



Utilizando RouterOS para capturar paquetes

Angel Velasco
angelvelpaz@gmail.com

MUM Uruguay 2017

Agenda

- **Introducción**
- **Objetivos**
- **Captura de paquetes**
- **Herramientas para capturar paquetes**
 - Packet Sniffer
 - TCPDump
- **Capturando tramas por la interfaz inalámbrica**
- **Wireshark**
- **Conclusiones**

Esta exposición presenta el uso de la herramienta *packet sniffer* incluida en routerOS para la captura de paquetes, y su posterior análisis.

En múltiples ocasiones los administradores de red o encargados de IT se enfrentan a problemas relacionados con la conectividad de los equipos que se encuentran conectados a la red, lo que puede generar varios dolores de cabeza tanto al encargado como al usuario.

Introducción

Mostrar el funcionamiento de la herramienta Packet Sniffer.

Proponer escenarios para el uso de Packet Sniffer.

Mostrar los inconvenientes relacionados con la captura de paquetes

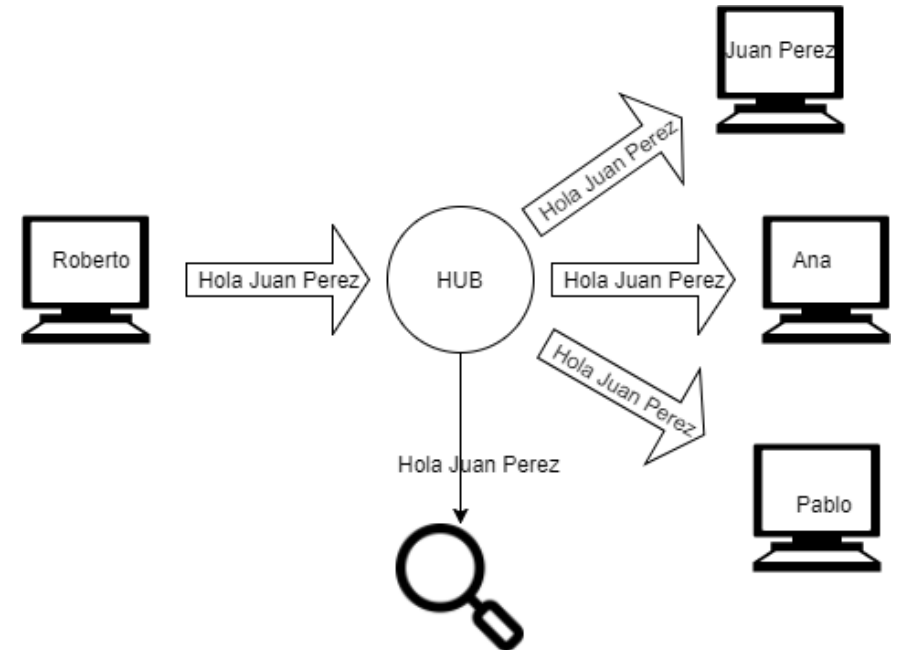
Proponer el uso de Wireshark como herramienta de apoyo para solucionar problemas.

Objetivos

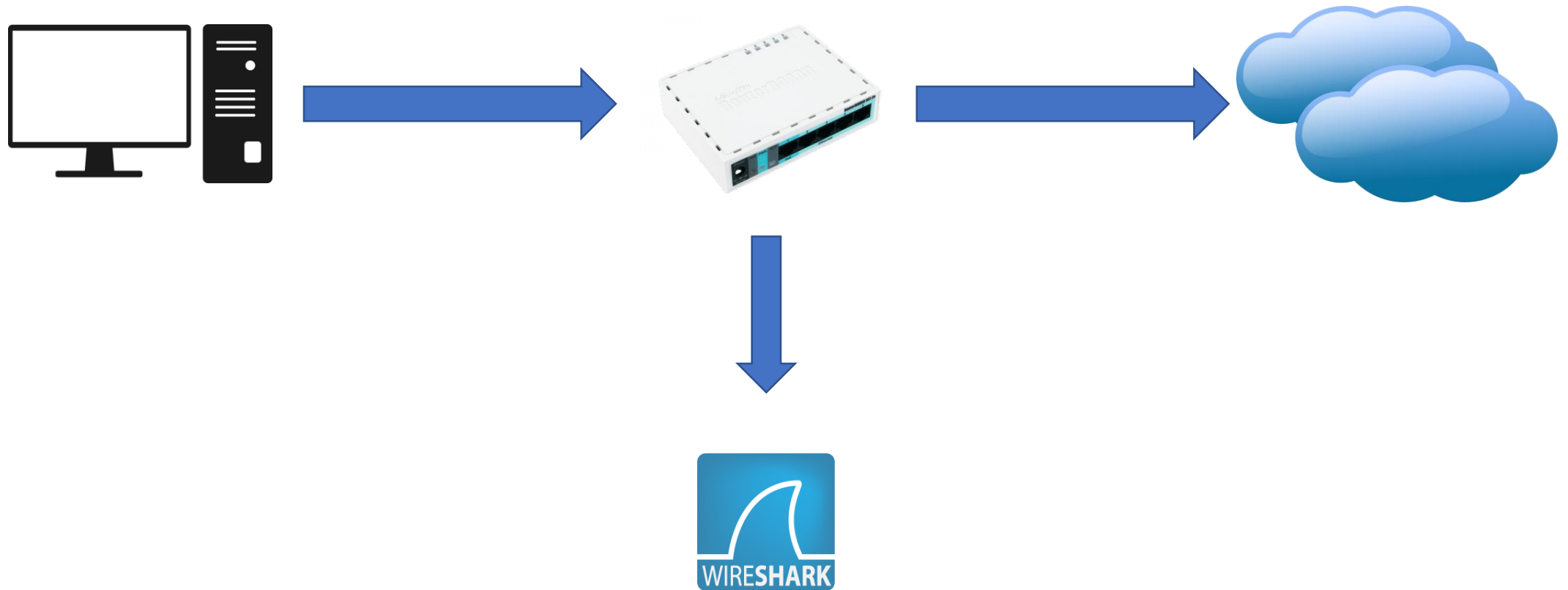
Existen varios métodos de captura de paquetes, y diferentes escenarios de aplicación

