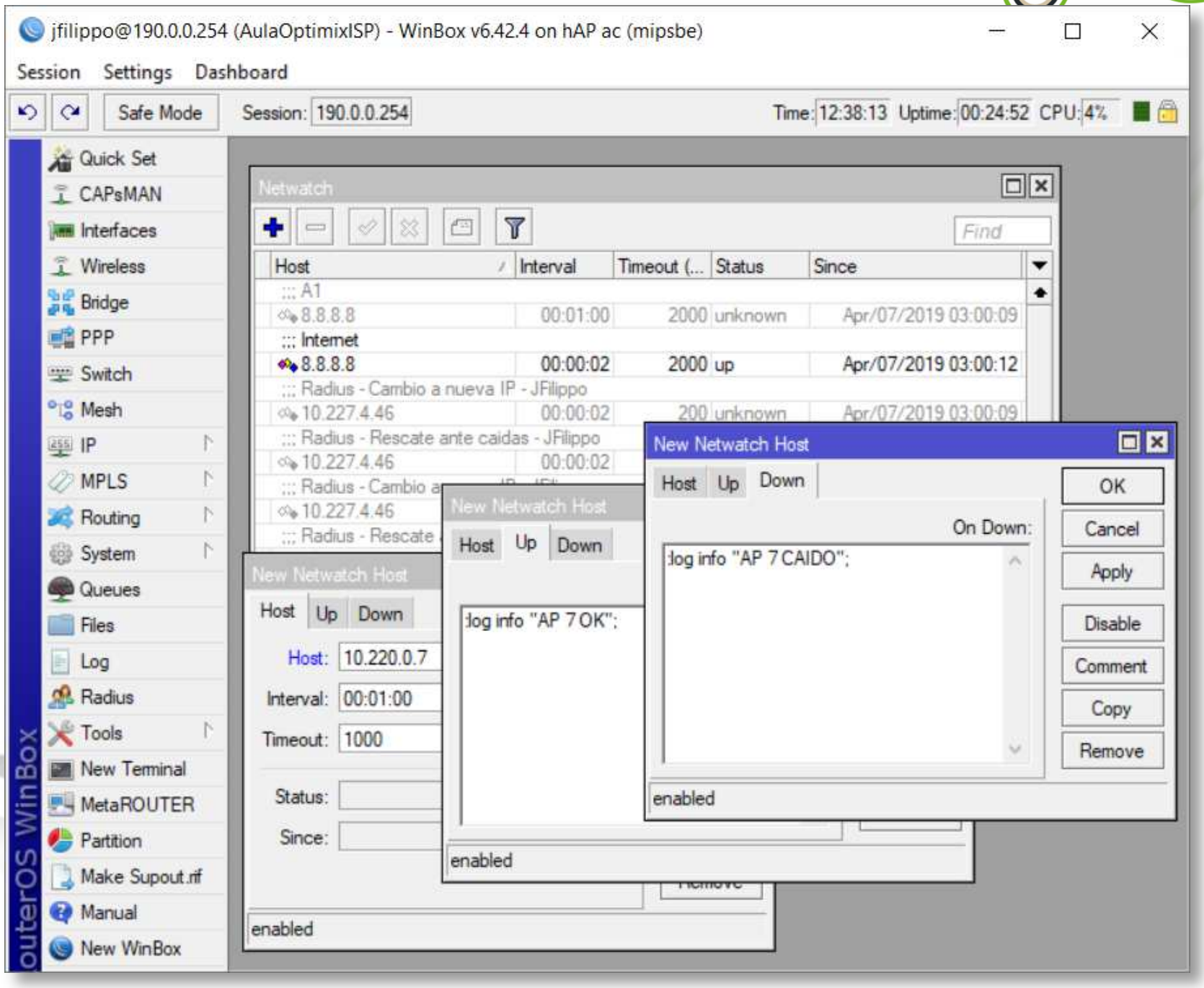
- Las interrupciones en el servicio WiFi, típicamente se asocian a debilidades en el wireless:
  - Saturación en las placas inalámbricas de los Access Points.
  - Interferencias externas, o autogeneradas entre Access Points.
- Incluso, cuando la población de usuarios es baja, se supone que el WiFi es el que falla.

