2. herramientas de gestión basadas en SNMP

Las herramientas y software para el monitoreo de equipos basadas en el protocolo SNMP permiten ver el estado de la red monitoreando sus interacciones e incluso pueden algunas monitorear la temperatura de los dispositivos

Las herramientas que encontramos son:

2.1 **Network Performance Monitor** de **SolarWinds (NPM)**

Es una plataforma orientada a la web con la cual se cubren las necesidades de monitoreo de fallas, ancho de banda, rendimiento y adaptable a las necesidades puntuales de cada organización.

NPM utiliza un sistema de network sonar discovery (detección de sonar de red) el cual permite identificar toda la red conectada por protocolo SNMP para identificar que equipos se monitorearan

Una vez dentro del sistema los equipos se pueden dividir con diferentes etiquetas y monitorear el uso de recursos de estos mismo, y ubicar los equipos monitorizados mediante el uso de un atlas

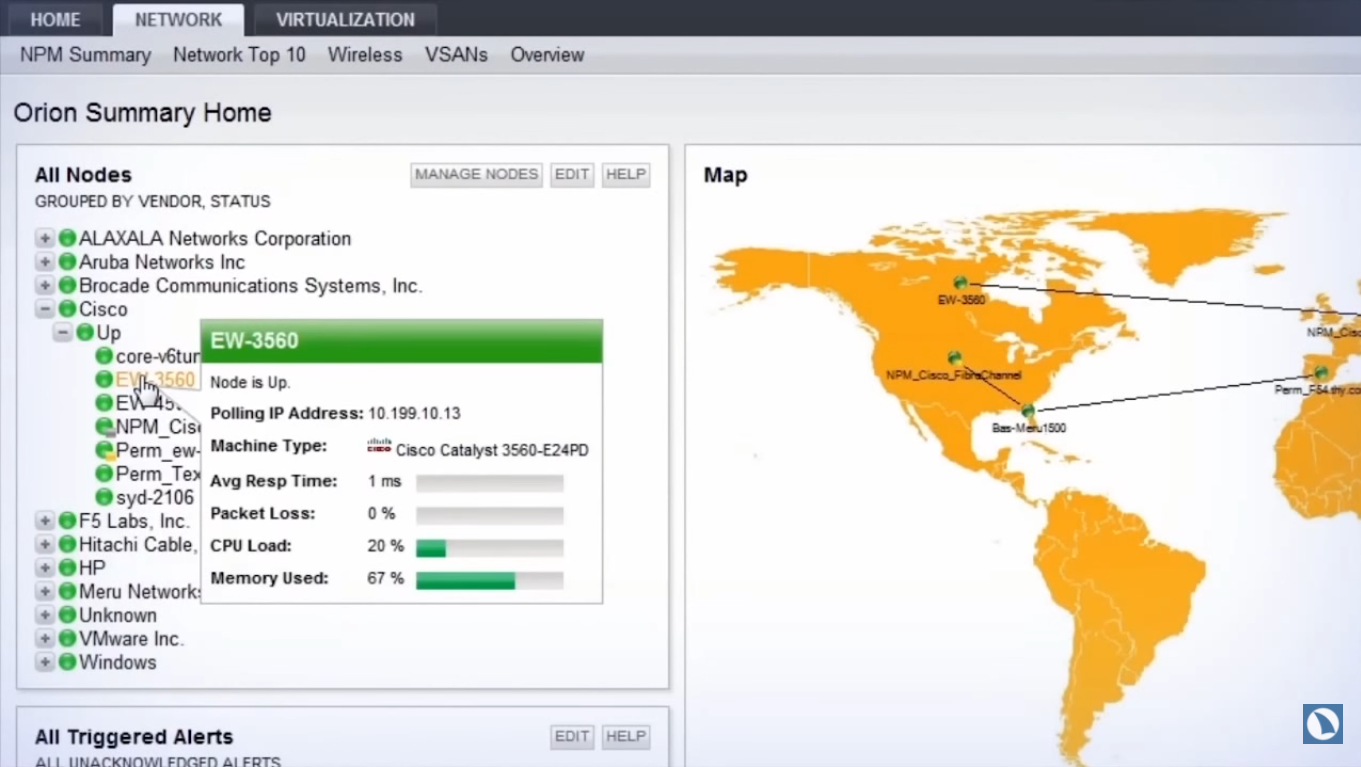


Figura 1. Equipos monitorizados y su ubicación

Con NPM se puede visualizar cada una de las características el equipo monitoreado como su disco, CPU y memoria

Características claves de NPM

* **Rendimiento y gestión de fallos**

A través de una interfaz web de vanguardia, ofrece una vista unificada del rendimiento de cientos o miles de nodos e interfaces en tu red. Por medio de una plataforma única, supervisa y analiza en tiempo real las mediciones de rendimiento de la red para enrutadores, conmutadores, servidores y cualquier otro dispositivo habilitado para SNMP.

* **Interfaz intuitiva**

Proporciona una interfaz web altamente “amigable” y personalizable, que admite múltiples vistas por usuario y departamento, así como vistas sobre mapas, en tiempo real y "Top 10" de vistas de su red global.

