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

Introducción

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.

Objetivos

Mostrar el funcionamiento de la herramienta Packet Sniffer.

Proponer escenarios para el uso de Packet Sniffer.

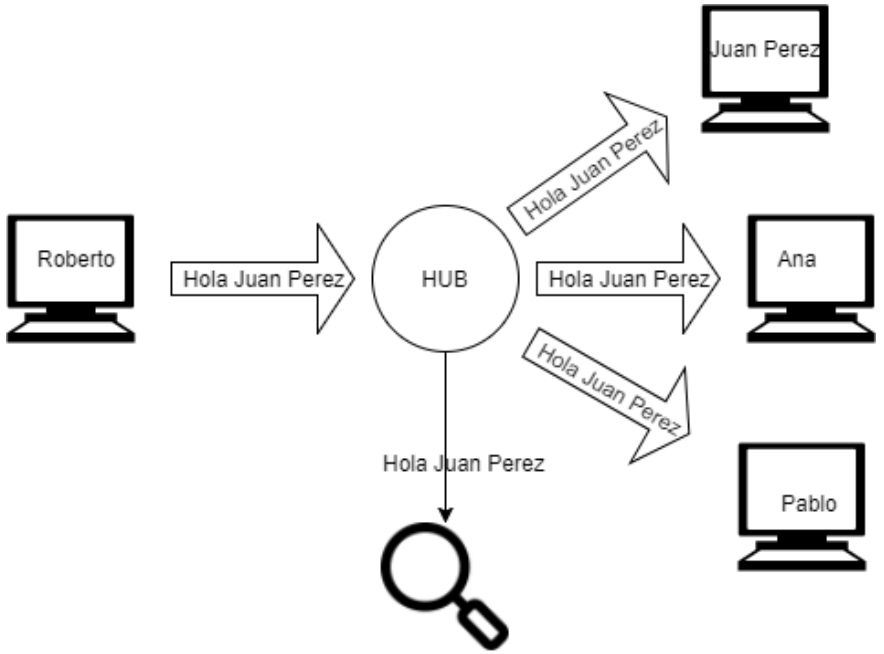
Mostrar los inconvenientes relacionados con la captura de paquetes

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

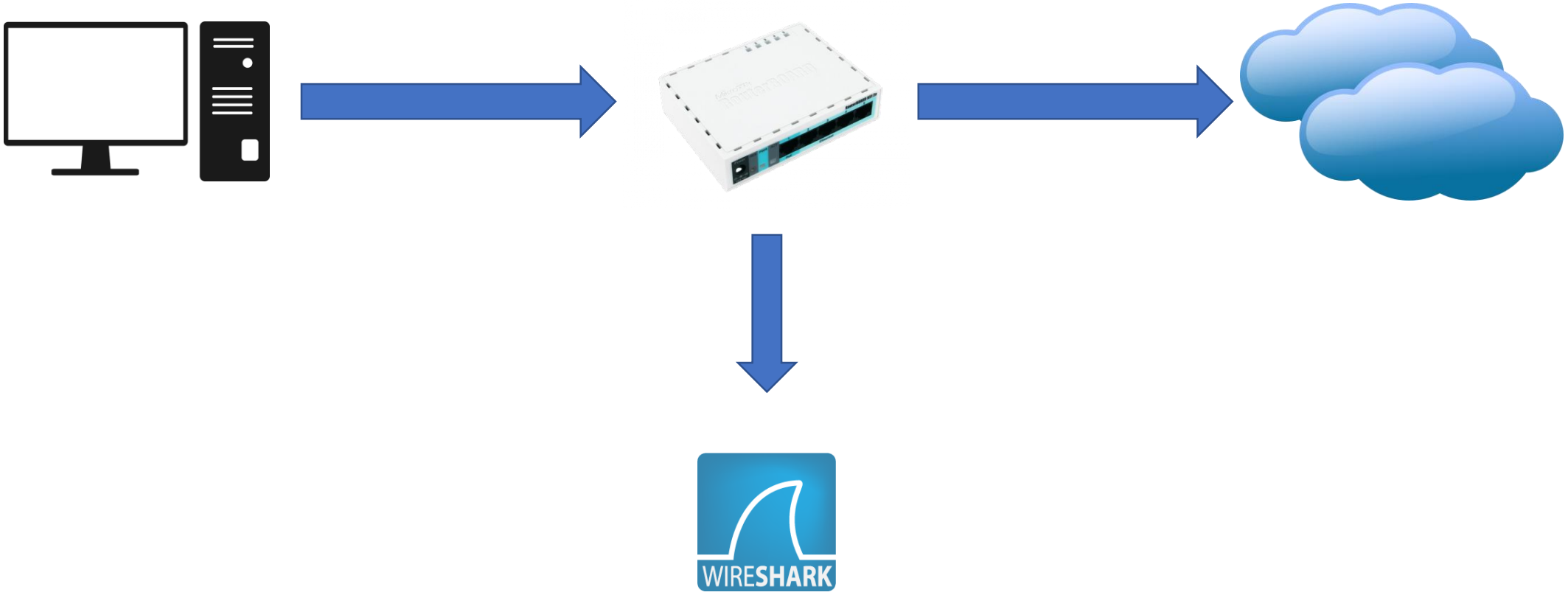
Métodos para capturar paquetes

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

- 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.