3) El *WiFi* se corta *para algunos*



Tools*-> *Netwatch

- En el menú ***Tools***, submenú ***Netwatch***, dejamos monitoreando una IP, y al caerse/volver, ejecuta un script distinto para cada evento.
- El script también podría ejecutar el comando ***ping***, y verificar si la caída es momentánea o permanente, para que la interpretación de caída no se produzca por meras inestabilidades.
- Los scripts de ***Netwatch*** no tienen privilegios ilimitados, pero pueden encender ***Scheduler***s, que sí pueden tenerlos.


jfilippo@190.0.0.254 (AulaOptimixISP) - WinBox v6.42.4 on hAP ac (mipsbe)
Session Settings Dashboard
Safe Mode
Session: 190.0.0.254
Time: 12:38:13 Uptime: 00:24:52 CPU: 4%
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Partition
Make Supout.rif
Manual
New WinBox
RouterOS WinBox
Netwatch
Find
Host
Interval
Timeout (...
Status
Since
::: A1
8.8.8.8 00:01:00 2000 unknown Apr/07/2019 03:00:09
::: Internet
8.8.8.8 00:00:02 2000 up Apr/07/2019 03:00:12
::: Radius - Cambio a nueva IP - JFilippo
10.227.4.46 00:00:02 200 unknown Apr/07/2019 03:00:09
::: Radius - Rescate ante caidas - JFilippo
10.227.4.46 00:00:02
New Netwatch Host
Host Up Down
Host: 10.220.0.7
Interval: 00:01:00
Timeout: 1000
Status:
Since:
enabled
log info "AP 7 OK";
log info "AP 7 CAIDO";
On Down:
OK
Cancel
Apply
Disable
Comment
Copy
Remove