Métodos para
capturar
paquetes

- Capturar el tráfico en la interfaz del computador donde se tiene un determinado problema de conexión.
- Utilizar un HUB o concentrador para capturar todos los paquetes que se trafican por esa red.
- Crear una réplica de cada uno de los paquetes del tráfico cursado por cada uno de los puertos de un switch. (Port Mirroring)
- Sobre determinada interfaz de un router.



- Realizando una captura del tráfico que se cursa a través del puerto de entrada o de salida del router.



TCPDUMP

- Herramienta de captura de paquetes nativa de Linux
- No tiene disectores de paquetes.
- Permite crear un archivo .pcap para el posterior análisis de los paquetes capturados.

Packet Sniffer

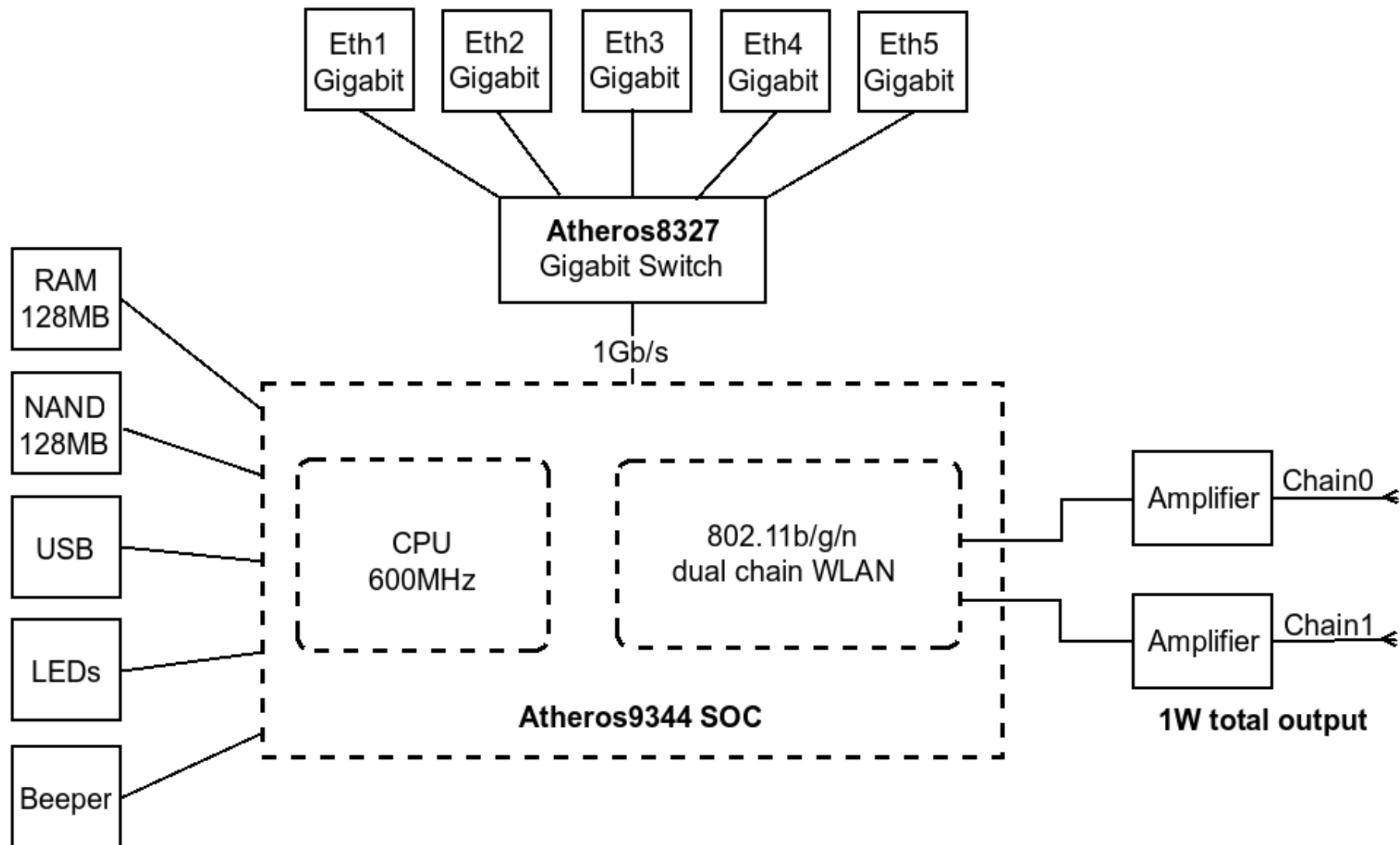
- Herramienta de captura de paquetes de RouterOS
- Disponible en todos los modelos de RouterBoard
- Permite realizar streaming de la captura a una PC con Wireshark.
- Permite crear un archivo .pcap para su posterior análisis.

