TAREA ONLINE UNIDAD 6 .-

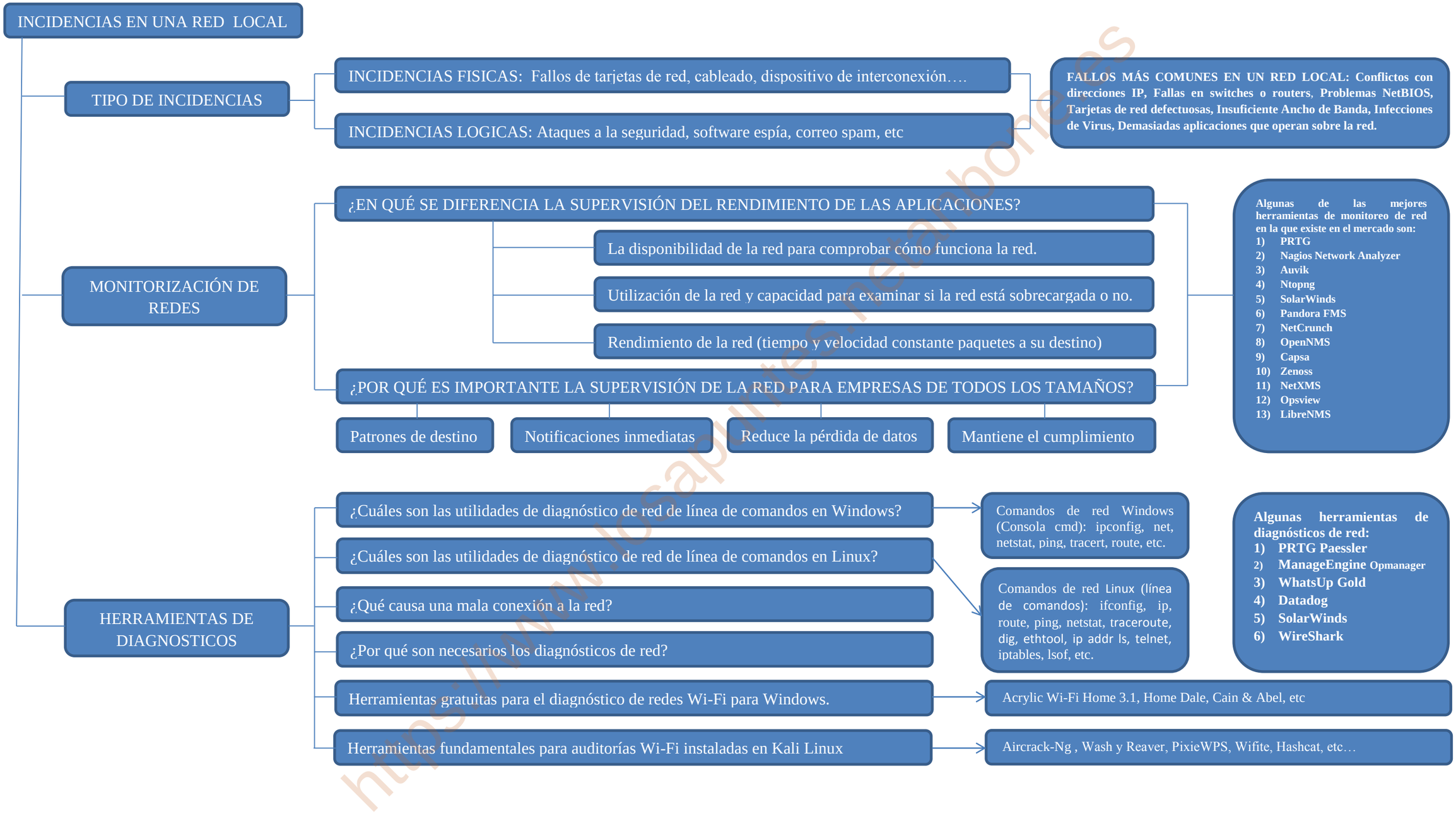
RESOLUCIÓN DE INCIDENCIAS DE RED

IES CASTILLO DE LUNA, ROTA (CÁDIZ)
GRADO MEDIO SEMIPRESENCIAL SISTEMA MICROINFORMÁTICOS Y REDES
MODULO: REDES LOCALES
CURSO ACADEMICO: 2021/2022
ALUMNO: ANTONIO NAVAS BERNAL
MAYO 2022

INDICE

Realizar un mapa conceptual del tema, explicando:

MAPA CONCEPTUAL DE INCIDENCIAS EN REDES LOCALES



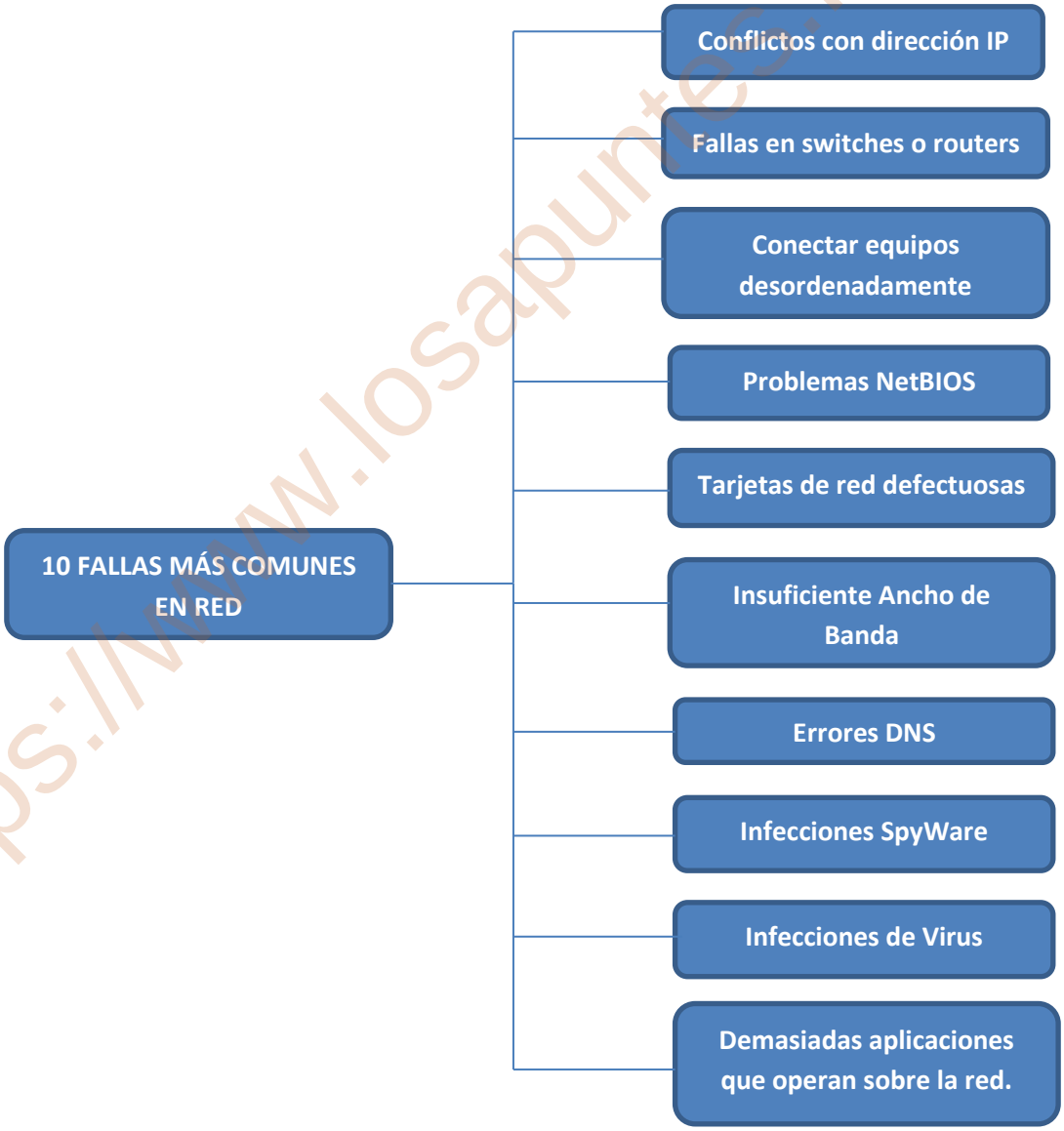
1) Las posibles incidencias de pueden ocurrir en una red.

Las incidencias a nivel de red, que son las que se derivan de la capa 3 de la pila OSI, y en específico, los problemas relacionados con **el protocolo de direccionamiento de Internet**; IP *Internet Protocol* ya que es el protocolo que usa, junto con la capa de transporte, para identificar el puesto de destino en la red mundial de Internet. Los fallos más habituales a nivel de red son, por tanto, consecuencia del direccionamiento o *enrutamiento* de direcciones IP, y los de aplicación, suelen derivar del control de acceso, o reasignación de direcciones locales, por lo que los protocolos ACL (*Access Control List*) y NAT (*Network Address Translation*) son de especial importancia.

Una red "Lenta" es un problema serio, usuarios disgustados, ralentización en el trabajo, sobrecarga de trabajo para el departamento de computación, etc.

Muchas veces al enfrentarnos a estas situaciones pensamos que hay un extraño y complejo problema que afecta nuestra red, mas suele no ser así y muchas veces se puede lograr una mejora significativa solo con revisar las cosas más básicas.

Las fallas más comunes en la red son:



1.- Conflictos con direcciones IP

Los servicios DHCP en general, poseen sistemas que les ayuda a prevenir que asignen una IP repetida a un equipo en la red. Sin embargo ocasionalmente puede ocurrir que 2 equipos tengan la misma IP, ya que uno de ellos puede estar configurado estáticamente. Este hecho se conoce como IP Duplicada.