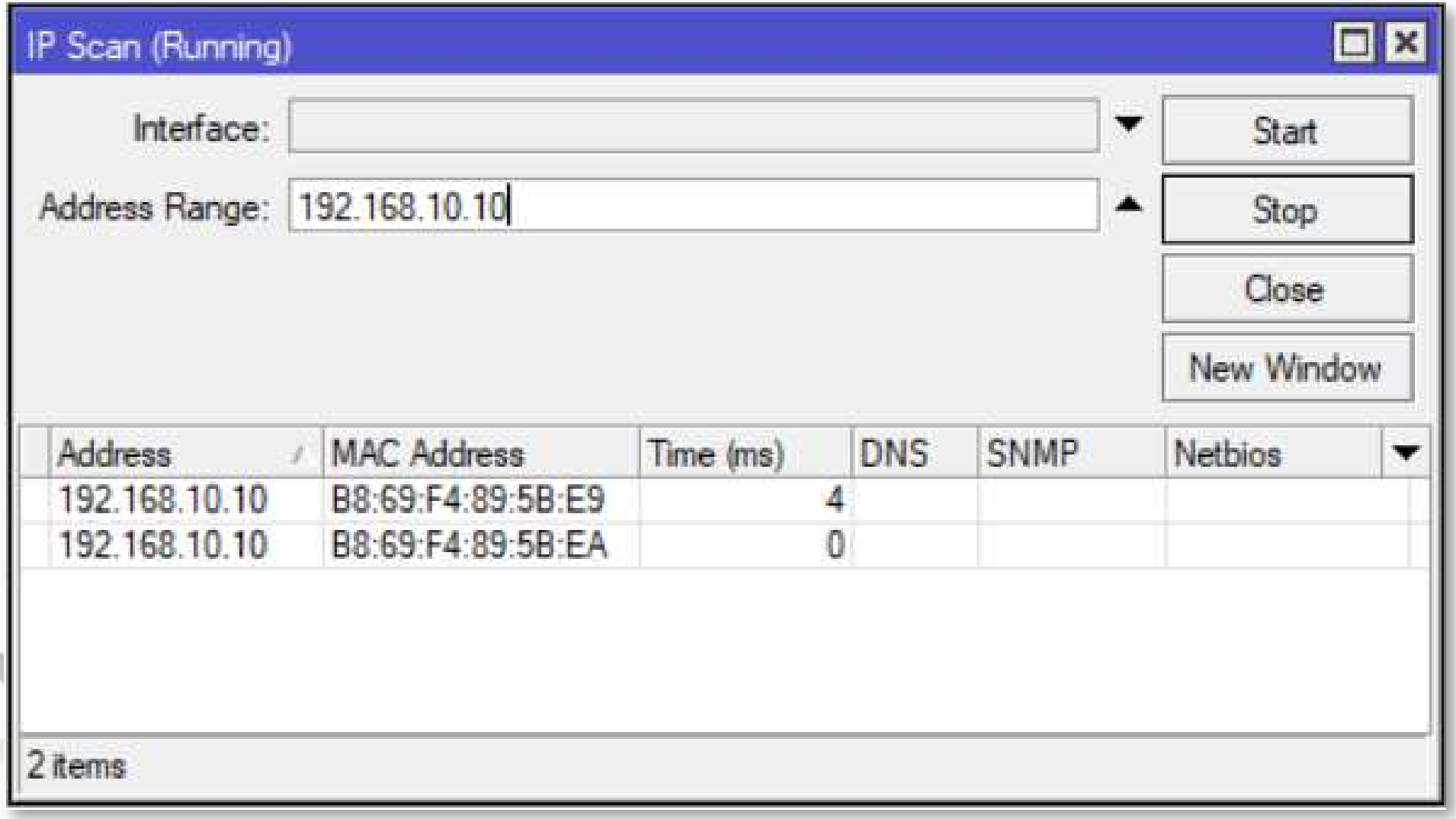
4) *Internet* se corta para *una* PC

- Un usuario dice que no tiene Internet.
- Su conexión física está okey, pero no tiene Internet.
- Verificamos su dirección IP, y está correcta, pero no logramos hacer ping al gateway.
- Nos bajamos el ***Winbox***, y vemos el MikroTik por ***Neighbor***s, pero no navega.