Herramientas
para capturar
paquetes

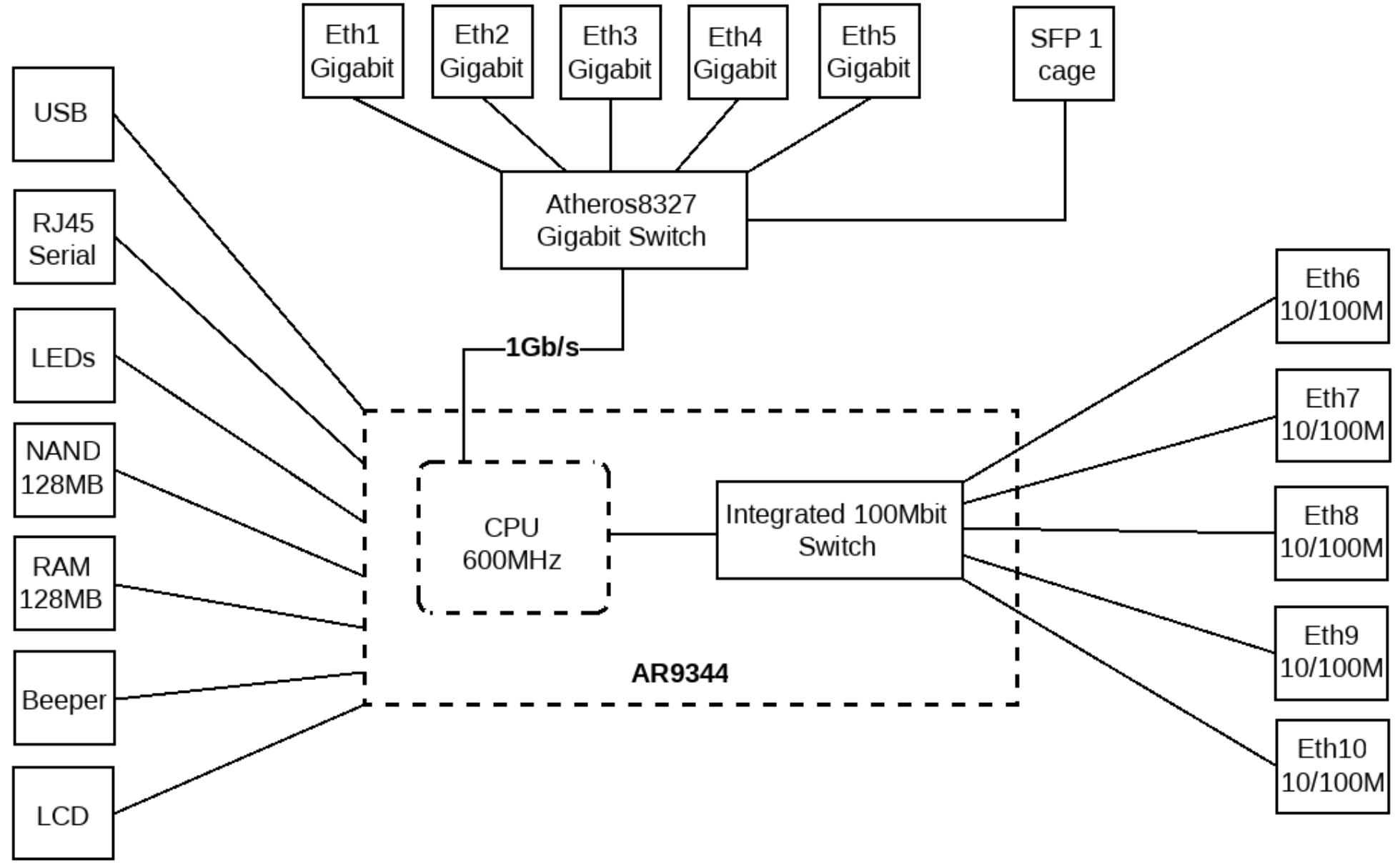
- Packet sniffer es una herramienta que puede capturar y analizar paquetes que ingresan, abandonan o atraviesan el router, excepto el tráfico que solamente atraviesa el chip encargado de la conmutación. [1]