Herramientas para capturar paquetes

TCPDUMP

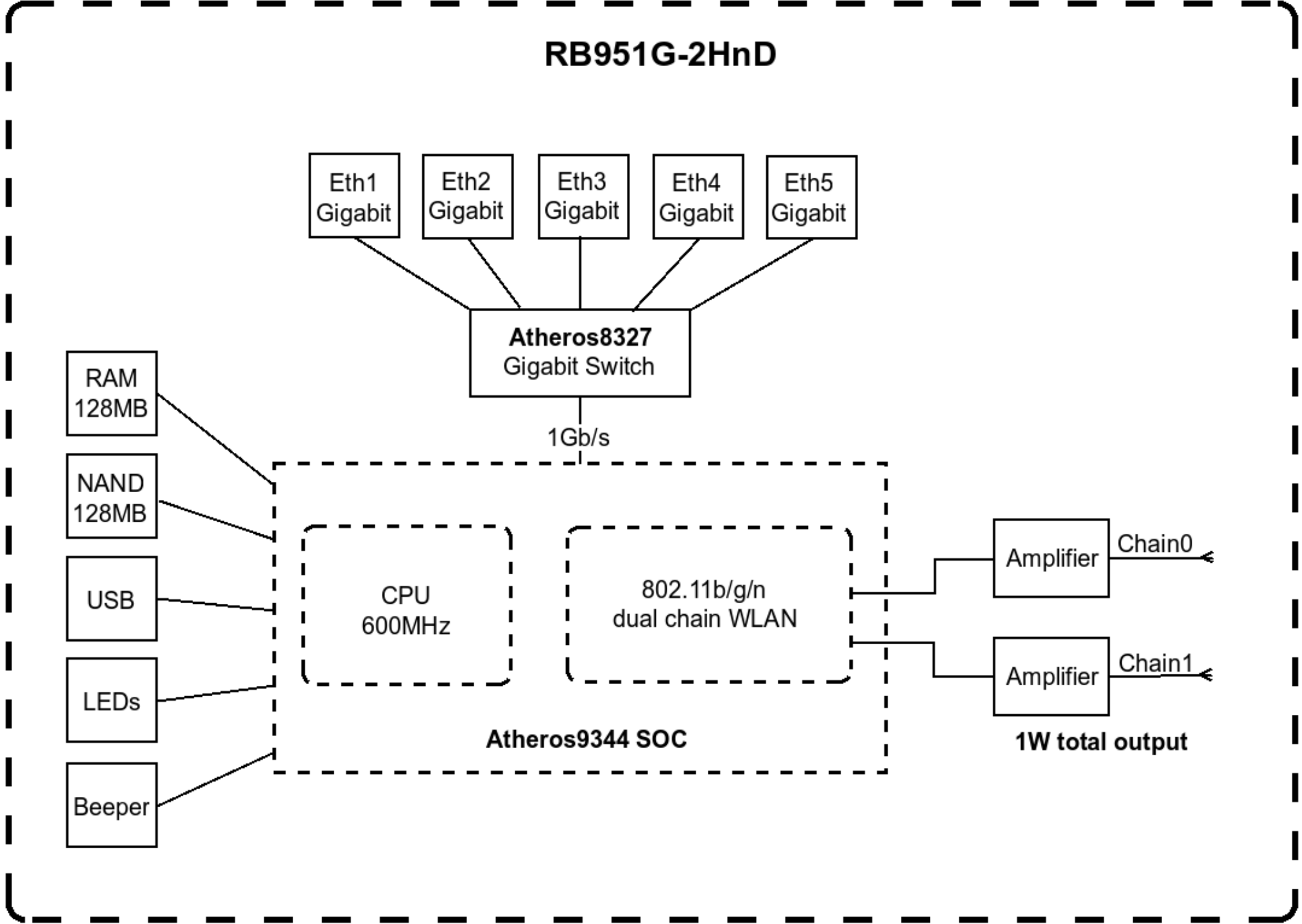
- Herramienta de captura de paquetes nativa de Linux
- No tiene disectores de paquetes.
- Permite crear un archivo .pcap para el posterior análisis de los paquetes capturados.