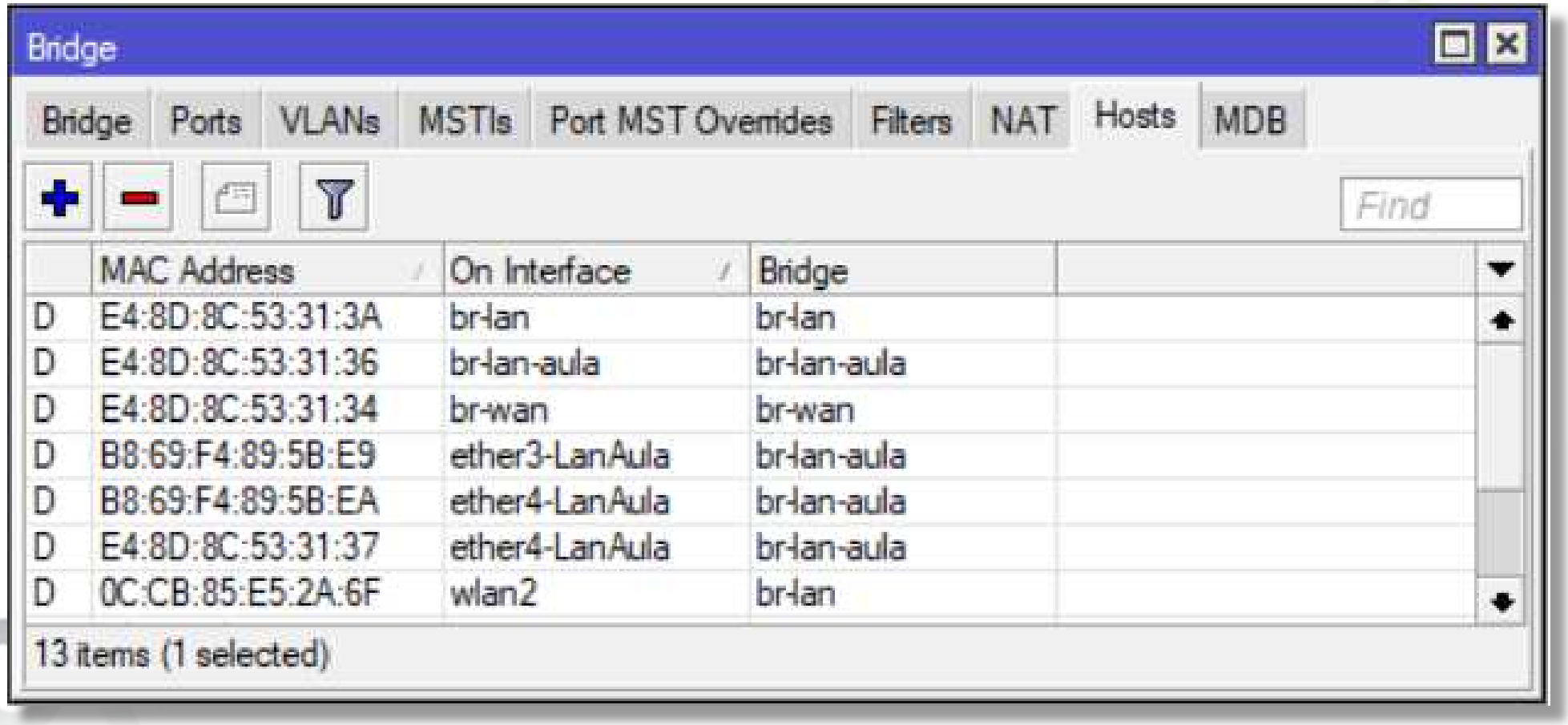
Conflicto de IP

- Los conflictos de IP, producen:
  - Que los usuarios acudan a un gateway que no brinda Internet (si la conflictuada es la IP gateway).
  - Que un usuario no pueda comunicarse con el gateway (si la conflictuada es la IP de la PC).
- Nuestra misión tiene dos desafíos:
  - Detectar la MAC del dispositivo que nos produce el conflicto de IP.
  - Detectar la ubicación, o a qué puerto ethernet está conectado, dicho dispositivo infractor.

Conflicto de IP, ***IP Scan***



Conflicto de IP, ***Bridge***, ***Hosts***



5) La LAN anda lento/mal

- Tenemos una operación WISP con paneles sectoriales, y los usuarios de uno de los paneles, acusan lentitud.
- Al ingresar al panel, vemos que los niveles de ruido están bien, y los niveles de señal también.
- Pero desde el router de servicio a los clientes, hay mucha latencia, y la velocidad de la interface nunca supera los 10Mb/s o los 100Mb/s.

Registración ethernet

- Si un puerto ethernet se registra a 10Mb/s, cuando la necesidad es 100Mb/s, o se registra a 100Mb/s cuando la necesidad es gigabit, tendremos saturación.
- El problema de esta falla, es que suele ser inconstante, por lo que necesitamos un proceso automático que monitoree periódicamente (ej: cada 10 minutos) la interface, y actúe (ej: deshabilite y vuelva a habilitar la interface).