Lo primero es mantener nuestra red ordenada, eso nos evita problemas y nos ayuda a detectar la falla rápidamente si se presenta. Después podemos verificar que no tenemos 2 servidores DHCP funcionando, por ejemplo nuestro servidor de datos que actúa también como servidor DHCP y un router, que generalmente servidor DHCP es su configuración por defecto.

2.- Fallas en switches o Routers

En algunos casos las fallas en la red no tienen una causa aparente. Por ejemplo, nuestra máquina puede enviar y recibir correos sin problemas mas no tiene acceso a internet, o estamos tranquilamente navegando la red cuando de un momento a otro se pierde el acceso y pasados algunos minutos hay internet de nuevo.

Cuando los problemas de conectividad son locales el problema puede solucionarse reiniciando el switch de acceso o router.

Si estos problemas se repiten demasiado frecuentemente, es necesario revisar la calidad de nuestra fuente de energía, cambios del suministro eléctrico puede provocar equipos pegados o incluso daños en nuestros routers o switches. Después de todas estas verificaciones tal vez sería bueno probar con otro switch, ya que quizás el que tienes está dañado y todo lo que hagas no corregirá el problema.

3.- Conectar equipos desordenadamente

La necesidad de conectividad suele crecer demasiado rápido, y esto provoca que se terminen conectando equipos simplemente al “switch más cercano” o conectar un switch al “switch más cercano” y así infinitamente.

Cuando esto ocurre los datos deben recorrer largas distancias antes de llegar a su destino, además de aumentar los lugares que podrían causar fallas.

Una buena Práctica es anticiparse al crecimiento y evitar estos parches en nuestra red por nuevos usuarios, o reorganizar procurando consolidar lo disperso en un sistema potente y estable.

4.- Problemas NetBIOS

NetBIOS es un protocolo de Windows que permite a las computadoras en una red “hablar”. Sin embargo frecuentemente no trabaja adecuadamente provocando lentitud en nuestra red o generando errores al acceder los archivos compartidos y a veces el corte del servicio.

Una Opción es identificar los equipos con conflictos y renombrar uno de ellos. Para analizar los nombres de la red puede utilizar una herramienta como AngryIpScanner.

Comportamientos extraños en los recursos de la red pueden ser causados cuando los ordenadores tienen el mismo nombre. Deshabilitar el servicio de resolución de nombres WINS/NetBT podría solucionar este problema.

5.- Tarjetas de red defectuosas

Un problema común es la presencia de este tipo de fallas. Cuando un equipo produce errores esporádicos o intermitentes, sobre todo cuando están relacionados con una estación de trabajo en particular. Una manera muy fácil de verificar el funcionamiento de nuestra tarjeta es prestar atención el LED verde o blanco que viene en cada una de ellas, que debe parpadear o permanecer encendida, sino, debes verificar que el cable está conectado correctamente y en buenas condiciones.

6.- Insuficiente Ancho de Banda

Puede ocurrir que simplemente el ancho de banda que tenemos no abastece todas las exigencias de la red, puede ser de manera local como de internet, es bueno invertir en nuestra red de comunicaciones, un cable Cat5E puede ser muy poco si las exigencias son muy altas, tenemos cables Cat6 o incluso Cat7 que se pueden utilizar en la red. También nuestro ancho de banda en la red local puede ser afectada por la calidad de nuestros Switches o routers, 1 solo switch 10/100 puede hacer lenta una red de 10/100/1000, Así que cuidado.

7.- Errores DNS

Básicamente los servidores DNS nos ayudan a resolver nombres, para acceder a google.com después de escribirlo en nuestro navegador el sistema lo resuelve y luego vemos la página en nuestro navegador. Puede darse el caso en que Windows nos informe que tenemos acceso a internet, más al intentar acceder a alguna Web nos dé error NAME NOT RESOLVED, verifica tus DNS.

8.- Infecciones SpyWare

En esencia un virus de este tipo transmite información de nuestro ordenador a una entidad externa, obviamente sin nuestro permiso.

Esto podría saturar nuestra red compartiendo nuestros datos sin darnos cuenta, así que cuidado, siempre mantenga su antivirus activo y actualizado.

9.- Infecciones de Virus

En este punto son clave las normas o políticas de la empresa en cuanto al uso de internet, la disciplina puede ahorrarnos muchísimos problemas.

Ante una falla repentina, nunca está de más un escaneo de virus en cada terminal de la red. Una sola terminal infectada puede estar generando miles de correos SPAM que congestionan nuestra red.

10.- Demasiadas aplicaciones que operan sobre la red.

En muchos casos desde internet se instalan programas que se conectan a internet, software P2P (peer to peer), etc. Que sobrecargan inútilmente nuestra red. Identificarlos y desactivar los que no son esenciales es crítico.

2) Programas o Software que se utiliza para monitorizar una red, ya sea en Unix o en Windows.

El monitoreo de red es el proceso en el que se supervisan los componentes de la red, como servidores, cortafuegos, conmutadores, enrutadores, etc., es lo que se puede llamar supervisión de red.

De manera similar, el software utilizado para monitorear todos esos componentes se conoce como software de monitoreo de red. Es un arma crucial en su caja de herramientas que puede solucionar problemas de red e informar al administrador las cosas van mal.

La herramienta recopila datos útiles de varias partes de su red y ayuda a controlar y administrar la red. Aquí, la atención se centra en la supervisión de fallas, la supervisión de cuentas y la supervisión del rendimiento.

Para examinar su red, el software puede enviar señales (o pings) a diferentes puertos del sistema. Si el monitoreo de la red es proactivo, ayudará a encontrar la solución a un problema de red dado antes para evitar tiempos de inactividad o fallas de la red.

Todo el proceso se desarrolla principalmente en tres pasos:

- Ping: esta técnica básica utilizada por el software para probar la disponibilidad de la red
- SNMP (Protocolo simple de administración de red): monitorea los dispositivos por separado dentro de una red con la ayuda de una herramienta de monitoreo
- Scripts: llenan los vacíos entre las funcionalidades de la herramienta de monitoreo

¿En qué se diferencia de la supervisión del rendimiento de las aplicaciones?

Supervisión del rendimiento de la aplicación: Software evalúa cómo funcionan o funcionan sus aplicaciones utilizando los recursos que requieren, como el acceso a la red.

Por otro lado, el monitoreo de la red monitorea los dispositivos que operan la red, por ejemplo, servidores, enrutadores y conmutadores.

Supervisa principalmente tres cosas:

- La disponibilidad de la red para comprobar cómo funciona la red.
- Utilización de la red y capacidad para examinar si la red está sobrecargada o no.
- Rendimiento de la red para comprobar si los paquetes de datos llegan a los destinos respectivos a tiempo y con una velocidad constante.

¿Por qué es importante la supervisión de la red para empresas de todos los tamaños?

Muchas organizaciones pasan por alto el monitoreo de la red, pensando que todo está bien con sus redes. Pero solo porque todo parece estar bien en la actualidad, no significa que permanecerá como está, especialmente en la era de Ataques cibernéticos y otros factores.

El software de monitoreo de red está diseñado para mantener su red funcionando de manera óptima. También es una excelente manera de mejorar el rendimiento de la red.

El software alerta a los administradores sobre la identificación de un enlace de red débil o equipo sobrecargado antes de que se convierta en un problema. De esta manera, los administradores pueden ajustar fácilmente las configuraciones de red según los requisitos para eliminar los cuellos de botella y reducir las cargas innecesarias.

Patrones de destino

Estas herramientas son excelentes para encontrar los patrones de rendimiento de su red. Por lo tanto, si encuentra que el equipo tiene un rendimiento deficiente, los administradores podrían determinar su causa en una fase inicial e implementar una solución perfecta para ello.

Notificaciones inmediatas

Los sistemas tradicionales pueden necesitar que verifique todo manualmente para ver si hay un error en su red. Las herramientas de tutoría en red son avanzadas y no pierden tiempo en enviarle notificaciones. Como resultado de esta rapidez, es eficiente para minimizar los tiempos de inactividad y los problemas para que pueda tomar medidas inmediatas.

Reduce la pérdida de datos.

Si su red está infiltrada y es propensa a errores, puede perder datos comerciales esenciales, ¡cuyos impactos son alarmantemente peligrosos!