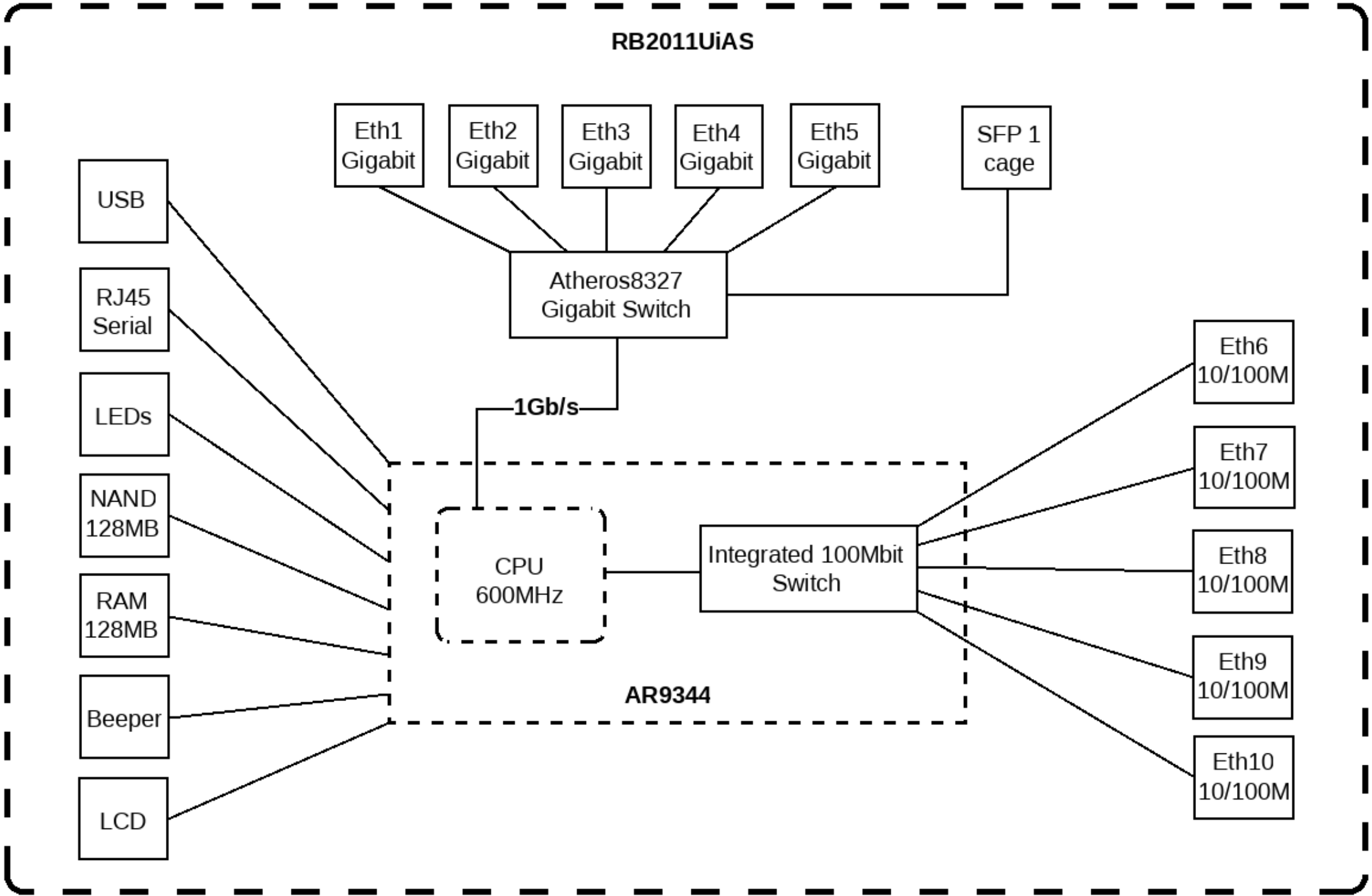
Packet Sniffer

- 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.

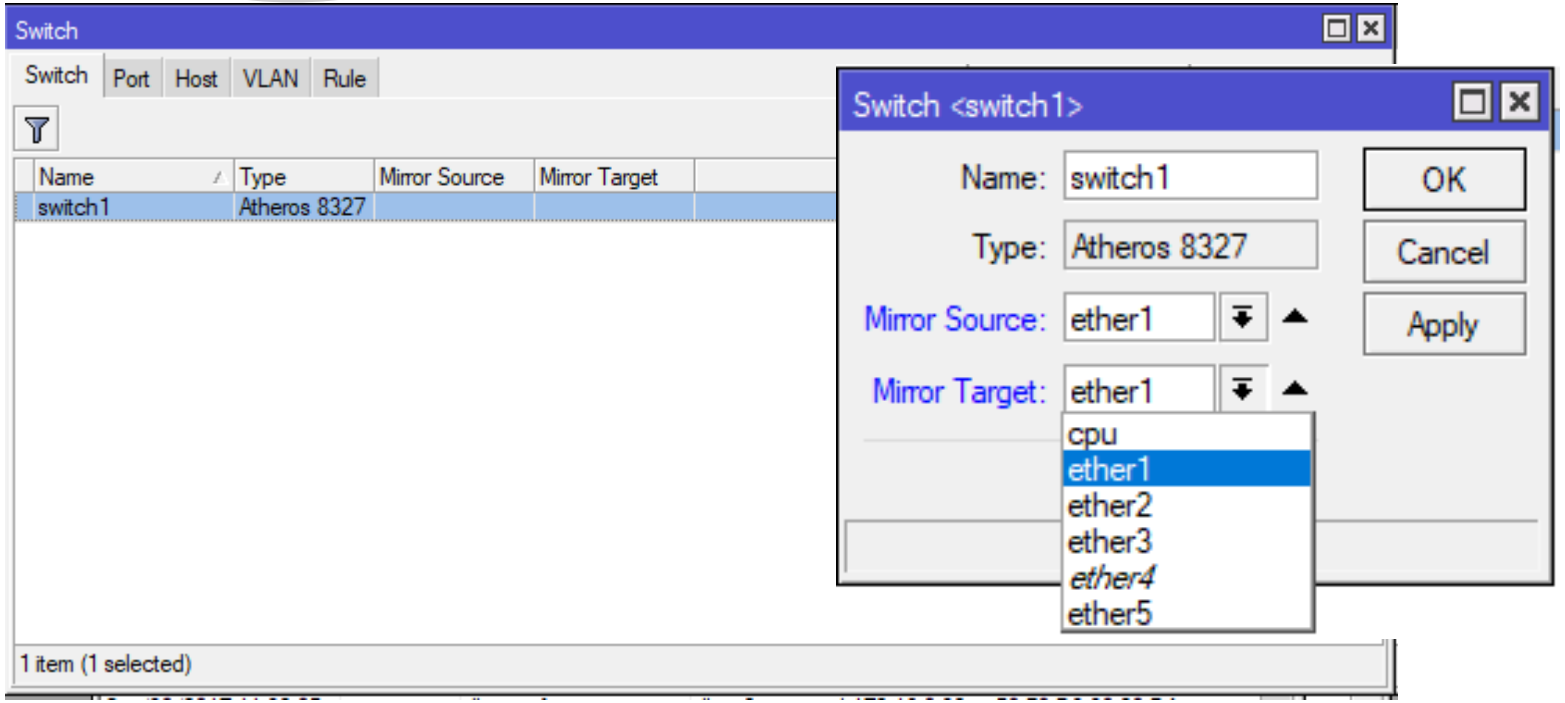
Packet Sniffer

- 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]


RB951G-2HnD
Eth1 Gigabit
Eth2 Gigabit
Eth3 Gigabit
Eth4 Gigabit
Eth5 Gigabit
Atheros8327
Gigabit Switch
1Gb/s
RAM 128MB
NAND 128MB
USB
LEDs
Beeper
CPU 600MHz
802.11b/g/n dual chain WLAN
Atheros9344 SOC
Amplifier
Chain0
Amplifier
Chain1
1W total output


RB2011UiAS
Eth1 Gigabit
Eth2 Gigabit
Eth3 Gigabit
Eth4 Gigabit
Eth5 Gigabit
SFP 1 cage
USB
RJ45 Serial
LEDs
NAND 128MB
RAM 128MB
Beeper
LCD
Atheros8327 Gigabit Switch
1Gb/s
CPU 600MHz
Integrated 100Mbit Switch
AR9344
Eth6 10/100M
Eth7 10/100M
Eth8 10/100M
Eth9 10/100M
Eth10 10/100M