Registración ethernet

```
:local myPort "ether1-Panel1 ";
:local myPingIp "10.227.36.101/27";
:local myComment "FS-AViveroRTS2";
:local myNormal "1Gbps";
#:local myNormal "100Mbps";

:log info ("Se inicia la verificacion del puerto ".$myPort);

/interface ethernet monitor $myPort once do {
    :if ($rate!=$myNormal) do {
        :log info ("Detecta ".$myPort." a algo que no es ".$myNormal);
        /interface ethernet set $myPort auto-negotiation=no;
        :delay 5;
        :log info ("Deshabilita la interface ".$myPort);
        /interface ethernet disable $myPort;
        :delay 5;
        :log info ("Rehabilita la interface ".$myPort);
        /interface ethernet enable $myPort;
        /interface ethernet set $myPort auto-negotiation=yes;
        :delay 20;
        /interface ethernet monitor $myPort once do {
            :if ($rate!=$myNormal) do {
                /ip address disable [find address=$myPingIp];
            }
        }
    }
```

Registración ethernet

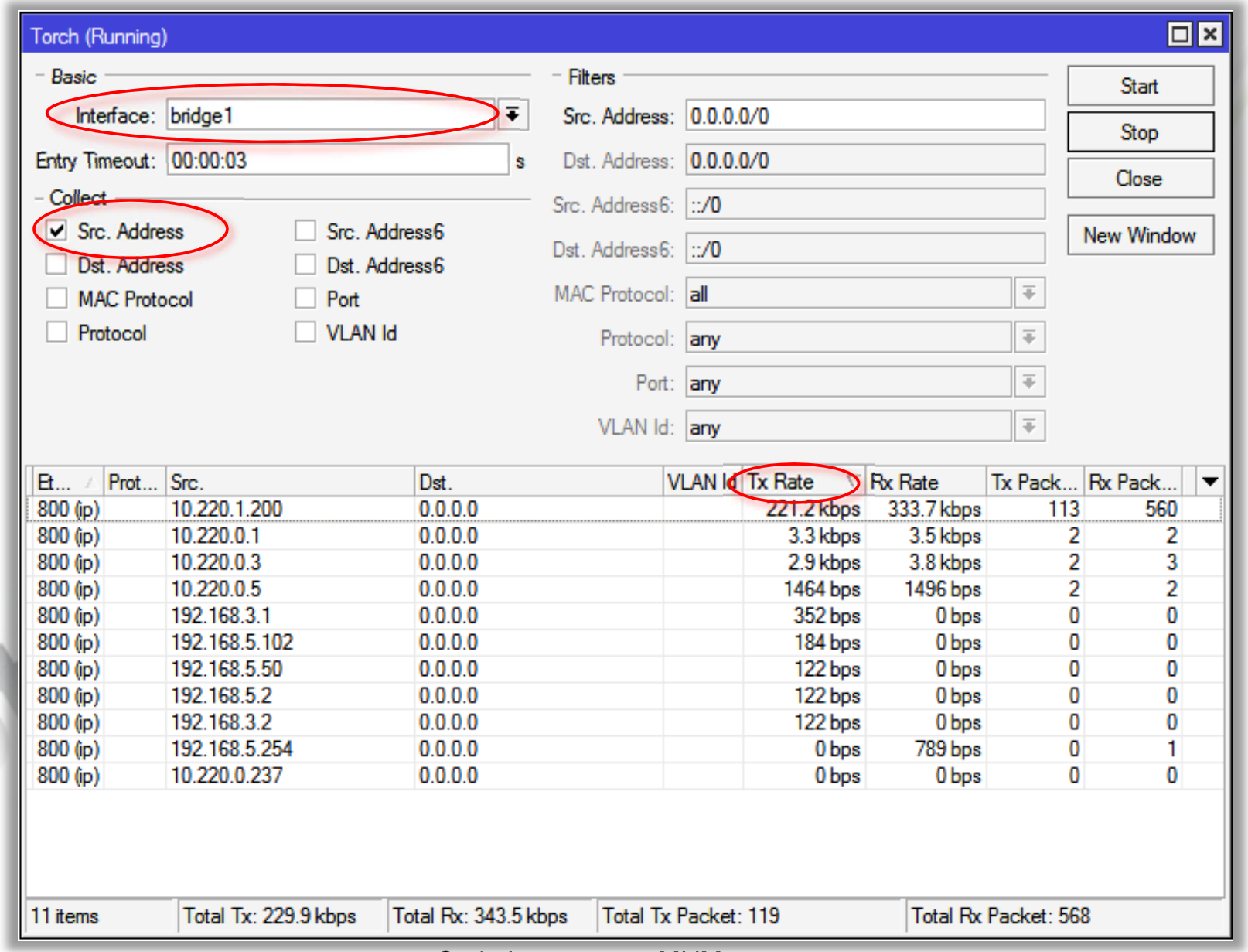
```
:if ($rate=$myNormal) do {
        :log info (" - ".$myComment." ".$myPort." a ".$myNormal);
        /ip address rem [find address=$myPingIp];
        /ip address add address=$myPingIp interface=alo comment=("IP monitoreo ".$myPort);
        :log info ("Detecta ".$myPort." Ok a ".$myNormal);
        quit;
    }
}

:log info ("Termina la verificacion del puerto ".$myPort);
/quit;
```