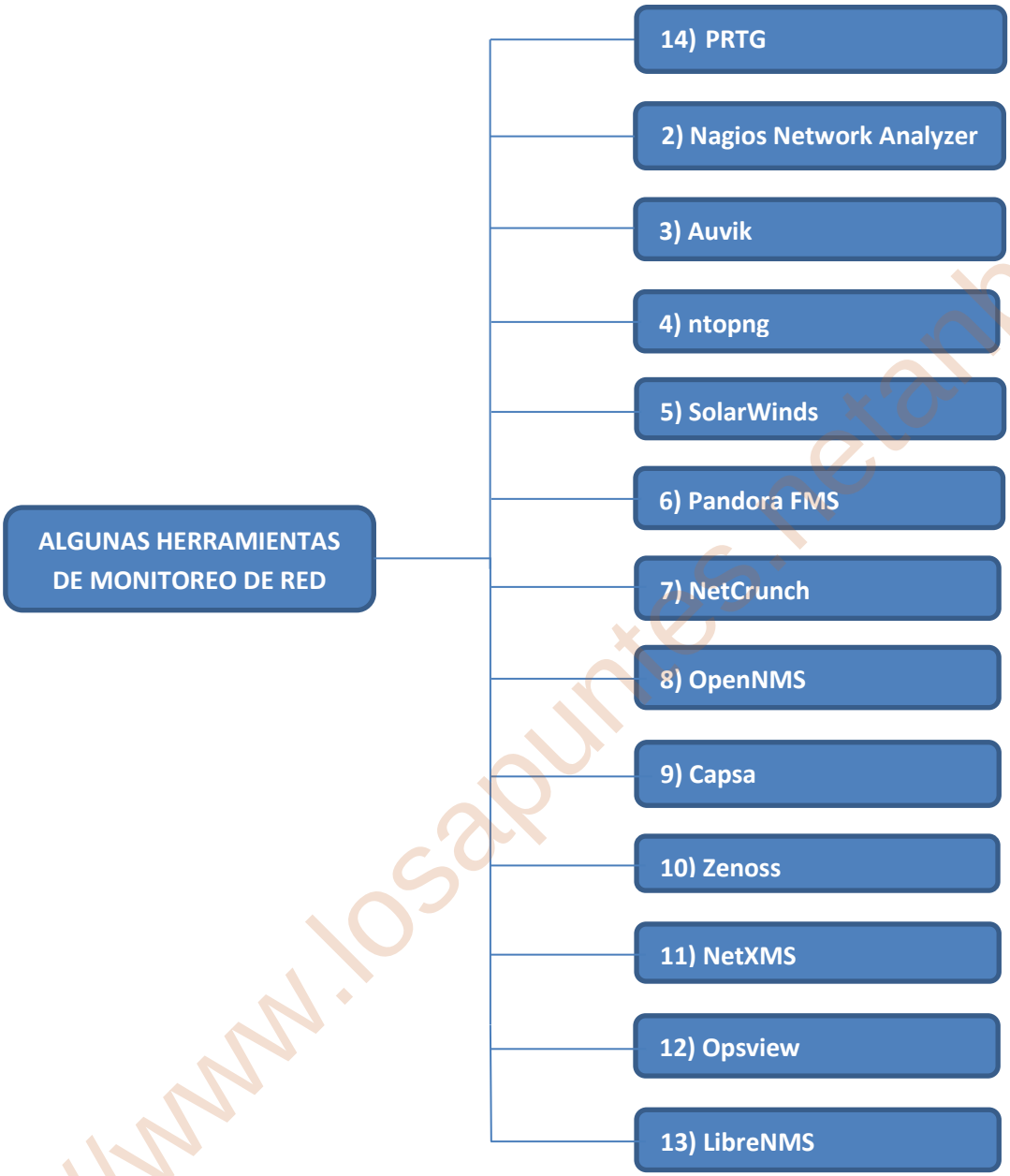
En consecuencia, sus archivos pueden corromperse, los correos electrónicos comienzan a caer, las amenazas a la seguridad, la productividad se deteriora y todo eso.

Los sistemas de monitoreo de red le brindan un respiro absoluto de tales cosas al detectar problemas de antemano y permitirles solucionarlos mientras aún hay tiempo.

Mantiene el cumplimiento

Las herramientas pueden compilar una enorme base de datos de información útil sobre el cumplimiento. Por lo tanto, si se produce algún problema de cumplimiento potencial, se le notificará para que lo resuelva antes de que los organismos reguladores puedan imponerle multas enormes. Por lo tanto, es mejor evitar todos estos problemas y aprovechar el software de monitoreo de red para ejecutar su negocio o empresa sin problemas.

Una vez resumido el concepto y el uso de la misma, algunas de las mejores herramientas de monitoreo de red en la que existe en el mercado son:



1) PRTG

No permita que los cuellos de botella de la infraestructura de TI obstaculicen su trabajo.

PRTG Network Monitor puede monitorear de manera eficiente sus dispositivos, sistemas y aplicaciones de red.

PRTG es una solución intuitiva que no requiere complementos adicionales y es adecuada para cualquier negocio, sin importar el tamaño. Le permite determinar los consumos de ancho de banda de la red, monitorear bases de datos, administrar aplicaciones y extraer sus estadísticas detalladas. También lo ayuda a administrar y monitorear servicios de computación en la nube, múltiples tipos de servidores en tiempo real, redes locales como enrutadores, impresoras, estaciones de trabajo, etc.

PRTG viene con características como:

- Tecnologías compatibles: admite SNMP, WMI, SSH para macOS, Linux o Unix, y análisis de tráfico mediante protocolos de flujo y rastreo de paquetes, solicitudes HTTP, Ping, SQL y API REST para devolver JSON y XML
- Mapas y paneles: PRTG utiliza mapas en tiempo real, incluido el estado en vivo, para ver su red. Cree paneles de control personalizados e integre componentes de red a través de más de 300 objetos de mapa como gráficos de tráfico, iconos de estado, listas principales, etc.
- Las alertas flexibles ofrecen muchos mecanismos incorporados para alertas como solicitudes HTTP, notificaciones push o correos electrónicos.
- Una interfaz de usuario con todas las funciones: su interfaz web está construida en AJAX mientras mantiene alta seguridad, rendimiento y diseño receptivo
- Solución de conmutación por error: cuando el nodo principal está inactivo o no está conectado, otro nodo se hace cargo de inmediato para proporcionar el manejo de la conmutación por error automáticamente
- Informes detallados: obtenga estadísticas, números y gráficos que contienen sus datos de monitoreo. Exporte información histórica de monitoreo en archivos PDF, CSV, XML y HTML y ejecute informes a pedido o prográmelos mensualmente, semanalmente o diariamente.

2) Nagios Network Analyzer

Con la confianza de grandes marcas como Disney, Universal, Cisco y más, Nagios es una de las mejores herramientas disponibles en el mercado. Proporciona un análisis extenso de su red y fuentes de tráfico junto con las amenazas a la seguridad.

Por lo tanto, los administradores del sistema pueden recopilar rápidamente datos de alto nivel sobre el estado de la red para encontrar la mejor solución posible. El software viene con una poderosa interfaz web que es fácil de usar y permite consolidar notificaciones y alertas.

Nagios Network Analyzer ofrece una vista centralizada de los datos de ancho de banda de su red y los posibles compromisos con mayor claridad. Su panel intuitivo le permite analizar fuentes de datos fundamentales de NetFlow, comportamiento anormal de la red y métricas del servidor para evaluar la red.

El software puede adaptarse al entorno existente de los usuarios para una implementación sencilla, de modo que pueda comenzar rápidamente. Además, las funciones complementarias también le permiten enviar notificaciones SNMP para la gestión de capturas y la supervisión. Incluye calculadora para ancho de banda utilización que puede personalizar. Le ayuda a crear informes para resumir las direcciones IP, la utilización / fuente de ancho de banda, etc.

3) Auvik

Auvik es un software de monitoreo de red basado en la nube fácil de usar que le permite tener una visibilidad y un control precisos de su red. Le dará notificaciones y alertas instantáneamente cuando algo salga mal para que pueda detectar anomalías con la ayuda de herramientas de análisis de tráfico.

Identifique la causa raíz fácilmente a partir de los registros del dispositivo y realice un seguimiento de dónde está conectado cada dispositivo. Auvik tardará menos de una hora en monitorear su red para descubrir sus activos de TI, conocer la configuración de la red y ver los cambios. Cifra datos con cifrado AES-256 y ofrece actualizaciones de rendimiento y seguridad automáticamente.

Auvik TrafficInsights le brinda una descripción general completa de quién está en la red, qué están haciendo y hacia dónde se dirige el tráfico. También puede navegar por el panorama general, reducir los dispositivos para investigar correctamente y profundizar para extraer información. Conectar sus dispositivos de forma remota en el inventario de Auvik también le permite conocer los problemas sin moverse de su escritorio.

Puede dormir bien sabiendo que obtiene copias de seguridad de las configuraciones, como configuraciones de dispositivos, configuraciones históricas, etc. Además, puede restaurar rápidamente todas las configuraciones cuando sea necesario. Garantizará que solo los usuarios autorizados puedan realizar cambios en la red con configuraciones de permisos, apalancamiento 2FA y registros de auditoría. También puede utilizar herramientas comerciales de terceros para crear un potente flujo de trabajo.

4) ntopng

ntopng es la versión de próxima generación de ntop, una de las mejores herramientas de monitoreo de tráfico de red. Esta herramienta basada en libpcap está escrita de forma portátil para ejecutarse en cualquier plataforma UNIX, Windows o macOS.

Obtiene una interfaz web inteligente para explorar información sobre el tráfico histórico y en tiempo real junto con los hosts activos. Puede ordenar el tráfico según el protocolo L7, el puerto, la dirección IP, los sistemas autónomos y el rendimiento.

ntopng produce informes de métricas de red que incluyen protocolos de aplicaciones, remitentes y receptores, latencias de aplicaciones y redes, estadísticas de TCP como retransmisiones, paquetes perdidos, tiempo de ida y vuelta (o RTT) y más.

Puede superponer y geolocalizar hosts en un mapa y explorar protocolos de aplicaciones con la tecnología ntop Deep Packet Inspection (nDPI). ntopng admite túneles IPv4,

IPv6, GTP o GRE, junto con ElasticSearch, MySQL, LogStash para exportar datos monitoreados.

5) SolarWinds

SolarWinds es un nombre popular en la industria y su NetFlow Traffic Analyzer (NTA) (NTA) es otro producto increíble de la empresa. Es una solución poderosa con muchas funciones y herramientas útiles creadas para traducir detalles finos en informes y gráficos completos.

NTA le ayuda a identificar los mayores recursos que agotan su ancho de banda y otros usos y tráfico de la red. Recopila métricas de tráfico de red de varias fuentes de datos, incluido NetFlow.

De esta manera, puede comprender qué aplicaciones, protocolos y usuarios consumen el mayor ancho de banda. También puede examinar sus patrones de tráfico y monitorear puertos específicos, direcciones IP, etc. para encontrar la causa real de los problemas de red.