* **Alertas avanzadas**

Permite la configuración de alertas avanzadas para eventos correlacionados y combinaciones complejas de estados del dispositivo.

* **Generador de informes**

El avanzado motor de informes de **Orion NPM** te permite generar reportes de red personalizados rápidamente, los cuales pueden ser impresos, o visualizados en la web.

2.2 wireshark

Permite analizar la red como si viéramos una placa con un microscopio en un laboratorio por así decirlo y proporciona herramientas y comandos para filtrar y analizar con más detalles el tráfico de red, acercándose a la causa raíz del problema.

Los administradores de sistemas y de red lo usan para identificar dispositivos defectuosos que están descartando paquetes, problemas de latencia en peticiones causadas por máquinas defectuosas que enrutan el tráfico de red a cualquier lado del mundo posible y exfiltraciones de datos o incluso intento de ataque con malware o de piratería contra una organización.

## **Características Wireshark**

* Permite seguir el rastro a los paquetes TCP stream, podemos ver todo lo relacionado con dicho paquete, el antes y el después, pudiendo aplicarles filtros personalizados a estos mismos sin perder el flujo.
* Se puede decodificar los paquetes y exportar en formatos específicos y guardar dichos objetos.
* Permite ver **estadísticas de los paquetes capturados** incluyendo un resumen, jerarquía de protocolos, conversaciones, puntos finales y gráfica de flujos entre otros.
* Análisis fácil e informativo mediante resolución de nombres por mac, por red, etc… y reensamblaje de paquetes.
* Cuenta con una herramienta de líneas de comandos para ejecutar funcionalidades llamada TShark, similar al terminal de linux. Entre los comandos más destacados, podemos mencionar rawshark, editcap, mergecap, text2pcap.

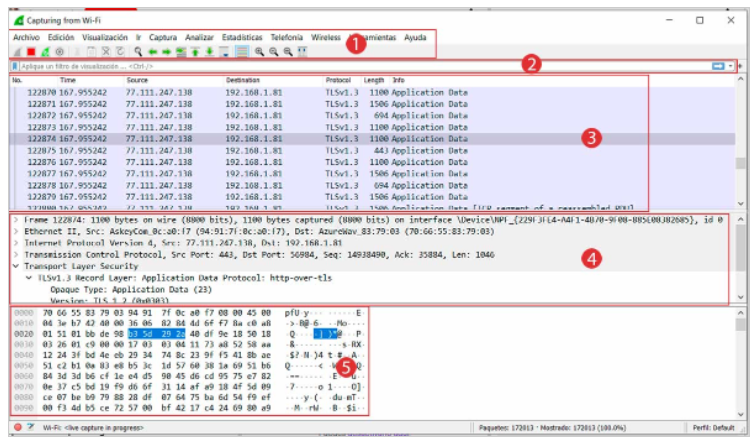


Figura 2. Componentes pantalla wireshark

1. **Barra de menú y de herramientas**: Este apartado es el común al 90% de las aplicaciones, por lo que no requiere de mayor explicación.
2. **Barra de filtrado**: Este apartado es fundamental, pues es en el que podemos definir las condiciones que deben cumplir los paquetes analizados para mostrarse en el apartado inferior. Definir los filtros es la parte más interesante, y también una de las más complejas de Wireshark. En este artículo veremos un primer ejemplo de uso, y próximamente profundizaremos en sus posibilidades.
3. **Paquetes capturados**: En este apartado se muestran todos los paquetes capturados por Wireshark. Como puedes ver, cada fila representa un paquete, y para cada uno de ellos, y por columnas (personalizables) se muestra un indicador de orden dentro de la sesión de captura, el momento de la captura, direcciones IP de origen y destino, protocolo de red empleado, longitud del paquete e información adicional.
4. **Contenido del paquete**: En este apartado puedes analizar, para cada paquete, información sobre cada una de sus capas (basadas en el modelo OSI).
5. **Contenido de la capa**: Si seleccionas una de las capas del paquete, en este apartado verás el contenido de la misma en un visor hexadecimal.

[Primeros pasos con Wireshark: ¿qué está pasando en tu red? (muyseguridad.net)](https://www.muyseguridad.net/2020/08/04/primeros-pasos-con-wireshark/)

[Wireshark: Qué es y ejemplos de uso | OpenWebinars](https://openwebinars.net/blog/wireshark-que-es-y-ejemplos-de-uso/)

[479) Solarwinds NPM | network performance monitor | introdución rápida - YouTube](https://www.youtube.com/watch?v=nbmtlCyUyG8&ab_channel=Danysoft)

[Guía completa para mejorar tu seguridad TI e infraestructura (e-dea.co)](https://www.e-dea.co/blog/resuelve-tus-problemas-de-infraestructura-ti-con-npm/network-performance-monitor" \l ":~:text=Orion%20NPM%20%28Network%20Performance%20Monitor%29%20de%20SolarWinds%20es,adaptable%20a%20las%20necesidades%20puntuales%20de%20cada%20organizaci%C3%B3n.)