PROCEDIMIENTO ADMINISTRATIVO Y TECNICO PARA SOLICITUDES POR PARTE DE LA POLICIA JUDICIAL.

Decreto presidencial 1704 de 2012 Artículos 1 y 2, compilado por el Decreto 1078 de 2015,
artículo 2.2.2.6.1 y 2.2.2.6.2

"Los proveedores de redes y servicios de telecomunicaciones que desarrollen su actividad comercial en el territorio nacional deberán implementar y garantizar en todo momento la infraestructura tecnológica necesaria que provea los puntos de conexión y de acceso a la captura del tráfico de las comunicaciones que cursen por sus redes, para que los organismos con funciones permanentes de Policía Judicial cumplan, previa autorización del Fiscal General de la Nación o su delegado, con todas aquellas labores inherentes a la interceptación de las comunicaciones requeridas.

ARTICULO 2.2.2.6.1- DEFINICIÓN DE INTERCEPTACIÓN LEGAL DE COMUNICACIONES: La interceptación de
las comunicaciones, cualquiera que sea su origen o tecnología, es un mecanismo de seguridad pública que busca optimizar la labor de investigación de los delitos que adelantan las autoridades y organismos competentes, en el marco de la Constitución y la Ley

ARTICULO 2.2.2.6.2.- DEBER DE LOS PROVEEDORES DE REDES Y SERVICIOS DE TELECOMUNICACIONES. Los
proveedores de redes y servicios de telecomunicaciones que desarrollen su actividad comercial en el territorio nacional deberán implementar y garantizar en todo momento la infraestructura tecnológica necesaria que provea los puntos de conexión y de acceso a la captura del tráfico de las comunicaciones que cursen por sus redes, para que los organismos con funciones permanentes de Policía Judicial cumplan, previa autorización del Fiscal General de la Nación o su delegado, con todas aquellas labores inherentes a la interceptación de las comunicaciones requeridas. Los proveedores de redes y servicios de telecomunicaciones deberán atender oportunamente los requerimientos de interceptación de comunicaciones que efectúe el Fiscal General de la Nación, de conformidad con lo establecido en el presente decreto y en el régimen legal vigente, para facilitar la labor de interceptación de los organismos permanentes de policía judicial.

PARÁGRAFO.- El Ministerio de Tecnologías de la Información y las Comunicaciones podrá, en los casos en que lo estime necesario, definir las especificaciones técnicas de los puntos de conexión y del tipo de tráfico a

interceptar e imponer a los proveedores de redes y servicios de telecomunicaciones, mediante resoluciones de carácter general, modelos y condiciones técnicas y protocolos sistemáticos a seguir, para atender las solicitudes de interceptación que efectué el Fiscal General de la Nación."

En cumplimiento de lo anterior se han desarrollado los siguientes procedimientos:

ADMINISTRATIVO:

- Se recibe el requerimiento por parte de la autoridad competente.
- Reportar a Gerencia dicha solicitud, para ser revisada y autorizada.
- Delegar y dar orden al personal encargado en la organización para que conceda acceso a la plataforma de administración de la red, para la verificación de lo solicitado por parte de las autoridades.

TECNICO:

Una vez recibido la autorización u orden por parte de Gerencia, se procede de la siguiente manera:

1. Se crea una VPN para dar acceso a la red de la empresa, de manera que puedan monitorear lo solicitado.
2. Se entrega datos de conexión de la VPN, tales como IP, usuario y clave.
3. Una vez conectado a la VPN y se haya establecido conexión con el equipo a intervenir vamos a encontrar la siguiente interfaz.

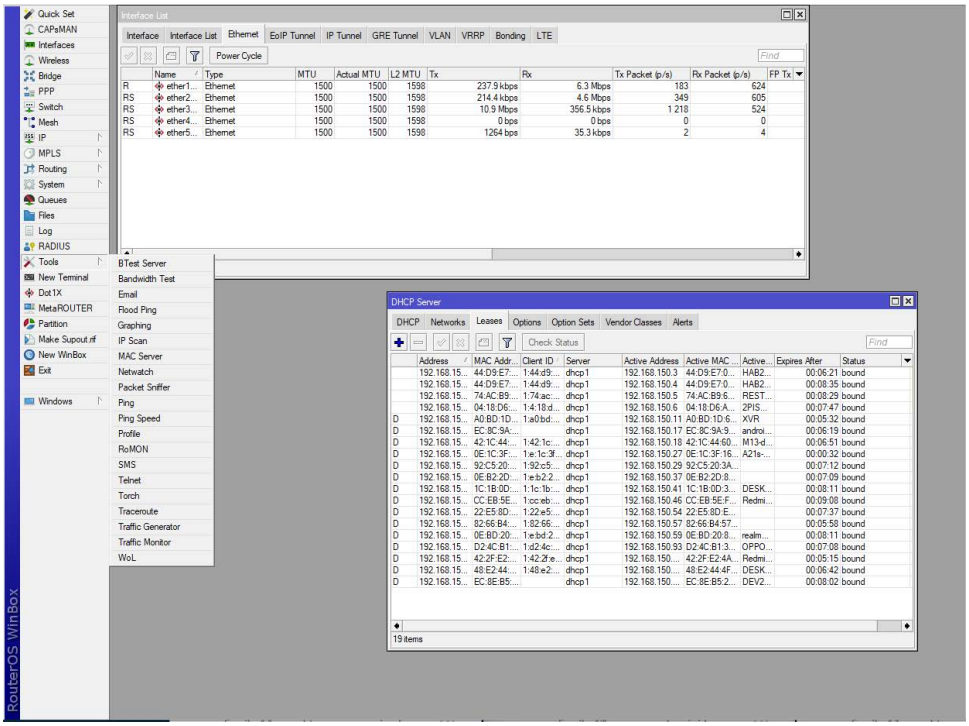

Figura.1

4. En el menú de Tools o herramientas, encontraremos todas las opciones que nos brinda Mikrotik para realizar una escaneo y monitoreó de la actividad del servicio cliente, como el **Sniffer** el cual nos permitirá supervisar, entre otras cosas:

- Tráfico total
- Rastreador de puertos
- Tráfico web (HTTP, HTTPS)
- Tráfico de correo (IMAP, POP3, SMTP)
- Tráfico de transferencia de archivos (FTP , P2P)
- Tráfico de infraestructura (DHCP , DNS, ICMP, SNMP)
- Mando a distancia (RDP, SSH , VNC).
- Otro tráfico UDP y TCP.

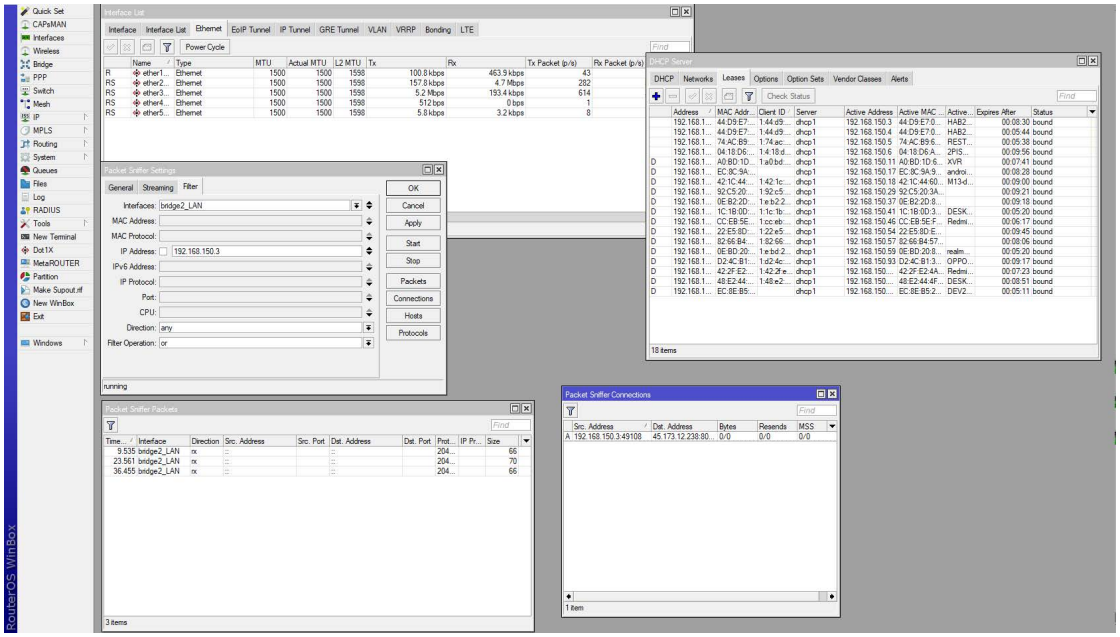

Figura.2

Entre las otras opciones también tenemos la herramienta **Torch**, la cual nos permite analizar el flujo de los datos en tiempo real.

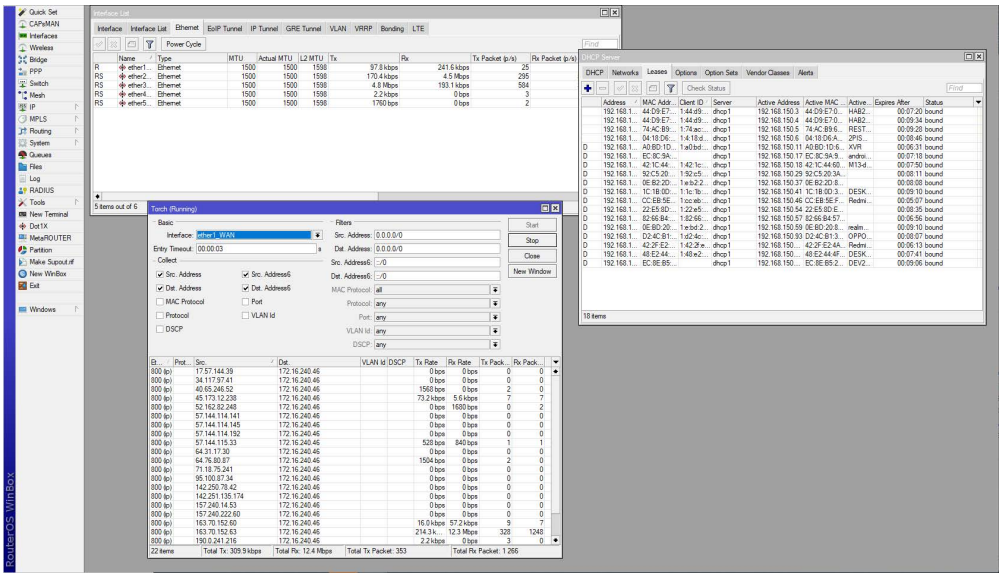

Figura 3