Packet Sniffer

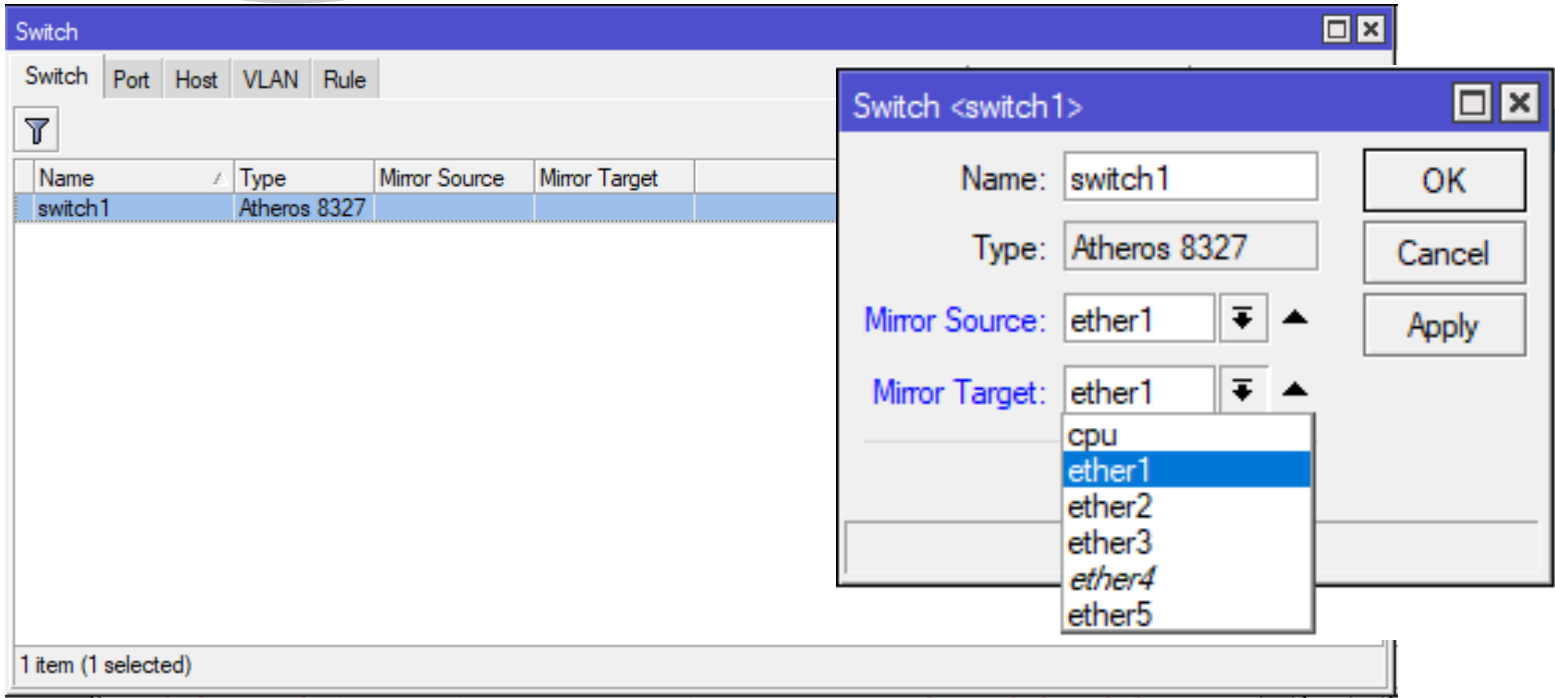
RB951G-2HnD



RB2011UiAS



Port Mirror SwitchOS



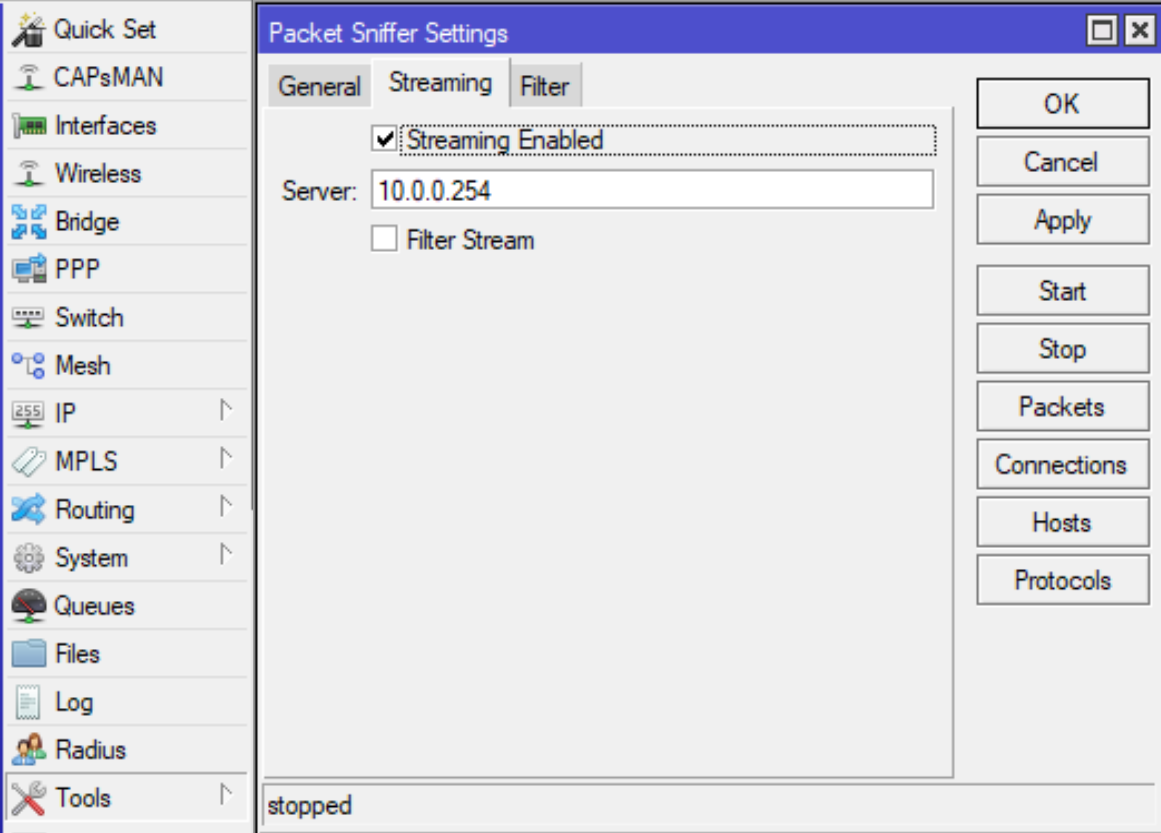
```
[root@RB] > /tool sniffer
```

```
[admin@RB]tool sniffer> set streaming-  
server=10.0.0.2 \