Port Mirror SwitchOS



Port Mirror RouterOS

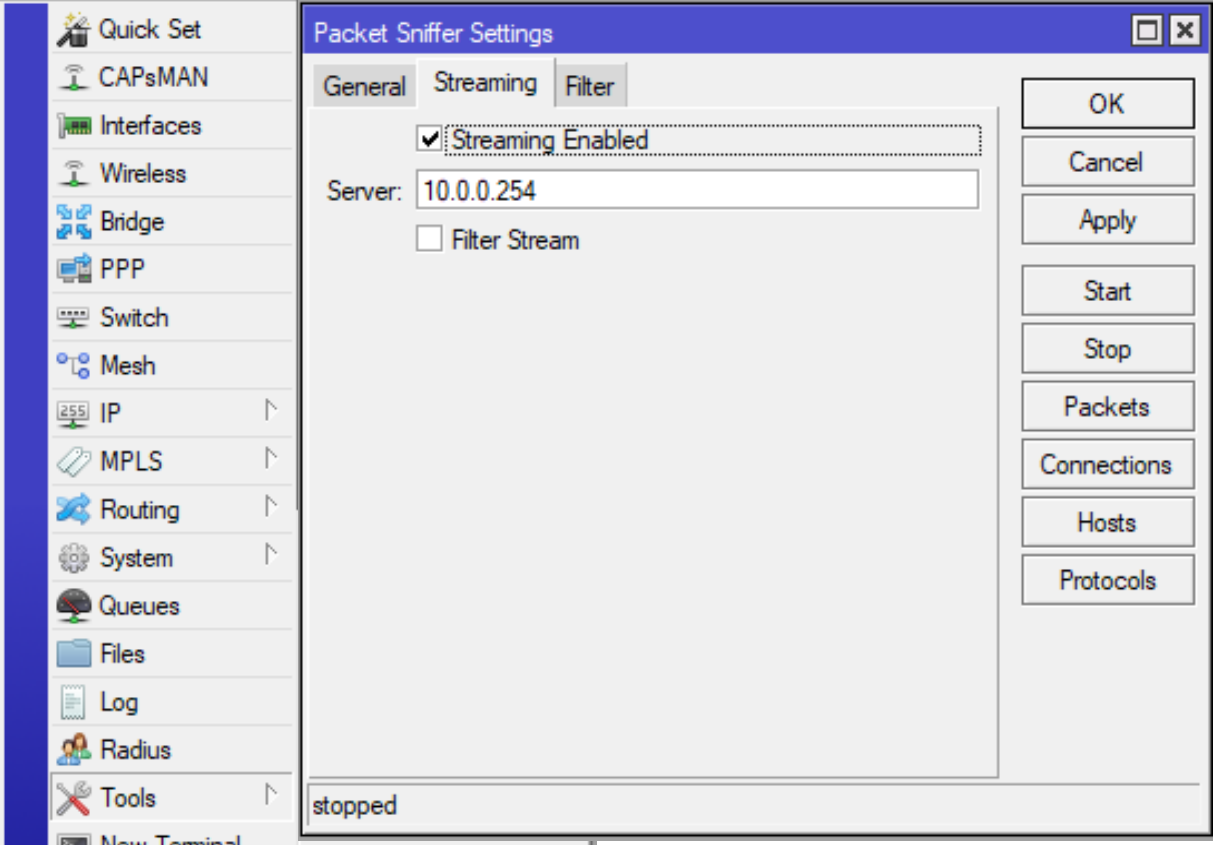
[root@RB] > /tool sniffer

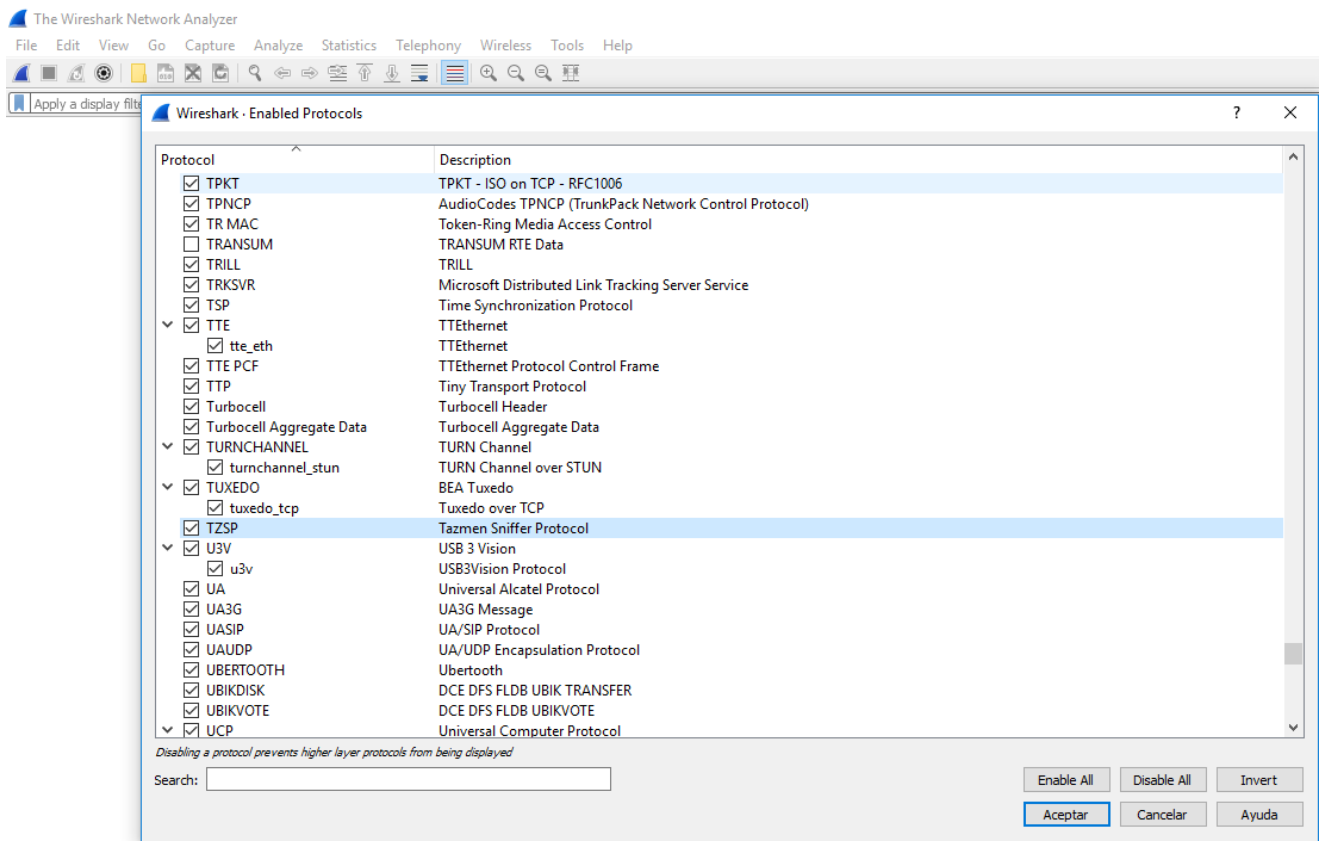
[admin@RB]tool sniffer> set streaming-server=10.0.0.2 \