NTA viene con características como:

- Solución rápida y segura: NTA fomenta la resolución rápida de problemas, una mayor visibilidad de los flujos de tráfico malicioso y una mayor eficiencia.
- Integración total: funciona sin problemas con plataformas Orion, como Network Performance Manager (NPM) y Network Configuration Manager (NCM).
- Conversación: al combinar NTA con NCM, puede ver las conversaciones de tráfico basadas en las políticas de NCM.
- Monitoreo del ancho de banda: vea los registros de flujo de IPv4 e IPv6 y monitoree aplicaciones como Cisco NetFlow, sFlow, Juniper J-Flow, Huawei NetStream, etc.
- Alertas: Reciba notificaciones en caso de que algún dispositivo funcione mal para que pueda actuar rápidamente
- Análisis de tráfico: realice un seguimiento de los patrones durante minutos, días y meses para recopilar y correlacionar datos en formatos utilizables y presentarlos en una interfaz web para el control del tráfico.

6) Pandora FMS

Supervise cientos y miles de dispositivos, sistemas, aplicaciones y redes mediante pandora fms. Incluye un montón de funciones en una única licencia para ofrecer una solución de red homogénea.

Pandora FMS ha eliminado con éxito los cuellos de botella en los sistemas de red desde 2004. Puede monitorear fácilmente las redes de sus clientes sin acceso externo a través de sus servidores de clientes. Los servidores se implementan rápidamente y se administran de forma centralizada, a pesar de que no hay conexión directa.

Algunas de las características básicas de Pandora FMS son:

- Detección de cambios en la configuración del sistema de red
- Inventario remoto de software y licencias

- Monitoreo para computadoras Linux, Unix y Windows
- Gráficos históricos, hasta hace 3 años
- Informes avanzados de tiempo de actividad, gráficos para la planificación de la capacidad, SLA y más
- Gestión de capturas SNMP y sondeo SNMP versión 3
- IPAM integrado para administrar direcciones IP
- Sondas descentralizadas para disfrutar de una mayor escalabilidad y flexibilidad.
- NetFlow para la gestión del rendimiento y la capacidad de las redes
- Detección automática de redes en los niveles 2 y 3

Ejecute análisis de red en tiempo real utilizando NetFlow, sFlow o JFlow con Pandora FMS. Obtenga un análisis en profundidad de las estadísticas de tráfico, informes y mapas dinámicos basados en el tráfico nodal.

7) NetCrunch

NetCrunch es una plataforma de monitoreo eficiente para varios componentes de red como servidores, enrutadores, servicios de virtualización, cámaras, dispositivos IoT, cortafuegos, y más. Es una solución asequible y fácil de usar en la que puede ver con precisión el rendimiento y el estado de sus componentes de red.

Lo que distingue a NetCrunch de los demás es su capacidad para administrar y configurar alertas, monitorear la configuración de acuerdo con políticas y métricas de rendimiento. Incluso puede controlar parámetros de disponibilidad como Ping, SSH, HTTP, FTP, etc. NetCrunch observa todas las conexiones y luego las refleja en diferentes vistas gráficas automáticamente como mapas de segmento de capa 2.

Además, puede monitorear tecnologías basadas en flujo, incluyendo JFlow, sfFlow, NetFlow, etc. Puede monitorear sistemas operativos como BSD, macOS X, Linux y Windows sin agentes. Es compatible con el monitoreo de Hyper-V y ESXi y permite monitores web, Dockers, registros de texto, servidores SQL, nube, etc.

NetCrunch puede recibir alertas de activación y eventos en ciertas reglas predefinidas como Syslog, trampas SNMP, mensajes web, Registro de eventos de Windows, etc. Le permite analizar registros de texto con sensores SSH sin descargar todos los registros de datos.

8) OpenNMS

OpenNMS es una plataforma integrada, de código abierto y de nivel empresarial para la creación de servicios de monitoreo de redes. Su comunidad se dedica a crear soluciones interoperables.

La plataforma normaliza los mensajes específicos del dispositivo y del proveedor junto con las medidas de rendimiento específicas del protocolo. Aquí, se puede acceder a los datos a través de una API REST para aplicaciones de gestión de flujo de trabajo de alto nivel. También puede ampliar esta plataforma ejecutando scripts en el sistema operativo o utilizando una API Java nativa.

Aprovecha para construir tu integración de emisión de boletos o usa sus integraciones predefinidas. Utilice eventos monitoreados para generar alarmas y luego reenviarlas a aplicaciones externas integradas en sus flujos de trabajo de administración.

9) Capsa

Capsa es una herramienta portátil para monitorear, analizar y solucionar problemas de red. Viene con una interfaz simple que es fácil tanto para los usuarios novatos como para los veteranos y evalúa las amenazas en línea.

Es adecuado tanto para WLAN como para LAN y tiene captura de paquetes de paquetes capacidades en tiempo real, monitoreo 24 × 7, análisis de protocolo sofisticado, diagnóstico experto y decodificación de paquetes.

Algunas de las características de Capsa son:

- Análisis de llamadas de VolP para ayudarlo a solucionar problemas de redes relacionadas con VolP.
- Varias formas de recibir notificaciones
- Programador de tareas para programar la captura y el análisis de paquetes diariamente, semanalmente o por única vez
- Análisis de flujo de TCP para proporcionar datos sobre redes lentas, descargas, transacciones CRM, etc.
- Gráficos para el ancho de banda de la red y las estadísticas de tráfico.
- Supervisa múltiples comportamientos de red como HTTP, DNS, correos electrónicos, FTP, Yahoo Messenger y MSN

10) Zenoss

Zenoss le permite monitorear todas sus redes virtuales y físicas, incluida la infraestructura local y en la nube. Extrae, ingiere, correlaciona e indexa sus datos en una arquitectura cohesiva para una inteligencia procesable. Recopila y registra datos de sus sistemas para comprender el estado actual de su infraestructura y aplicaciones.

La herramienta ayuda a mitigar las interrupciones de la red al alertar, aislar y resolver problemas de inmediato. Zenoss utiliza una red dinámica y centralizada y un inventario de direcciones IP para dispositivos, creando un mapa automático para la topología de la red y actualizándolos.

Zenoss suprime los eventos sintomáticos en las fallas de red de capa 3 para eliminar la propagación de problemas, acelerar su aislamiento e identificar la causa raíz. Muestra métricas de disponibilidad y rendimiento de la red, como velocidades, operaciones y patrones del tráfico entrante y saliente. Además, puede visualizar rutas de red cruciales en entornos locales, en la nube o híbridos.

11) NetXMS

Otro sistema de monitoreo de red de código abierto en la lista es NetXMS. Opera en redes enormes que tienen miles de servidores; por tanto, es escalable. También es altamente personalizable, ya que puede integrarlo fácilmente con otras soluciones de terceros.

NetXMS es compatible con Windows y los principales sistemas Unix y ofrece cifrado estándar de la industria para una mejor seguridad y control de acceso. Ofrece descubrimiento automático de dispositivos de Capa 2 y 3, búsqueda y visualización. Es compatible con SNMPv3, descubrimiento activo mediante sondas de exploración y descubrimiento pasivo a través de interfaces y tablas de enrutamiento.

NetXMS es compatible con NAT y ofrece proxies para ICMP, SNMP y protocolo nativo. Promueve la administración remota y le permite enviar comandos SNMP, transferir archivos, etc. También admite el escalado horizontal y la tutoría distribuida.

12) Opsview

El analizador de redes de Opsview le permite ver el uso del protocolo de su red, transferencias de datos, pérdida de paquetes, nodos finales que reciben y transmiten datos, y más. Con Opsview, puede encontrar trampas SNMP, traducirlas a través de SNMP MIB y aplicar reglas para determinar alertas y sus mensajes.

Net Audit le permite realizar copias de seguridad de las configuraciones de red, eliminando el riesgo de perder la configuración si se realiza algún cambio.

Flow Collector permite el análisis y la recopilación de dispositivos habilitados para el flujo como Cisco NetFlow, conmutadores HP, etc. Por lo tanto, puede identificar aplicaciones problemáticas rápidamente y tomar medidas de mitigación como redirigir el tráfico, optimizar la configuración, aumentar el ancho de banda, etc.

13) LibreNMS

La solución de monitoreo de red con todas las funciones: LibreNMS tiene muchas capacidades útiles. Puede descubrir automáticamente su red mediante SNMP, ARP, BGP, OSPF, LLDP, FDP y CDP. Ofrece un sistema de alerta altamente flexible y le notifica a través de Slack, IRC, correos electrónicos, etc.

Con el acceso a la API, puede administrar, recuperar y mapear datos. LibreNMS promueve el escalado horizontal con encuestas distribuidas para crecer más con la red. También viene con aplicaciones nativas de iPhone y Android para que pueda monitorear sobre la marcha.

Además, se integra con NfSen, SmokePing, collectd, RANCID y Oxidized.

Mejores prácticas para el monitoreo de redes

Elegir un buen software de monitoreo de red es solo el primer paso. A continuación, debe aplicar las mejores prácticas para implementar el monitoreo de la red.

- Conciencia sobre su red: es vital rastrear en su red todos los cambios implementados, áreas cubiertas, hardware y servidores involucrados, dispositivos remotos, los tipos de red que requieren monitoreo y más.
- Haga planes de alerta: las alertas deben llegar a las personas adecuadas y en el momento adecuado; de lo contrario, la instalación del software de monitoreo no ayudará. Designar un responsable específico para que se ocupe de diferentes aspectos de la red con responsabilidades claras.
- Evaluación regular: considere evaluar su red regularmente porque las redes, junto con los miembros de su equipo, cambian.

3) Explica las herramientas de diagnóstico más utilizadas en Unix, Windows, para redes cableadas como inalámbricas.

¿Alguna vez ha experimentado una interrupción o desconexión de Internet, una red de área local (LAN) completa o una falla en la red de área amplia (WAN)? La principal causa de estos incidentes es el mal funcionamiento del dispositivo de red o la latencia en el ancho de banda de la red.