```

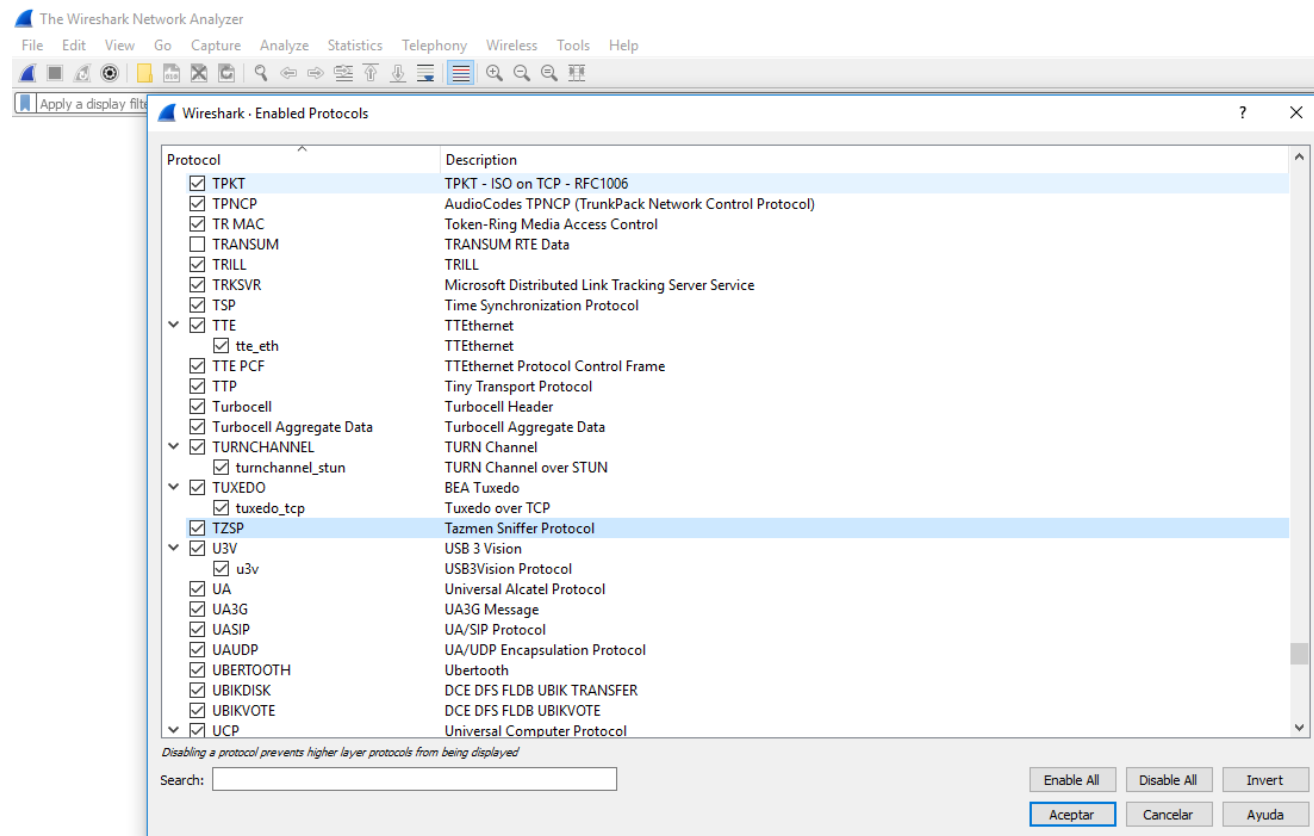
```
\... streaming-enabled=yes
```

La opción streaming permite hacer una copia de los paquetes que atraviesan el router y los envía a una dirección IP específica donde estará instalado Wireshark