\... 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





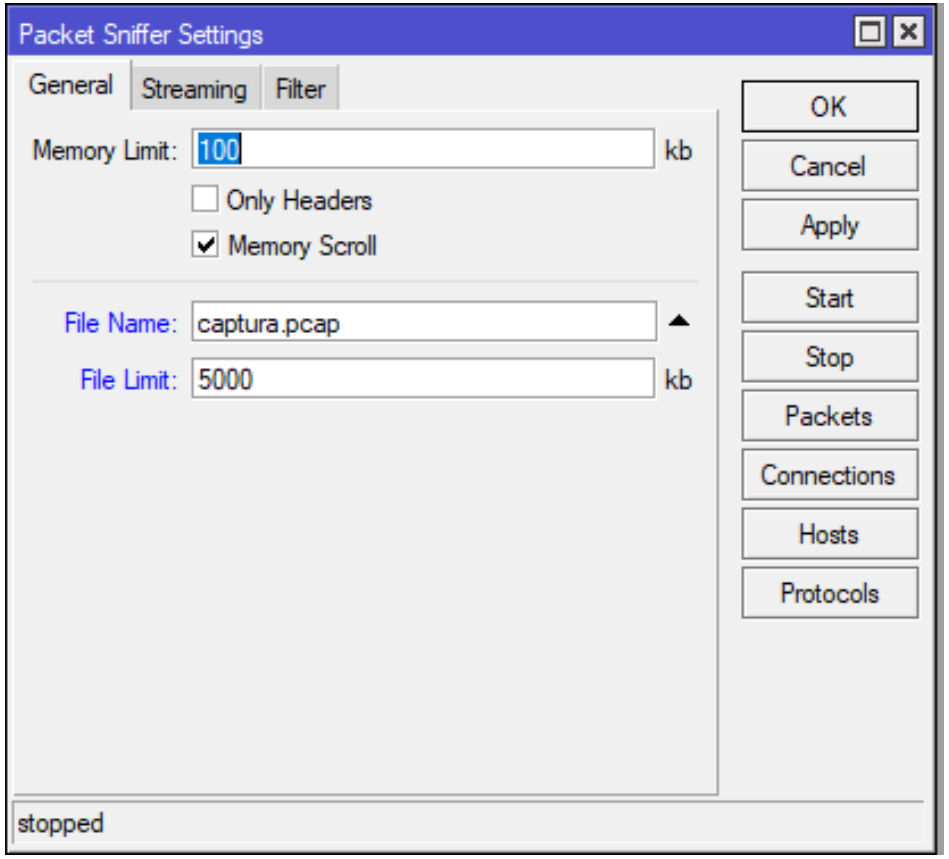
Streamming de paquetes por una interfaz hacia wireshark