- En este script, la interface **`alo`** es un bridge sin puertos, que se crea solo para que albergue la IP de monitoreo.

6) Internet anda lento

- La velocidad de Internet en la empresa sigue siendo insufrible a pesar de que en los últimos meses se pidieron dos aumentos de ancho de banda.
- Simultáneamente, el empleado más risueño de la empresa, sigue ofreciendo cada día una mayor variedad de películas que él mismo descarga.
- Es momento de estudiar cuál es el ancho de banda habitual que consumen nuestros usuarios.
- ***Torch***, es una herramienta que nos permite ver fácil y rápidamente, el consumo de todos nuestros usuarios, presentándolos de mayor a menor!

Tools-> Torch


Torch (Running)
Basic
Interface: bridge1
Entry Timeout: 00:00:03 s
Collect
Src. Address
Dst. Address
MAC Protocol
Protocol
Src. Address6
Dst. Address6
Port
VLAN Id
Filters
Src. Address: 0.0.0.0/0
Dst. Address: 0.0.0.0/0
Src. Address6: ::/0
Dst. Address6: ::/0
MAC Protocol: all
Protocol: any
Port: any
VLAN Id: any
Start
Stop
Close
New Window
Et... Prot... Src. Dst. VLAN Id Tx Rate Rx Rate Tx Pack... Rx Pack...
800 (ip) 10.220.1.200 0.0.0.0 221.2 kbps 333.7 kbps 113 560
800 (ip) 10.220.0.1 0.0.0.0 3.3 kbps 3.5 kbps 2 2
800 (ip) 10.220.0.3 0.0.0.0 2.9 kbps 3.8 kbps 2 3
800 (ip) 10.220.0.5 0.0.0.0 1464 bps 1496 bps 2 2
800 (ip) 192.168.3.1 0.0.0.0 352 bps 0 bps 0 0
800 (ip) 192.168.5.102 0.0.0.0 184 bps 0 bps 0 0
800 (ip) 192.168.5.50 0.0.0.0 122 bps 0 bps 0 0
800 (ip) 192.168.5.2 0.0.0.0 122 bps 0 bps 0 0
800 (ip) 192.168.3.2 0.0.0.0 122 bps 0 bps 0 0
800 (ip) 192.168.5.254 0.0.0.0 0 bps 789 bps 0 1
800 (ip) 10.220.0.237 0.0.0.0 0 bps 0 bps 0 0
11 items
Total Tx: 229.9 kbps
Total Rx: 343.5 kbps
Total Tx Packet: 119
Total Rx Packet: 568

7) Todo anda lento

- Cuando se desarrollan redes extensas en capa 2, los loops eventuales pueden hacerla colapsar.
- Pueden producirse incongruencias ARP en la red, que solemos resolver reiniciando todos los equipos.
- En *MikroTik*, podemos hacer una limpieza de las tablas ARP, borrándolas en ***IP***, ***ARP*** (entrando por Winbox), o conectándonos por consola y ejecutando:

```
/ip arp remove [find]
```