Packet Sniffer/ streaming



Netwatch
Packet Sniffer
Ping
Ping Speed
Profile
RoMON
SMS
Telnet
Torch
Traceroute
Traffic Generator
Traffic Monitor



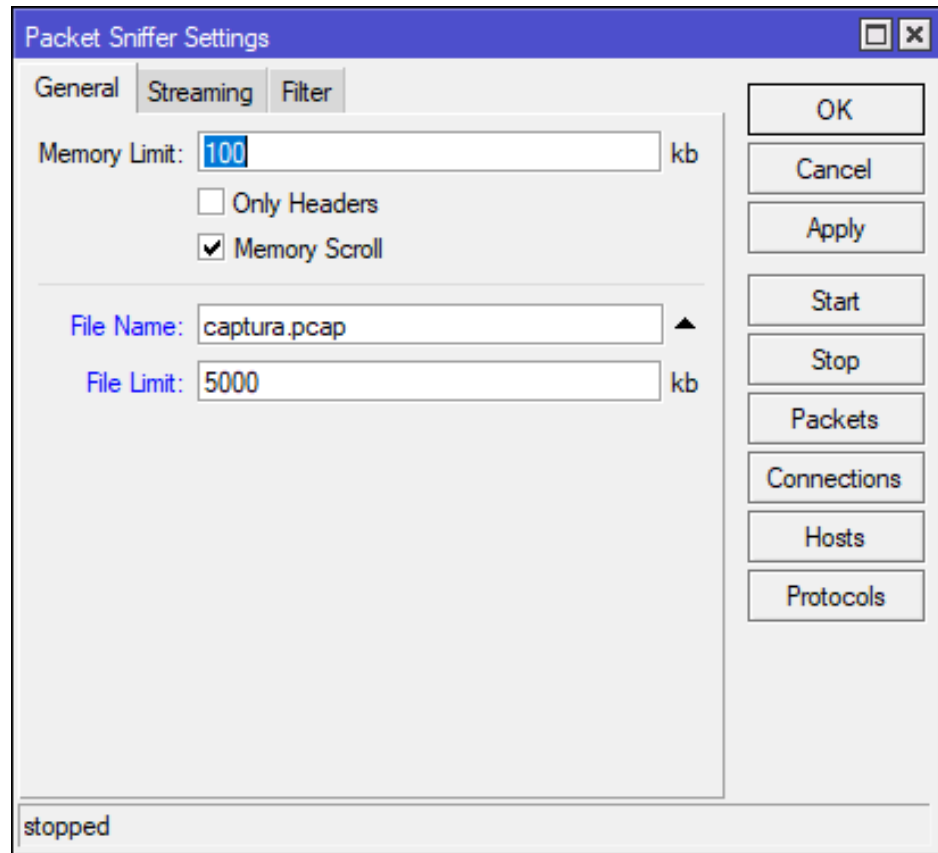
Streamming de paquetes
por una interfaz hacia
wireshark

interface: all
only-headers: no
memory-limit: 100KiB
memory-scroll: yes
file-name:
file-limit: 1000KiB
streaming-enabled: yes
streaming-server: 10.0.02
filter-stream: yes
filter-mac-address:
filter-mac-protocol:
filter-ip-address:
filter-ip-protocol:
filter-port:
filter-direction: any
running: no

Packet Sniffer/ streaming

```
[admin@RB]tool sniffer set file  
name=capture.pcap file-limit=1000
```

Existe la opción de almacenar la captura en un archivo dentro de la routerboard



Packet Sniffer/
file

Wireless Tables

Interfaces Nstreme Dual Access List Registration Connect List Security Profiles Channels

+ - ✓ ✗ [Filter] CAP WPS Client Setup Repeater Scanner Freq. Usage Alignment Wireless Sniffer Wireless Snooper Find

	Name	Type	Actual MTU	Tx	Rx	Tx P...	R...	FP Tx /	FP Rx	FP ...	F...	MA...	ARP	Mode	Band	Chann...	Frequen...	SSID
R	wlan1	Wireless (Atheros AR9...	1500	0 bps	0 bps	0	0	0 bps	0 bps	0	0	4C:...	enabled	station	2GHz-...	20/40...	auto	WiFi-Ar

1 item out of 5

Wireless Sniffer

Interface: wlan1 [Start]

Processed Packets: 0 [Stop]

Memory Size: 0 B [Close]

Memory Saved Packets: 0 [Settings]

Memory Over Limit Packets: 0 [Save...]