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

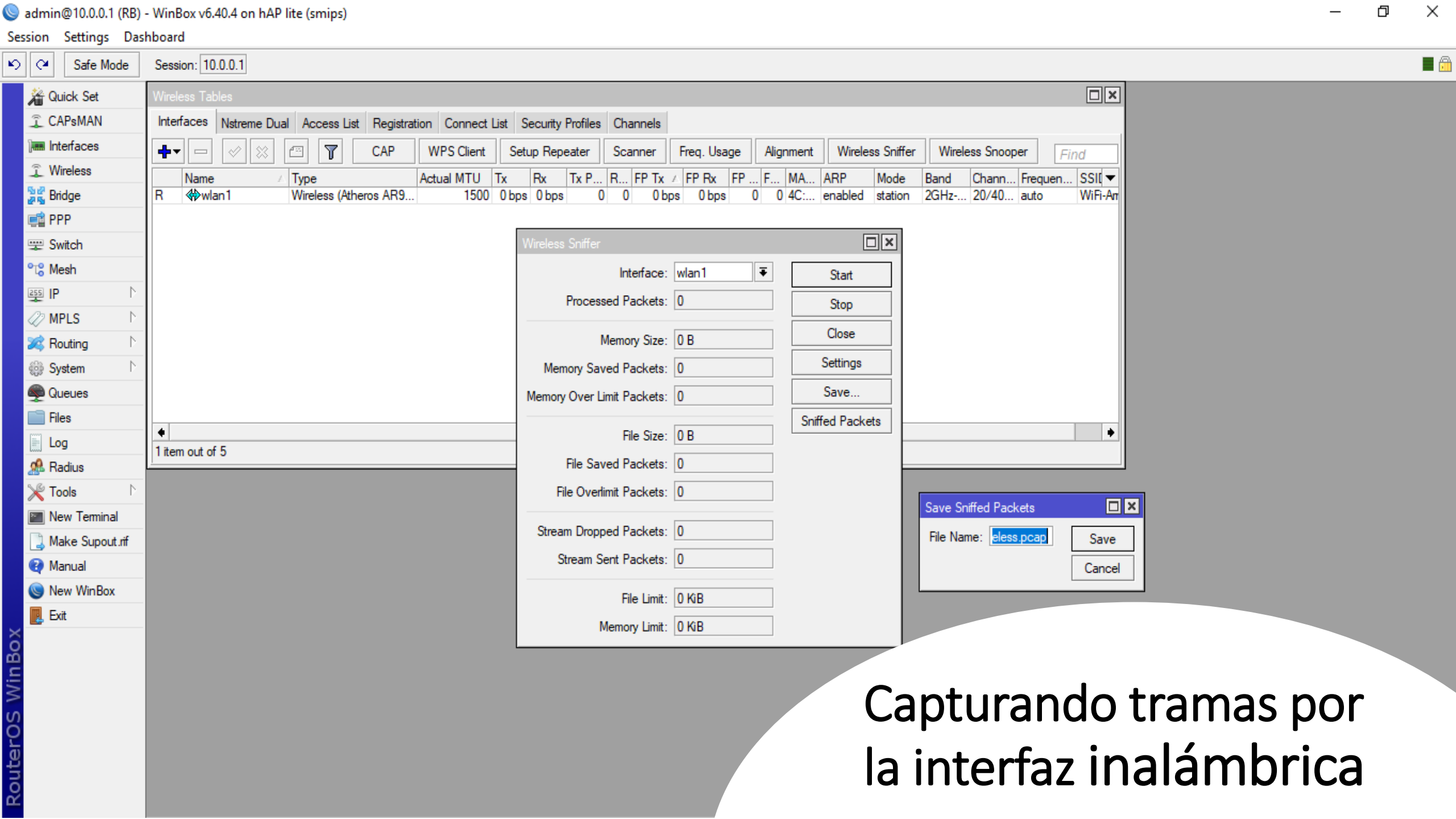
Packet Sniffer/ streaming

[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