Los fallos o retrasos de la red provocan una pérdida masiva de ventas o una pérdida de confianza en la empresa, o una gran cantidad de usuarios insatisfechos.

Para abordar estas interrupciones y fallas, las organizaciones utilizan herramientas de diagnóstico de red para monitorear la infraestructura y los dispositivos de red. La herramienta alerta con anticipación para que los administradores puedan tomar las medidas necesarias para prevenir desastres.

Las herramientas de diagnóstico de red están diseñadas para escanear, analizar, identificar bloqueos en la infraestructura de red y enviar advertencias mucho antes de que ocurran errores. Dichas herramientas tienden a reducir las tareas tediosas como la administración de la red, el mantenimiento de la red, la resolución de problemas, la optimización del rendimiento, etc.

1.a) ¿Cuáles son las utilidades de diagnóstico de red de línea de comandos en Windows?

Hay muchas utilidades de línea de comandos que se utilizan para el diagnóstico de redes en Windows. A continuación, se muestran las 8 herramientas más utilizadas:

Silbido: Se utiliza para verificar la pérdida de paquetes y la latencia en la red.

seguimiento: Si desea saber cuántos saltos / dispositivos de red están disponibles entre el nodo de origen y el nodo de destino en la red, **Tracert** hará este trabajo. Se utiliza para encontrar los problemas de enrutamiento en la red.

ipconfig: Si desea comprobar el Dirección IP (IP4 / IP6), escapada predeterminada, DNS nombres del host, Ipconfig proporcionará todos estos detalles. Esta herramienta de línea de comandos mostrará los paquetes descartados y la cantidad de tráfico que fluye desde la interfaz de red.

NET: Este comando permite realizar un diagnóstico de funcionamiento de la red Microsoft en varios aspectos. También se utiliza para el acceso a recursos compartidos.

Netstat: Ayuda a averiguar qué puertos están abiertos y cuáles están escuchando. Desde el punto de vista de la seguridad, es de gran ayuda saber si algún puerto se ha visto comprometido por los atacantes.

escáner: En una red grande, si desea encontrar direcciones IP duplicadas o asignaciones de direcciones IP inapropiadas a los dispositivos, esta herramienta desempeñará un papel fundamental para lograrlo.

Ping: Informa del estado de un host. Es necesario permitir paquetes ICMP para sufuncionamiento

Nmap: Es usado para de **ping** dispositivos de red, transmisión de paquetes para encontrar detalles de hosts como puertos, versiones de SO, etc. Esta información recopilada puede integrarse en otras herramientas para encontrar problemas de conectividad y susceptibilidades.

Tracert: Indica la ruta por la que pasa nuestra petición hasta llegar al host destino.

Route: muestra y modifica la información sobre las rutas IP del equipo.

1.b) ¿Cuáles son las utilidades de diagnóstico de red de línea de comandos en Linux?

Hay muchas utilidades de línea de comandos que se utilizan para el diagnóstico de redes en Linux. A continuación, se muestran las herramientas más utilizadas:

Ifconfig: lo podrás utilizar para consultar la configuración de red del adaptador, aunque también te permite su modificación. Se puede utilizar este comando para comprobar si no hay ningún otro equipo que tiene asignada la misma dirección IP o para consultar si está activo el adaptador. (Equivalente de ipconfig en Windows).

Ip: lo puedes utilizar para consultar la configuración de los parámetros TCP/IP y de encaminamiento del equipo y también para modificarlos a bajo nivel.

Route: podrás consultar o establecer los parámetros de encaminamiento del equipo a bajo nivel.

Ping: al igual que en Windows, se utiliza para comprobar si el equipo puede enviar mensajes a la red o alcanzar a otros equipos.

Netstat: se utiliza para consultar los puertos abiertos o los puertos que están a la escucha en el equipo. Este comando se utiliza prácticamente igual que en Windows.

Traceroute: Este comando te permite ver los saltos que son necesarios para llegar al destino.

Dig: Al poner este comando nos permite verificar si el DNS funciona correctamente, antes de esto hay que asegurarse de que DNS en hemos puesto en la configuración.

Ethtool: Este comando nos permite ver si la tarjeta de red está físicamente conectada a la red, a parte también nos permite ver si está conectado al switch.

ip addr ls: Esto nos permite ver todas las tarjetas de red que tengamos y su respectiva IP.

Mtr: Significa My TraceRoute y te permite ver los saltos del router y un ping a cada uno. Con esto podemos ver que router tiene retrasos en el trafico de red.

Nslookup: Este comando sirve para saber la IP del host al que queremos llegar, y viceversa.

nmtui-edit: Significa Network Manager Text User Interface. Te permite configurar y modificar desde el terminal, con una interfaz gráfica, las configuraciones de la red.

Telnet: Con este comando se puede acceder a otra máquina para acceder de manera remonta, también se puede utilizar para consultar si tiene el puerto que queramos abierto o cerrado.

nmcli: Está enfocado a administrar las conexiones de red y sus configuraciones. Se puede utilizar para controlar Network Manager y modificar la configuración.

Tcpdump: Este comando sirve para capturar el tráfico de red de los paquetes, este comando es como el Wireshark pero sin interfaz gráfica.

iptables: Es ideal para gestionar el cortafuegos de los equipos, permite filtrar, bloquear o permitir algún tráfico.

lsof: Se encarga de listar los puertos abiertos en el servidor

Con estos comandos mejorar de una manera mucho más precisa los diferentes parámetros de una red en sistemas Linux.

2. ¿Qué son las herramientas de diagnóstico de red (NDT)?

Los NDT se utilizan para identificar, analizar, solucionar problemas y administrar redes de TI. Es la mejor herramienta para identificar problemas de rendimiento de la red y ayudar a tomar medidas preventivas antes de que ocurran cortes de red. Se pueden utilizar en redes LAN, WAN y WWW. Hay varias herramientas de pago y gratuitas en esta categoría.

3. ¿Qué herramientas debería utilizar para diagnosticar problemas con DNS?

Las herramientas pueden ser específicas para los sistemas operativos Windows o Linux, e incluso existen herramientas basadas en navegador. Las siguientes son las principales herramientas que se utilizan para diagnosticar errores del servidor de nombres de dominio (DNS):

- Dig and Host: Usado para el sistema operativo Linux
- Nslookup: línea de comandos para sistemas Windows
- Búsqueda de DNS: Herramienta basada en navegador

4. ¿Qué causa una mala conexión a la red?

Hay varias razones para una mala conexión de red, pero las siguientes son muy comunes:

- Congestión de la red debido a aplicaciones de hardware o software
- Problema de configuración de hardware
- Problemas con el sistema operativo o el software
- Problemas en la conexión física en la red.

5. ¿Cuáles son los problemas habituales de la red?

Aquí hay algunos problemas que seguramente ocurrirán en la red:

- Dirección IP duplicada o agotada
- Un problema para resolver un nombre de dominio
- El usuario no puede conectarse al servidor: el problema puede estar relacionado con el hardware o el software
- Problemas con las conexiones físicas a dispositivos de red como cortafuegos, SAN, enrutadores, conmutadores y más.
- Conexión de red lenta

6. ¿Por qué son necesarios los diagnósticos de red?

Con los logros innovadores de hoy en TI, existe una alta probabilidad de el malware o ataques digitales, interrupciones, choques y picos de tráfico inesperados. El uso de una herramienta de diagnóstico de red para mitigar este impacto le advertirá sobre fallas graves antes de que ocurra un incidente.

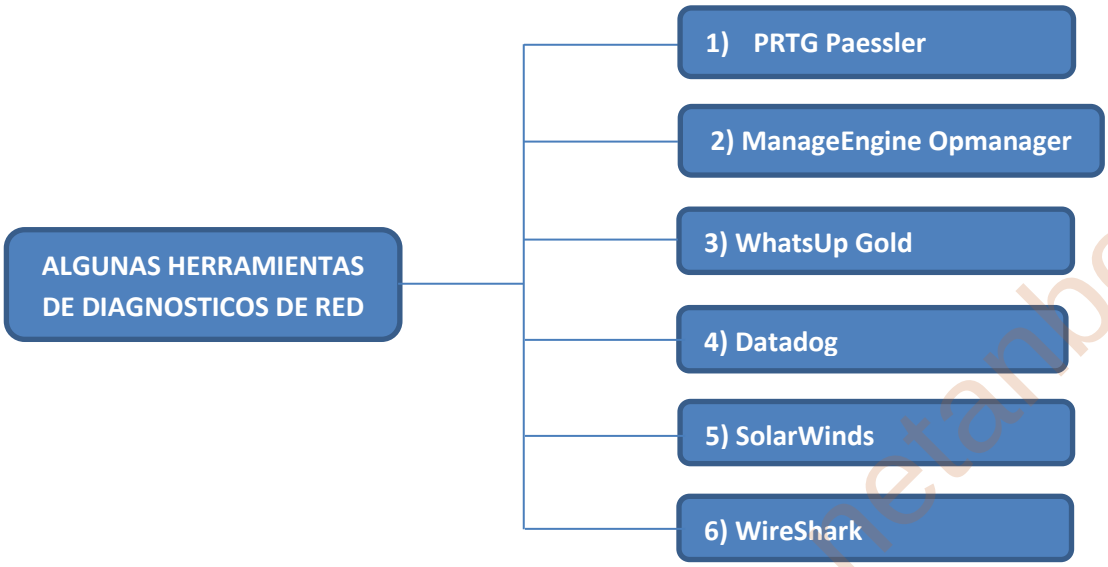
Además, esta herramienta mejora la gestión de la red al detectar errores y solucionarlos más rápidamente. Estas actividades evitan cortes, interrupciones importantes y superan Latencia de conexion.