File Size: 0 B [Sniffed Packets]

File Saved Packets: 0

File Overlimit Packets: 0

Stream Dropped Packets: 0

Stream Sent Packets: 0

File Limit: 0 KiB

Memory Limit: 0 KiB

Save Sniffed Packets

File Name: eless.pcap [Save]

[Cancel]

Capturando tramas por la interfaz inalámbrica



Wireshark

Wireshark es un analizador de protocolos open-source diseñado por Gerald Combs y que actualmente está disponible para plataformas Windows y Unix. [\[2\]](#)

```
> Frame 30: 104 bytes on wire (832 bits), 104 bytes captured (832 bits)
> Ethernet II, Src: Routerbo_64:69:51 (6c:3b:6b:64:69:51), Dst: LLDP_Multicast (01:80:c2:00:00:0e)
< Link Layer Discovery Protocol
  < Chassis Subtype = MAC address, Id: 6c:3b:6b:64:69:51
    0000 001. .... .... = TLV Type: Chassis Id (1)
    .... ...0 0000 0111 = TLV Length: 7
    Chassis Id Subtype: MAC address (4)
    Chassis Id: Routerbo_64:69:51 (6c:3b:6b:64:69:51)
  < Port Subtype = Interface name, Id: ether5
    0000 010. .... .... = TLV Type: Port Id (2)
    .... ...0 0000 0111 = TLV Length: 7
    Port Id Subtype: Interface name (5)
    Port Id: ether5
  > Time To Live = 120 sec
  < System Name = Dispensario
    0000 101. .... .... = TLV Type: System Name (5)
    .... ...0 0000 1011 = TLV Length: 11
    System Name: Dispensario
  < System Description = MikroTik RouterOS 6.40.3 (stable) RB951G-2HnD
    0000 110. .... .... = TLV Type: System Description (6)
    .... ...0 0010 1101 = TLV Length: 45
    System Description: MikroTik RouterOS 6.40.3 (stable) RB951G-2HnD
  > Capabilities
  > End of LLDPDU
```

LLDP

Wireshark · Endpoints · capture

Ethernet · 6 IPv4 · 6 TCP · 8 UDP · 2

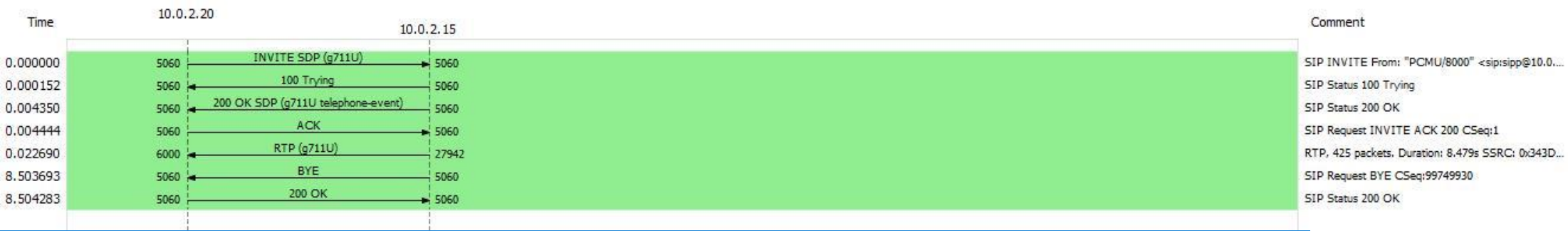
Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	AS Number	City	Latitude	Longitude
181.14.1.1	56612	370	285 k	134	12 k	236	272 k	Argentina	AS7303 Telecom Argentina S.A.	Buenos Aires, 07	-34.603298	-58.381599
186.47.1.1	8291	370	285 k	236	272 k	134	12 k	Ecuador	AS28006 CORPORACION NACIONAL DE TELECOMUNICACIONES - CNT EP	Quito, 18	-0.216700	-78.500000
186.47.1.2	23	2	114	1	54	1	60	Ecuador	AS28006 CORPORACION NACIONAL DE TELECOMUNICACIONES - CNT EP	Quito, 18	-0.216700	-78.500000
186.47.1.3	63122	3	210	2	132	1	78	Ecuador	AS28006 CORPORACION NACIONAL DE TELECOMUNICACIONES - CNT EP	Quito, 18	-0.216700	-78.500000
191.242.1.1	60740	4	228	2	114	2	114	Brazil	AS263151 CONECT TELECOM	Gandu, 05	-13.747500	-39.488201
192.168.20.100	23	2	114	1	60	1	54	—	—	—	—	—
192.168.20.101	63122	3	216	2	138	1	78	—	—	—	—	—
213.39.1.1	5938	6	426	2	156	4	270	United Kingdom	AS8928 Interoute Communications Limited	—	51.496399	-0.122400

Name resolution Limit to display filter Endpoint Types ▾

Copy ▾ Map Cerrar Ayuda

Se puede determinar el origen de una conexión utilizando las bases de datos de GEOIP