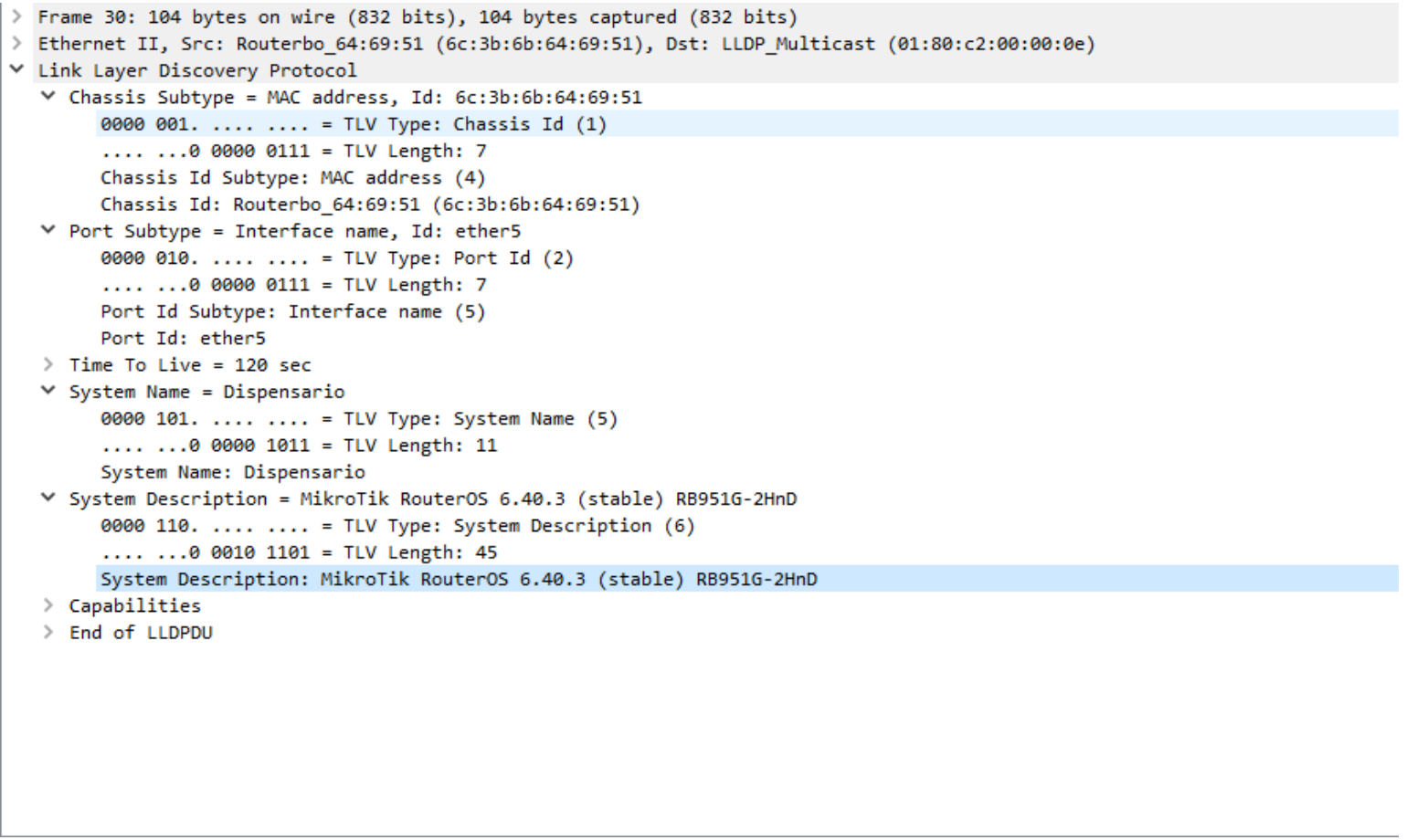
Packet Sniffer/ file



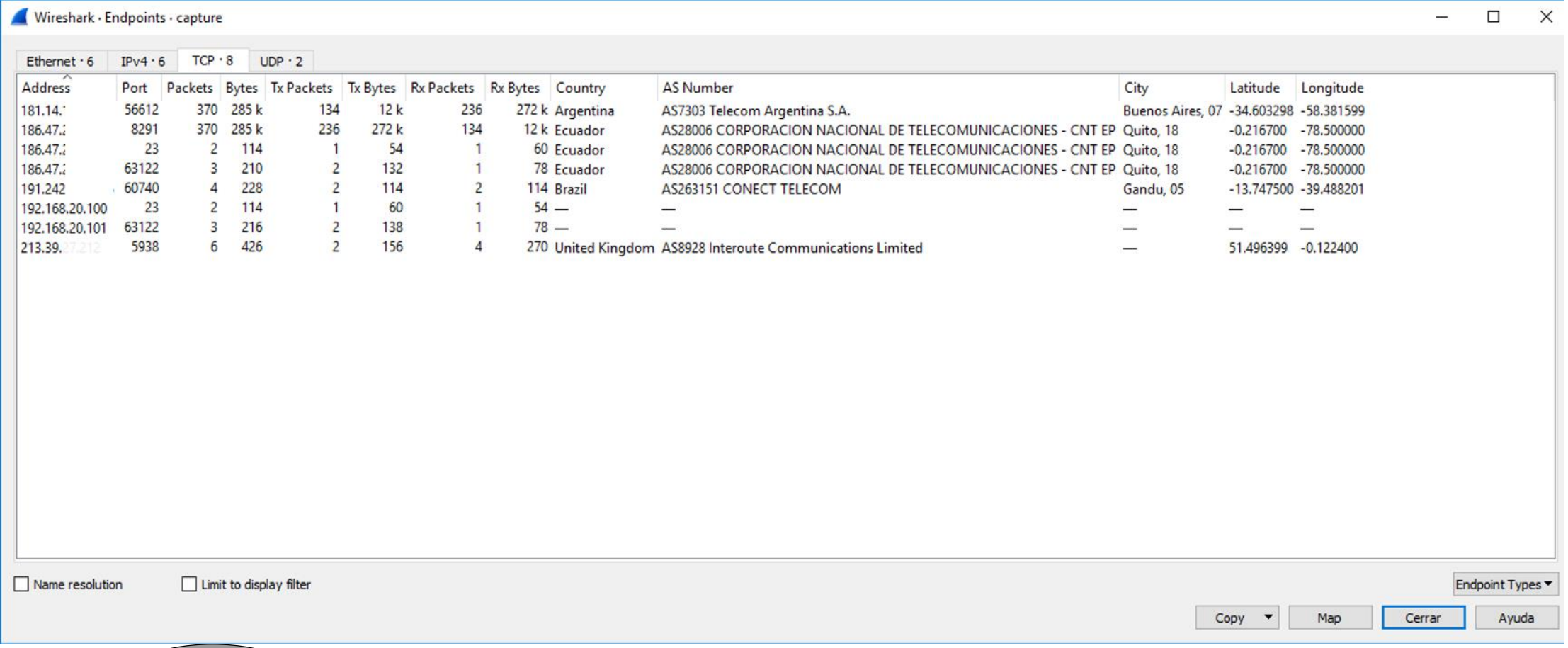
Capturando tramas por la interfaz inalámbrica