7. ¿Cuáles son las características principales de los END?

Proporcionan potentes capacidades para mejorar el rendimiento de la red y la infraestructura de TI mediante el diagnóstico de cuellos de botella y errores relacionados con dispositivos, aplicaciones, redes y servicios. También protegen la red de violaciones de seguridad.

Las herramientas de diagnóstico de red incluyen rastreadores de paquetes, herramientas de mapeo, paneles de control basados en el rendimiento y gráficos de visualización con información en tiempo real y datos históricos. También incluyen alertas inteligentes especiales para monitorear el estado de los dispositivos de red, problemas de rendimiento y picos en la actividad de tráfico sospechoso.

A continuación tenemos algunas de las mejores herramientas de diagnóstico de red:



1)PRTG Paessler

Paessler de PRTG: El ***software de diagnóstico*** y monitoreo de redes es confiable y ampliamente utilizado y tiene más de 300 mil instalaciones en todo el mundo.

Supervisa la infraestructura de TI las XNUMX horas del día y utiliza sensores preconfigurados para detectar rápidamente cargas de red y errores antes de que surjan problemas.

Esta herramienta monitorea y asegura que el sistema, los dispositivos de red, el ancho de banda de la red y el consumo de recursos estén funcionando sin problemas y le notifica con anticipación si se excede el umbral.

Características

- API dinámica para crear alertas personalizadas, generar notificaciones para enviar sistemas externos y solicitudes HTTP.
- Tecnología de flujo para monitorear el ancho de banda y otros detalles del tráfico.
- Sensor de rastreo de paquetes para indicar problemas de conectividad de red.
- Proporciona datos históricos que ayudan a aislar rápidamente las posibles causas de errores.
- Mecanismo de notificación personalizado para recibir notificaciones cuando se superan ciertos límites
- Informes personalizados

2) ManageEngine Opmanager

Administrador de operaciones de ManageEngine es una de las ***herramientas de diagnóstico*** y monitoreo de red asequibles y fáciles de usar. Es útil vigilar de cerca cualquier dispositivo que tenga una dirección IP.

Supervisa todo lo que forma parte de la infraestructura o red de TI, como enrutadores, conmutadores, dispositivos de seguridad, equilibrio de carga, configuraciones inalámbricas, servidores, entornos virtuales, dispositivos de impresión, cajas SAN y más.

Su vigilancia constante en la red ayuda a tener un control completo de la red y proporciona una visibilidad detallada. Si se produce un error, dificultad o bloqueo, el administrador de la red puede encontrar fácilmente la causa raíz del problema y solucionarlo rápidamente, evitando una interrupción importante.

Principales características

- Su función de monitoreo en tiempo real permite a los administradores observar de cerca la pérdida de paquetes de red, la lentitud en la red, problemas de rendimiento como errores y cuellos de botella, etc.
- Se pueden monitorear varias métricas de red física y virtual, como la memoria, el procesador, la utilización del disco, los hosts y las máquinas virtuales.
- Su panel de control personalizable se beneficia de ver el rendimiento de toda la red de un vistazo.
- Su aplicación móvil para Android y iPhone ayuda a monitorear toda la plataforma de red y recibir alertas y realizar una resolución de problemas básica mientras está fuera de la pantalla.

3) WhatsUp Gold

WhatsUp Gold es ***una herramienta integral de diagnóstico y monitoreo de redes para entornos virtuales, inalámbricos y cableados***.

La herramienta ayuda a identificar y solucionar problemas antes de que ocurran problemas importantes o interrupciones de la red. Supervisa la red y las aplicaciones y dispositivos en la nube y en el local red.

Características

- Monitor de rendimiento de aplicaciones: monitorice Linux, servidores web y aplicaciones de Microsoft.
- Monitoreo del consumo de ancho de banda en la red
- Monitoreo de recursos basado en la nube - AWS y supervisión, asignación y alertas de recursos del entorno de Azure para hosts, invitados y clústeres.
- Detección automática de dispositivos: detecta y enumera todos los dispositivos conectados a la red. Recopila el tipo de dispositivo, la empresa, el número de serie, la versión de firmware y más.

- Alertas en tiempo real: panel de control centralizado para monitorear rápidamente las alertas cuando se exceden los umbrales y tomar medidas antes de que se notifique a los usuarios.
- Monitorear entornos virtuales como VMware y Hyper-V
- Capacidad para integrar herramientas de terceros

4) Datadog

Datadog: Las herramientas proporcionan una solución de gestión de red completa para redes medianas y grandes empresas. Es una ***herramienta integral de diagnóstico*** y análisis de red que se ocupa de la infraestructura de TI, la administración de archivos de registro, la seguridad de la red, el análisis de los patrones de tráfico de la red y más.

Con la plataforma Datadog, los administradores de red pueden ver todos los servidores, la estructura de la nube, todos los parámetros de aplicaciones y hardware, bases de datos y más en una consola central.

Características

- No solo ofrece un panel simple, sino que también proporciona una vista personalizada de alta resolución de todas las métricas y eventos en tiempo real en forma de un panel interactivo en tiempo real.
- Conveniencia para crear condiciones de activación versátiles y recibir notificaciones para sus correos electrónicos, consola slack y más.
- Busque, filtre y analice rápidamente los archivos de registro de todos sus servicios, aplicaciones y plataformas para el diagnóstico y la resolución de problemas.
- Visualice el flujo de tráfico en un entorno basado en la nube a través de hosts separados para los centros de datos.
- Varios complementos como administración de incidentes, administración de seguridad, monitoreo sintético, etc.

5) SolarWinds

Vientos solares Network Monitor está desarrollado por ingenieros de redes y sistemas que saben lo que se necesita para administrar la exigente infraestructura de TI actual.

Es una herramienta de diagnóstico de red avanzada que se utiliza para diagnosticar y solucionar rápidamente errores de red y problemas de rendimiento, que cubre todos los entornos locales, híbridos y en la nube.

La utilidad de actualización automática de mapas permite a los administradores ver métricas, diseños contextuales y gráficos de red.

Su soporte de múltiples proveedores para monitorear el rendimiento y la disponibilidad de fallas lo hace compatible con casi todos los tipos de redes y proveedores de servicios.

Características

- Reduce las interrupciones de la red: su mecanismo de alerta inteligente permite la creación de umbrales definidos por el usuario.
- Rastree y muestre automáticamente métricas de rendimiento actuales e históricas a través de gráficos y paneles personalizados para un mejor análisis y una resolución más rápida.
- La herramienta ayuda a encontrar el origen del problema analizando el paquete de software para determinar si el problema está oculto en la aplicación o en la red.
- Permite el análisis de salto a lo largo de la ruta de la red para comprender mejor los cuellos de botella, el tráfico y los detalles de configuración de dispositivos y aplicaciones.

6) Wireshark

WireShark es una galardonada herramienta gratuita de análisis de datos de paquetes de red y se utiliza para el análisis y la resolución de problemas de la red. Esta herramienta permite a los administradores de red penetrar en la red a nivel microscópico para encontrar la causa exacta de la congestión y los errores.

Está desarrollado por voluntarios y expertos en redes de todo el mundo.

Este software es estándar en muchas instituciones comerciales, sin fines de lucro, gubernamentales y educativas.

Características

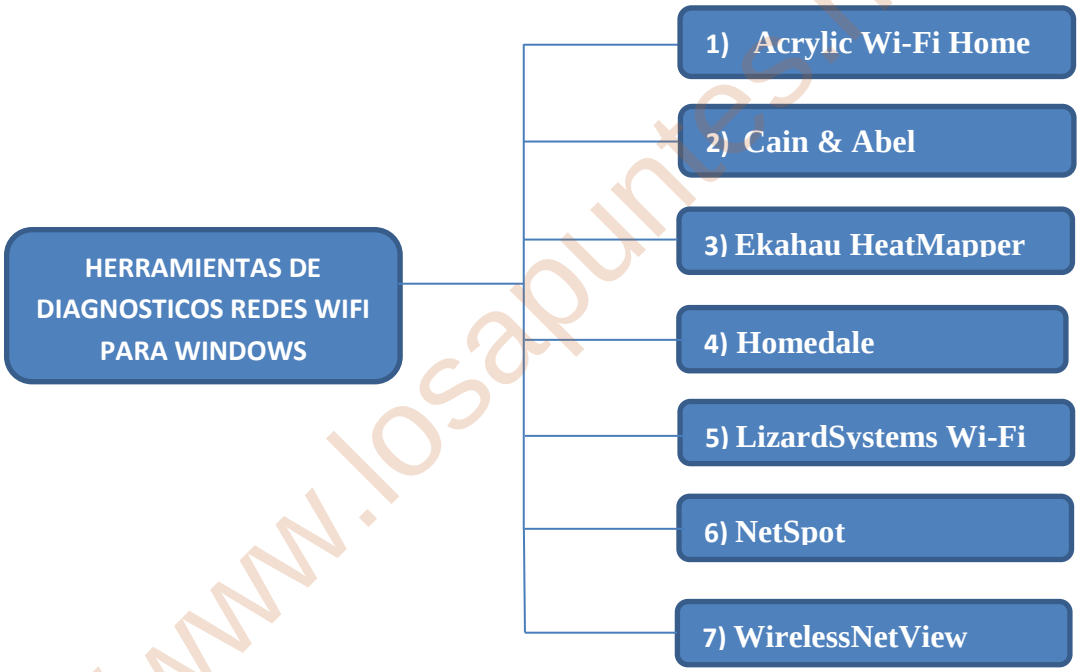
- Inspecciona cientos de protocolos mientras se agregan más cuando es necesario.
- Revisa cientos de registros y agrega más según sea necesario.
- Tiene la función de recopilar datos en vivo y extraerlos fuera de línea para su análisis.
- Es compatible con casi todos los sistemas operativos: Windows, Linux, Mac, Solaris, FreeBSD, NetBSD, etc.
- Esta herramienta está integrada con potentes filtros de visualización en esta categoría de herramientas.
- Se pueden aplicar reglas de color para un análisis rápido e intuitivo

Herramientas gratuitas para el diagnóstico de redes Wi-Fi para Windows

He aquí siete herramientas gratuitas **para Windows**, que brindan detalles básicos sobre las señales de Wi-Fi cercanas: **SSID, potencia de la señal, canales, direcciones MAC y nivel de seguridad.**

Algunas incluso pueden revelar SSID "ocultas" o indicar los niveles de ruido de su conexión inalámbrica. Uno de ellos incluye **herramientas de descifrado de contraseñas Wi-Fi**, útiles para fines educativos o para realizar pruebas de penetración.