8) Internet sigue lento

- Cuando creemos que nuestro proveedor no nos brinda el ancho de banda prometido, necesitamos realizar pruebas de stress para verificarlo.
- El problema radica cuando:
  - Debemos iniciar un reclamo estando lejos del sitio donde tenemos el servicio defectuoso.
  - El proveedor nos pide desconectar nuestro router del borde, y conectar directamente una PC.
- Algo vital en estos casos, es ser convincente asegurándole al operador técnico que nos atendió, que estamos físicamente en el domicilio, y que tenemos nuestra PC directamente conectada!

Tools -> Fetch

- Cuando nuestro proveedor nos restringe el ancho de banda más allá de lo prometido, necesitamos realizar pruebas de stress para analizarlo.
- Para eso, *Mikro**Tik*** nos brinda un comando, mediante el cual podemos descargar archivos Web, directamente desde el router, para producir ese stress!

```
tool fetch url="http://sftp.fibertel.com.ar/services/file-50MB.img"
      status: finished
  downloaded: 51200KiB
       total: 51200KiB
    duration: 6s
```

Optimix .com.ar
Internet Engineering

Registro y Alarmas!

Para estar al tanto de lo que pasa en la red!

Siempre un paso adelante

- Para diagnosticar la red, tenemos que enterarnos de lo que le ocurre, mediante un Registro, o una Alarma.
- El Registro natural es el ***Log***, que debemos modificar para que se guarde en disco, y no en RAM.
- Pero a veces, necesitamos de Alarmas, mediante la recepción de un email, o inhibiendo la respuesta al ping (que es la herramienta natural de monitoreo de un recurso).

Logs

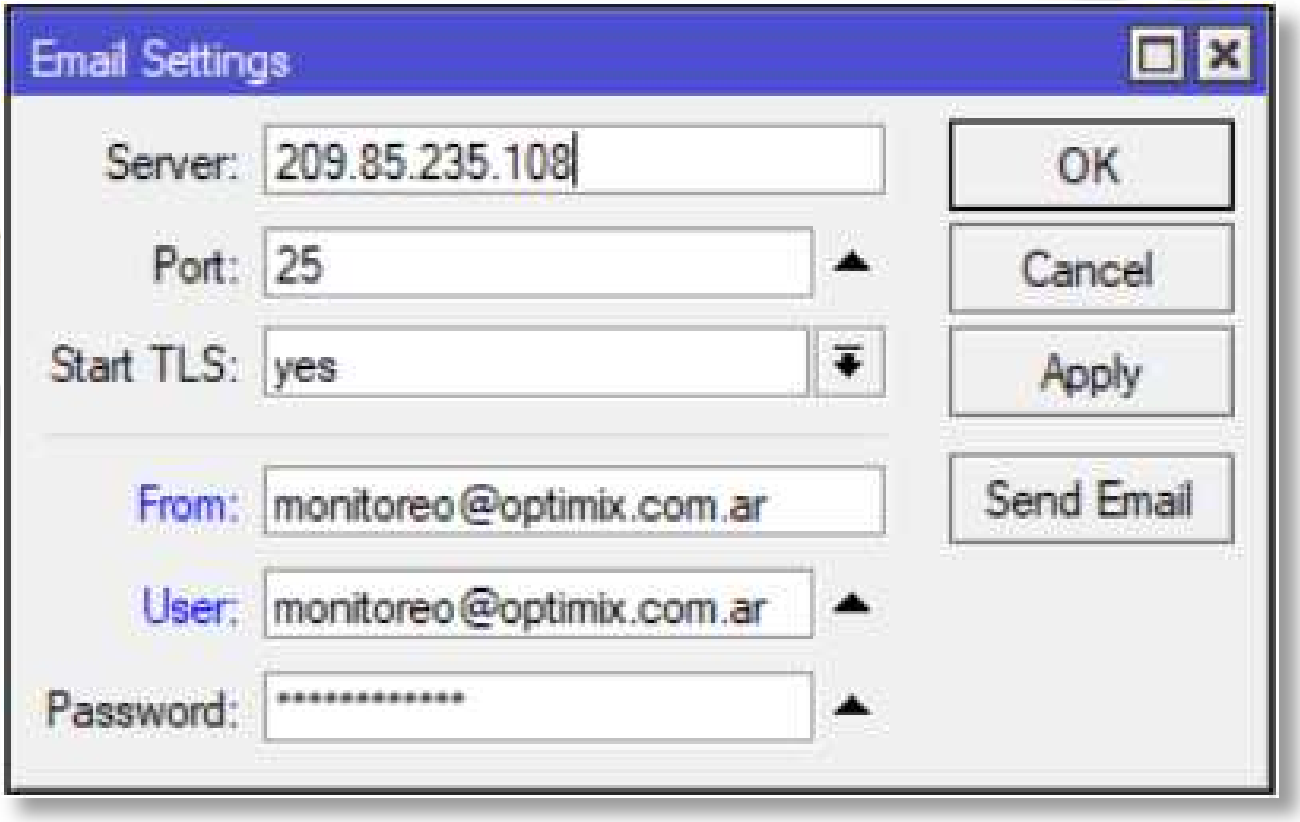
- Los ***Log***s, guardan por defecto los eventos en el router, pero además podemos escribir en ellos mediante un script, para dejar nuestro registro intencional.

```
:log info "Internet CAIDO – Proveedor Aaaa";
```

```
:log info "Internet OK – Proveedor Aaaa";
```