Wireshark

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

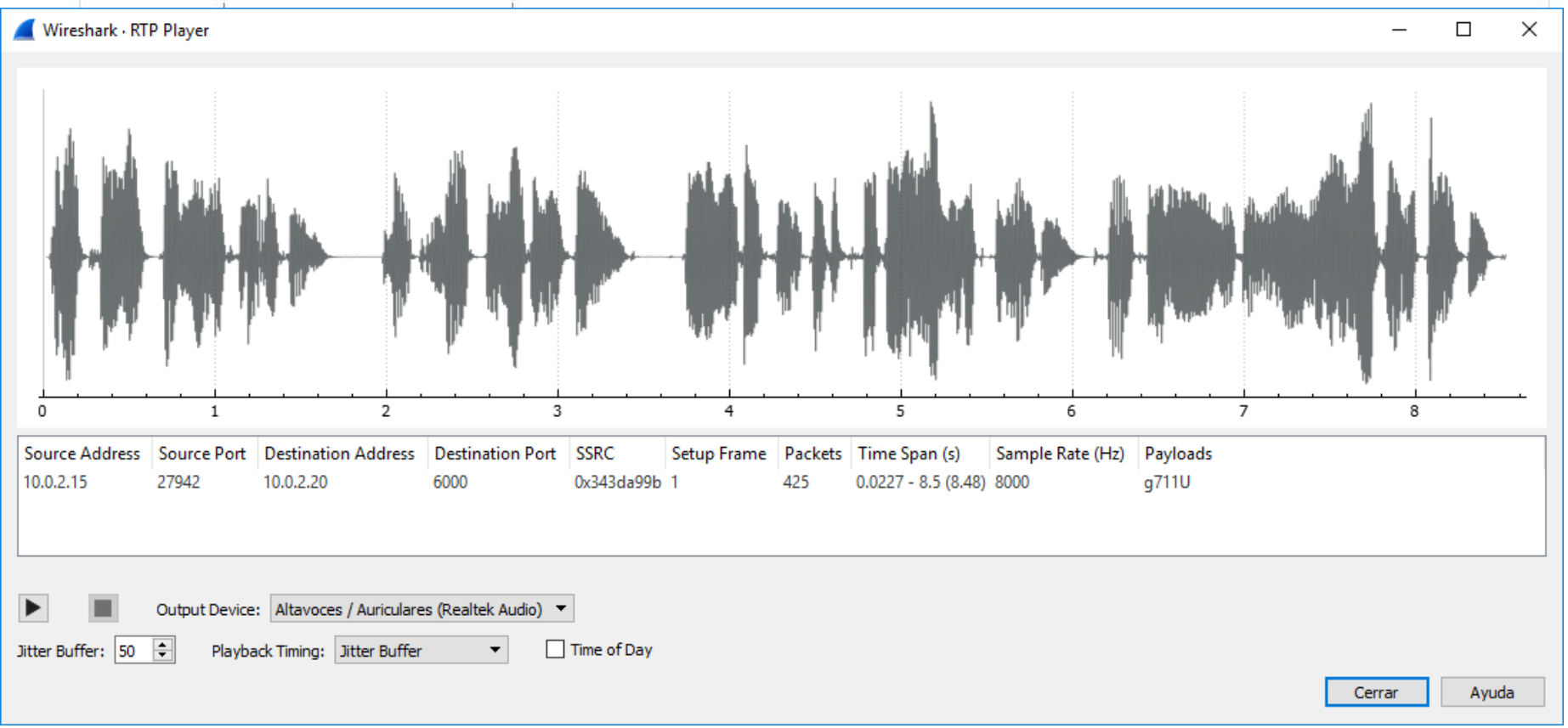

Frame 30: 104 bytes on wire (832 bits), 104 bytes captured (832 bits)
Ethernet II, Src: Routerbo_64:69:51 (6c:3b:6b:64:69:51), Dst: LLDP_Multicast (01:80:c2:00:00:0e)
Link Layer Discovery Protocol
Chassis Subtype = MAC address, Id: 6c:3b:6b:64:69:51
0000 001. .... = TLV Type: Chassis Id (1)
....0 0000 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



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

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



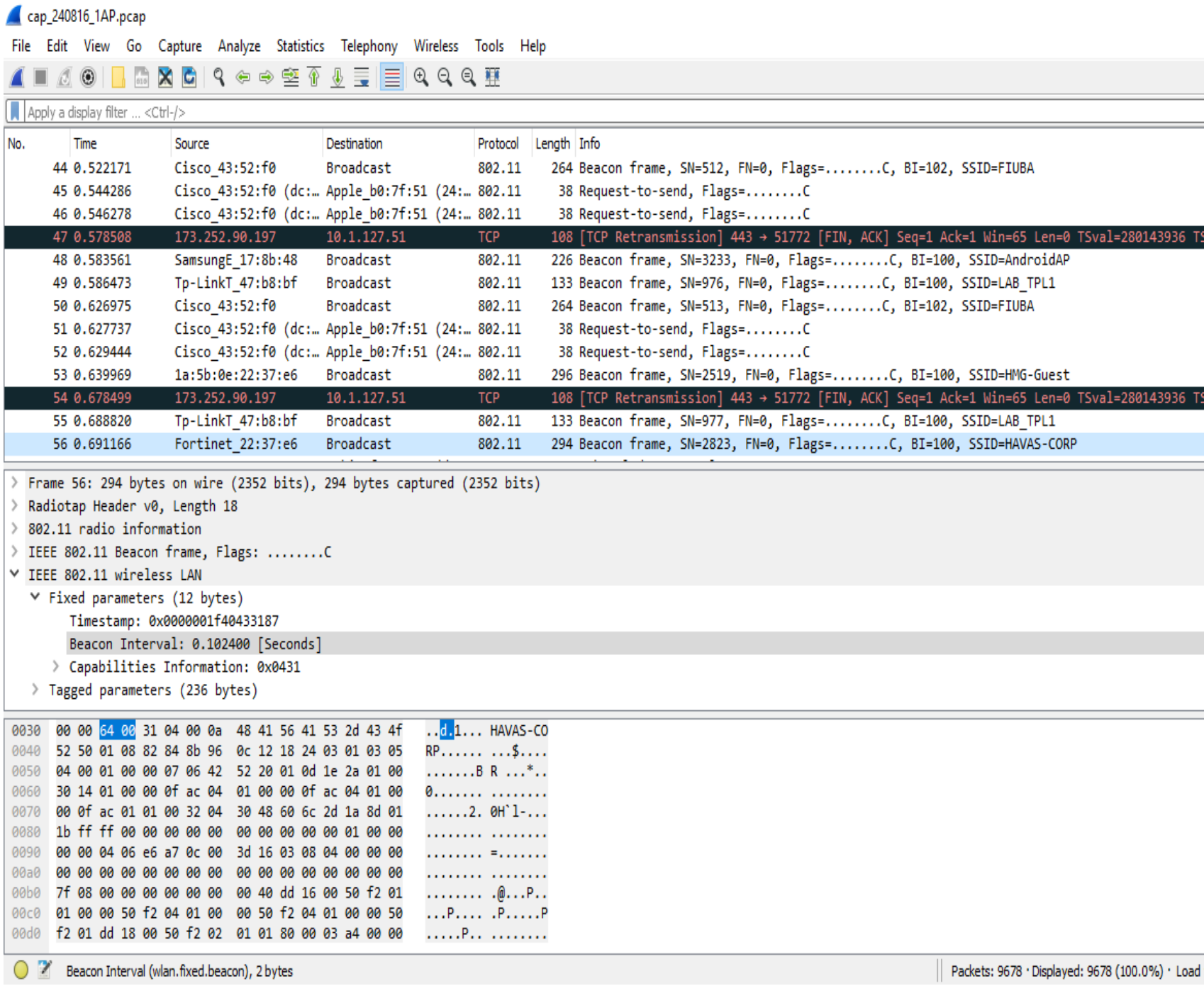
https://wiki.wireshark.org/HowToDecodeG729

Filtros y patrones de búsqueda

Lista de tramas y paquetes

Disección del contenido de paquetes

Presentación en hexadecimal del paquete



Conclusiones

- 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.

Bibliografía

[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