La mayoría de estas herramientas son **versiones gratuitas de herramientas de pago** hechas por los mismos proveedores y carecen de algunas de las características incluidas en las versiones comerciales.



1)Acrylic Wi-Fi Home 3.1 (Windows)

Tarlogic Security ofrece Acrylic Wi-Fi Home , un stumbler de Wi-Fi que es una versión reducida de su versión comercial. La edición gratuita tiene una **GUI simple** pero atractiva. Siempre se podrá ver la lista de SSID y sus detalles en la parte superior de la aplicación. Muestra **valores negativos de dBm para RSSI**, puede detectar el estándar 802.11 (incluido 802.11ac), reconoce anchos de banda mayores y muestra los múltiples canales utilizados.

No revela los SSID ocultos, pero sí muestra otros detalles sobre ellos. La aplicación tiene una función de inventario en la que se puede asignar y guardar nombres de SSID y/o clientes detectados. En la parte inferior se observan las **clasificaciones de red del SSID** seleccionado, y un gráfico que muestra la **intensidad de señal de cada SSID.**

Aunque está un poco escondido, hay un modo avanzado que muestra dos gráficos adicionales, uno para las frecuencias **2.4GHz** y otro para las de **5GHz**. Da un vistazo del uso de la banda, incluida la vinculación de canales y la intensidad de la señal al mismo tiempo.

Para exportar o guardar los datos capturados, la aplicación está limitada a copiar solo una fila de datos en el portapapeles y pegar el texto sin formato en un documento de texto o en una hoja de cálculo. También hay una función para publicar una captura de pantalla en Twitter.

2) Cain & Abel (Windows)

Es una aplicación de recuperación y craqueado de contraseñas multipropósito que también cuenta con **herramientas Wi-Fi para hacer stumbling y sniffing**. Al igual que Acrylic WiFi, también tiene un monitor o modo "promiscuo" para capturar más tráfico.

Su GUI tiene un aspecto y un tacto más antiguos y simplistas. Tiene una barra de herramientas estilo antiguo en la parte superior con iconos para mostrar diferentes utilidades. La parte principal de la aplicación posee pestañas.

La pestaña Wireless es donde se encuentra el **stumbler de Wi-Fi**. Además del típico SSID e información de señal, muestra una lista y detalles de los clientes conectados. Para los SSID y los clientes, el stumbler **proporciona números de ciertos paquetes detectados**: todos los paquetes, WEP IVs únicos y solicitudes ARP.

Al igual que Acrylic WiFi, cualquier SSID oculto descubierto a partir de los paquetes se revela también en la GUI. La mayor parte de los estados y los datos capturados se pueden exportar a un archivo de texto simple.

Debido a la falta de gráficos y la incapacidad de distinguir en APs de 802.11ac y anchos de banda más grandes, Cain & Abel podría no ser una gran opción para hacer stumbling y monitorear el Wi-Fi. Pero ciertamente **sería útil para realizar pruebas de penetración.**

3) Ekahau HeatMapper (Windows)

Es una herramienta gratuita de encuesta en el sitio basada en mapas para uso doméstico, una versión reducida de su producto profesional. Muestra detalles de la red de forma similar a un stumbler de Wi-Fi, pero también genera un **mapa de calor en el que se puede visualizar los niveles de señal.**

La aplicación ofrece la opción de crear un plano o diseño del edificio que está siendo inspeccionando o un diseño de cuadrícula para tener una guía aproximada. El lado

izquierdo de la pantalla principal muestra una lista de los SSID y sus detalles, los cuales se pueden ordenar por señal, banda, SSID, dirección MAC y método de seguridad.

Incluye los detalles de la red principal, pero **carece de un indicador de los niveles de señal en dBm y valores porcentuales**. Solo muestra barras de señal en la lista y las **redes 802.11ac y 802.11n.**

Al igual que en otras herramientas, se debe hacer clic en la ubicación en el mapa mientras se camina por el edificio para poder generar el mapa de calor. Estimará automáticamente las ubicaciones de los puntos de acceso (AP) y los colocará en el mapa. Después de capturar algunos datos, al pasar el cursor sobre los iconos de los puntos de acceso, se mostrarán sus coberturas individualmente.

Al desplazarse sobre las áreas del mapa de calor, se muestra una ventana emergente con el **nivel de señal en valores negativos de dBm.** La única funcionalidad de exportación o de "guardar" de la aplicación es tomando un pantallazo simple del mapa de calor.

4) Homedale (Windows)

Homedale es un stumbler relativamente sencillo y portátil basado en Windows con una interfaz de línea de comandos opcional. Además de mostrar la red básica y los detalles de la señal, **es compatible con GPS y otras formas de geolocalización**.

Esta utilidad tiene una GUI simple que se parece más a un cuadro de diálogo de múltiples pestañas que a una aplicación completa. La primera pestaña, 'descripción general del adaptador', **muestra una lista de todos los adaptadores de red, su puerta de enlace IP y direcciones MAC.**

La pestaña de' puntos de acceso' indica muchos detalles esenciales. **No muestra el estándar 802.11 de cada SSID,** pero sí las velocidades de datos admitidas y los múltiples canales utilizados por todas las SSID con anchos de banda mayores.

Además, no revela los SSID ocultos reales, pero muestra los otros detalles de red de los SSID ocultos. Una característica es que permite guardar notas sobre los SSID de forma individual, que luego se pueden incluir en los datos exportados.

La pestaña 'gráfico de las señales de los puntos de acceso' muestra un gráfico de línea con los niveles de señal para cada SSID seleccionado. La pestaña 'uso de frecuencia' da un vistazo a las visualizaciones de banda para **la banda de 2,4 GHz** y cada subconjunto de **la banda de 5 GHz**. También muestra útilmente el uso de la banda (incluida la vinculación de canales) y la intensidad de la señal.

Para ser una aplicación gratuita, Homedale ofrece excelentes capacidades de exportación. **Es posible guardar la lista de redes como un archivo CSV**, registrar las redes de cada exploración (útil si se mueve mientras se está escaneando) y guardar una imagen de cada gráfico.

5) LizardSystems Wi-Fi Scanner (Windows)

LizardSystems ofrece una edición gratuita de su escáner de Wi-Fi para uso no comercial, que tiene las mismas características y funcionalidad que su producto pago. Además de la funcionalidad de stumbler Wi-Fi, la aplicación ofrece algunas excelentes capacidades de análisis y de reporte.

Tiene una interfaz gráfica de usuario moderna que es fácil de recorrer y entender. En la pestaña del escáner hay una lista de los SSID detectados. Junto con los detalles típicos, muestra la intensidad de la señal tanto en valores negativos de dBm como en porcentajes. Incluso muestra la cantidad de clientes conectados a cada SSID.

Al lado de la especificación de los estándares 802.11, se detallan los múltiples canales utilizados por cualquier SSID con anchos de banda mayores.

Puede usar la lista a la izquierda para filtrar los SSID que se muestran según el nivel de señal, el estándar 802.11, el método de seguridad y la banda de frecuencia. En la parte inferior de la pestaña de 'escáner', se permite alternar entre varios gráficos.

Además de la típica información sobre el nivel de las señales y los gráficos de uso de la banda, es posible visualizar **las velocidades de datos, la utilización de la banda y la cantidad de clientes**. Los detalles de la red en la parte inferior muestran detalles de la conexión actual. La pestaña 'detalles avanzados' visualiza distintos detalles como los paquetes sin procesar.

La pestaña 'conexión actual' brinda más detalles sobre la conexión inalámbrica del momento. Permite acceder y administrar la lista de perfiles de redes inalámbricas guardadas en Windows 10, lo que puede ser útil ya que Windows ya no permite el acceso nativo o la administración de esa lista.

En la pestaña de 'estadísticas inalámbricas' hay gráficos y **datos sobre diferentes tipos de paquetes de capa MAC y PHY**, útiles para realizar un análisis de red avanzado.

La función de exportación básica puede guardar la lista de redes en un archivo de texto sin formato. Además, genera un informe que enseña un resumen de los tipos de redes encontrados junto con todos los detalles de las SSID recolectadas, los comentarios que se haya agregado e imágenes de los gráficos.

6) NetSpot (Windows y Mac OS X)

Esta es la única herramienta reseñada aquí que está disponible tanto para Windows como para Mac OS X. Es una versión reducida de sus versiones pagas, Home y Professional.

En la pestaña 'descubrir' de Netspot se encuentra su stumbler Wi-Fi. Aunque tiene una GUI simple, tiene un aspecto moderno, y los detalles de red de los SSID se muestran en negrita y de forma clara. **Los niveles de señal se ven en valores negativos de dBm (nivel actual, mínimo y máximo) y en porcentajes**.

Sin embargo, no muestra ninguna red oculta en la lista de redes. Aunque hay un botón de exportación, no funciona en la edición gratuita.