E-mail

- Primero, configurar la cuenta de email en el *Mikro**Tik***, desde el menú ***Tools***, submenú ***Email***:



E-mail

- Y se usa mediante scripts:

```
:local Puerto "sfp01-Troncal";
:local Nota "MiRouter";

:log info "Comienza el envio del email";

/tool e-mail send to=noc@optimix.com.ar from=monitoreo@optimix.com.ar \
     subject=([/system identity get name]." ".$Nota." ".$Puerto." OK");

:log info "Email enviado con exito";
```

Ping caído

- Encender una regla de ***Firewall Filter***, hace que el router deje de contestar el ping destinado a una IP creada para esta alarma.

```
:local Ip "1.2.3.4";
:local Nota "Bloqueo el ping porque algo paso";

:log info "Comienza creacion de regla de firewall";

/ip firewall filter add chain=input dst-address=$Ip protocol=icmp \
                        action=drop place-before=0 comment=$Nota

:log info "Regla de firewall creada con exito";
```

Ping levantado nuevamente

- Eliminar aquella regla de ***Firewall Filter***, hace que el router vuelva a contestar el ping.

```
:local Ip "1.2.3.4";
:local Nota "Restauracion del ping";

:log info "Comienza eliminacion de regla de firewall";

/ip firewall filter remove [find chain=input dst-address=$Ip];

:log info "Regla de firewall eliminada con exito";
```

Optimix .com.ar
Internet Engineering

Conclusiones

Lo que no se ve, no existe!

- Para ver lo que ocurre/ocurrió en la red, debemos hacer que los eventos se registren.
- Este es el comienzo de la detección de fallas.
- Como siempre, en los ***Entrenamientos Oficiales Optimix***, se profundiza el análisis de fallas y configuraciones, en base a las necesidades que comparte cada alumno!
- Los scripts y mensajes, informan, y el conocimiento, corrige!

Entrenamientos Optimix Internet Engineering
MikroTik-México PreMUM 2019

Optimix .com.ar
Internet Engineering

Gracias!


info@optimix.com.ar


+52 55 2904 9054


optimixnetworks

MikroTik MEXICO