<http://dev.maxmind.com/geoip/legacy/geolite/#Downloads>



<https://wiki.wireshark.org/HowToDecodeG729>

Filtros y patrones de búsqueda



Lista de tramas y paquetes



Disección del contenido de paquetes



Presentación en hexadecimal del paquete



cap_240816_1AP.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
44	0.522171	Cisco_43:52:f0	Broadcast	802.11	264	Beacon frame, SN=512, FN=0, Flags=.....C, BI=102, SSID=FIUBA
45	0.544286	Cisco_43:52:f0 (dc:...	Apple_b0:7f:51 (24:...	802.11	38	Request-to-send, Flags=.....C
46	0.546278	Cisco_43:52:f0 (dc:...	Apple_b0:7f:51 (24:...	802.11	38	Request-to-send, Flags=.....C
47	0.578508	173.252.90.197	10.1.127.51	TCP	108	[TCP Retransmission] 443 → 51772 [FIN, ACK] Seq=1 Ack=1 Win=65 Len=0 TSval=280143936 TSeq=51772
48	0.583561	SamsungE_17:8b:48	Broadcast	802.11	226	Beacon frame, SN=3233, FN=0, Flags=.....C, BI=100, SSID=AndroidAP
49	0.586473	Tp-LinkT_47:b8:bf	Broadcast	802.11	133	Beacon frame, SN=976, FN=0, Flags=.....C, BI=100, SSID=LAB_TPL1
50	0.626975	Cisco_43:52:f0	Broadcast	802.11	264	Beacon frame, SN=513, FN=0, Flags=.....C, BI=102, SSID=FIUBA
51	0.627737	Cisco_43:52:f0 (dc:...	Apple_b0:7f:51 (24:...	802.11	38	Request-to-send, Flags=.....C
52	0.629444	Cisco_43:52:f0 (dc:...	Apple_b0:7f:51 (24:...	802.11	38	Request-to-send, Flags=.....C
53	0.639969	1a:5b:0e:22:37:e6	Broadcast	802.11	296	Beacon frame, SN=2519, FN=0, Flags=.....C, BI=100, SSID=HMG-Guest
54	0.678499	173.252.90.197	10.1.127.51	TCP	108	[TCP Retransmission] 443 → 51772 [FIN, ACK] Seq=1 Ack=1 Win=65 Len=0 TSval=280143936 TSeq=51772
55	0.688820	Tp-LinkT_47:b8:bf	Broadcast	802.11	133	Beacon frame, SN=977, FN=0, Flags=.....C, BI=100, SSID=LAB_TPL1
56	0.691166	Fortinet_22:37:e6	Broadcast	802.11	294	Beacon frame, SN=2823, FN=0, Flags=.....C, BI=100, SSID=HAVAS-CORP

> Frame 56: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits)

> Radiotap Header v0, Length 18

> 802.11 radio information

> IEEE 802.11 Beacon frame, Flags:C

▼ IEEE 802.11 wireless LAN

- ▼ Fixed parameters (12 bytes)
 - Timestamp: 0x0000001f40433187
 - Beacon Interval: 0.102400 [Seconds]
 - > Capabilities Information: 0x0431
 - > Tagged parameters (236 bytes)

```
0030 00 00 64 00 31 04 00 0a 48 41 56 41 53 2d 43 4f  .d.1... HAVAS-CO
0040 52 50 01 08 82 84 8b 96 0c 12 18 24 03 01 03 05  RP..... ..$....
0050 04 00 01 00 00 07 06 42 52 20 01 0d 1e 2a 01 00  .....B R ...*.
0060 30 14 01 00 00 0f ac 04 01 00 00 0f ac 04 01 00  0.....
0070 00 0f ac 01 01 00 32 04 30 48 60 6c 2d 1a 8d 01  .....2. 0H`l-...
0080 1b ff ff 00 00 00 00 00 00 00 00 00 00 01 00 00  .....
0090 00 00 04 06 e6 a7 0c 00 3d 16 03 08 04 00 00 00  ..... =.....
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00b0 7f 08 00 00 00 00 00 00 00 40 dd 16 00 50 f2 01  ..... .@...P..
00c0 01 00 00 50 f2 04 01 00 00 50 f2 04 01 00 00 50  ...P.... .P....P
00d0 f2 01 dd 18 00 50 f2 02 01 01 80 00 03 a4 00 00  ....P.. .....
```

Beacon Interval (wlan.fixed.beacon), 2 bytes

Packets: 9678 · Displayed: 9678 (100.0%) · Load

- La herramienta packet sniffer puede ayudar en el troubleshooting de una red.
- Se sugiere la utilización en RouterBoards con buena capacidad de procesamiento.
- El administrador de red es quien toma la decisión de como y que paquetes captura.
- Wireshark puede usarse como herramienta para estudiar diferentes protocolos que cursan en la red.

Conclusiones

[1]https://wiki.mikrotik.com/wiki/Manual:Tools/Packet_Sniffer

[2]https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_analisis_trafico_wireshark.pdf

Bibliografía