Al hacer clic en el botón 'detalles' en la parte inferior de la aplicación, se muestra un gráfico de señal combinado y un gráfico de uso de la banda para cada banda, que resalta convenientemente el SSID en los gráficos en función del cual se haya seleccionado de la lista de redes.

Además, tiene una vista tabular de los detalles de la señal de cada SSID para ver los **niveles exactos de cada escaneo en la aplicación**.

La edición gratuita de NetSpot entrega un buen Wi-Fi stumbler, aunque no admite redes ocultas. La aplicación muestra características que no funcionan, solo para usuarios de paga, pero brinda una mejor idea de las características disponibles en esa versión.

7) WirelessNetView (Windows)

WirelessNetView es una utilidad freeware de NirSoft, que se ofrece para fines personales o comerciales. Se trata de un stumbler Wi-Fi basado en Windows muy simple, disponible como una aplicación instalable o portátil.

La GUI de WirelessNetView es muy simple, básicamente es solo una ventana que muestra la lista de redes. En cuanto a la intensidad de la señal, enseña los valores negativos de dBm y los porcentajes, **vislumbra los valores de la última señal recibida y el promedio a lo largo del tiempo.**

Otro detalle único que ofrece es la frecuencia en la que se ha detectado cada SSID, lo que podría ser útil en determinadas situaciones. Al hacer doble clic en una red aparece un cuadro de diálogo con todos los detalles de esa red en particular, lo cual es útil, ya que ver todos los detalles en la lista principal requiere mucho espacio en las pantallas horizontales.

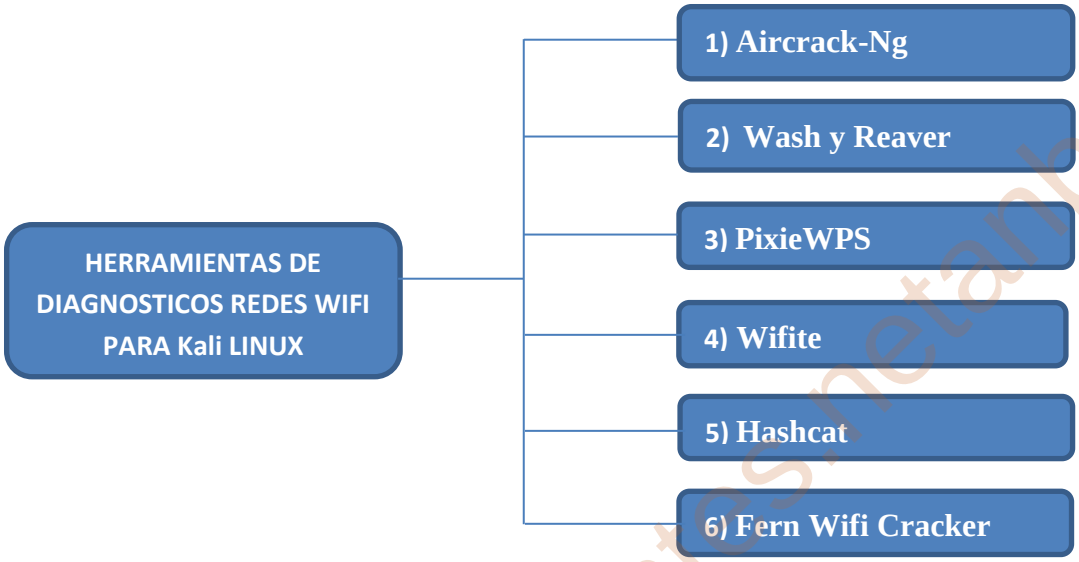
Al hacer clic con el botón derecho en una red de la lista, se pueden exportar detalles de esa red en particular o de todas las redes a un archivo de texto o HTML. El menú de la barra de herramientas de opciones dispone de algunas configuraciones y características adicionales, como **el filtrado, el formato de la dirección MAC y las preferencias de visualización.**

Ten en cuenta que **esta utilidad carece de funciones avanzadas, como gráficos, compatibilidad total con 802.11ac y el reconocimiento de todas las bandas para los puntos de acceso que utilizan anchos de banda más grandes**. Sin embargo, aún podría ser útil para hacer stumbling Wi-Fi simple, especialmente si encuentra valiosas algunas de sus características únicas.

Las utilidades de Wireless Diagnostics de Mac OS X son bastante impresionantes en comparación con las herramientas inalámbricas provistas por Microsoft en los sistemas operativos Windows. **Sin embargo, falta un gráfico que muestre el uso de la banda para cada canal Wi-Fi.**

Herramientas fundamentales para auditorías Wi-Fi instaladas en Kali Linux

Kali Linux es el sistema operativo orientado a auditorías de todo tipo más utilizado del mundo. Esta distribución incorpora por defecto una gran cantidad de herramientas para realizar auditorías Wi-Fi, que a continuación tenemos seis herramientas fundamentales para auditar toda clase de redes inalámbricas;



1)Aircrack-Ng

Aircrack-ng es la herramienta más conocida y utilizada para la realización de auditorías inalámbricas. Si alguna vez has probado la seguridad de WEP o WPA, estamos seguros que has utilizado esta herramienta. Debido a que es una de las herramientas fundamentales para auditorías, viene por defecto en la distribución de Kali Linux.

Dentro de la suite Aircrack-ng que sirve para crackear las contraseñas inalámbricas con WEP o WPA, también tenemos otras herramientas como Aireplay-ng que nos sirve para generar tráfico en un punto de acceso y hacer ataques de desautenticación, Airodump-ng que nos sirve para capturar todos los paquetes que viajan por el aire de los diferentes routers o AP inalámbricos al alcance, y también tenemos Airbase-ng que nos servirá para configurar puntos de acceso falsos y hacer que las víctimas se conecten a ellos para lanzar ataques de ingeniería social.

2) Wash y Reaver

Wash y Reaver son dos herramientas diferentes para auditar equipos con el protocolo WPS (Wi-Fi Protected Setup) activado pero forman parte del mismo «paquete». Para poder comprobar la seguridad del WPS deberemos utilizar las dos, por lo que es fundamental hablar de ambas a la vez.

Wash se encarga de determinar si el router o punto de acceso Wi-Fi tiene habilitado el WPS o no, además, nos dirá qué versión de WPS está utilizando y si el WPS está bloqueado por demasiados intentos fallidos. Después de que se descubriera la

vulnerabilidad en el protocolo WPS, los fabricantes decidieron que el WPS de autobloquee tras un cierto número de intentos.

3) PixieWPS

Esta herramienta también ataca el WPS, pero solo de ciertos routers que son vulnerables a ataques de WPS de manera offline. Actualmente todos los routers y AP nuevos no son vulnerables con este fallo, pero los que ya lo son podrás aprovecharlo para crackear dicho WPS en segundos.

4) Wifite

Wifite es una herramienta automatizada que se encarga de crackear redes con claves WEP, WPA, WPA2 e incluso WPS. Esta herramienta se encarga de capturar el handshake de WPA, desautenticar a los clientes inalámbricos, falsificar la dirección MAC y guardar la contraseña de la red. Es necesario tener aircrack-ng y reaver instalado para que todos los ataques funcionen, pero como Kali Linux los integra por defecto no deberemos preocuparnos.

5) Hashcat

Es la herramienta por excelencia para crackear contraseñas utilizando tanto la CPU como la GPU de nuestro ordenador. Esta herramienta te servirá para crackear por fuerza bruta o diccionario el handshake WPA que hayas capturado previamente con la suite Aircrack-ng. Hashcat es hoy en día la herramienta más optimizada y más rápida para realizar este tipo de tareas.

6) Fern Wifi Cracker

Esta herramienta está escrita en Python y tiene una interfaz gráfica de usuario, es capaz de atacar redes WEP y WPA así como claves WPS, también es capaz de realizar ataques sencillos de hombre en el medio.

WEBGRAFIA

1) Las posibles incidencias de pueden ocurrir en una red.

Incidencias técnicas en una red local

https://www.adrformacion.com/knowledge/administracion-de-sistemas/incidencias_tecnicas_en_una_red_local.html

10 Fallas Comunes en Redes

https://blog.zenitx.com/10-fallas-comunes-en-redes/

Resolución de Problemas de Red

https://ccnadesdecero.es/resolucion-problemas-red-sintomas-causas/

Cómo detectar problemas en la red: conoce estos sencillos pasos

https://www.testdevelocidad.es/2019/04/11/detectar-problemas-red-solucionarlos-internet/

Nueve problemas de red comunes y cómo resolverlos

https://www.computerweekly.com/es/respuesta/Nueve-problemas-de-red-communes-y-como-resolverlos

2) Programas o Software que se utiliza para monitorizar una red, ya sea en Unix o en Windows.

13 Software de monitoreo de red para pequeñas y empresas

https://geekflare.com/es/network-monitoring-software/

Las 13 mejores herramientas de monitorización gratuitas y de código abierto

https://devopslatam.com/las-13-mejores-herramientas-de-monitorizacion-gratuitas-y-de-codigo-abierto/

Comandos de red para utilizar en Windows y Linux (actualizado 2020)

https://pandorafms.com/blog/es/comandos-de-red/

Las 16 mejores herramientas de monitoreo de Redes

https://pandorafms.com/blog/es/herramientas-de-monitoreo-de-redes/

Las mejores herramientas de monitorización de software libre

https://colaboratorio.net/davidochobits/sysadmin/2017/las-mejores-herramientas-de-monitorizacion-de-software-libre/

Monitoriza la red de tu servidor Linux con estas herramientas gratis

https://www.redeszone.net/tutoriales/servidores/monitoriza-red-servidor-linux-herramientas-gratis/

Tres alternativas para monitorizar el tráfico de red

https://www.pymesyautonomos.com/tecnologia/tres-alternativas-para-monitorizar-el-trafico-de-red

3 herramientas para monitorizar la red que debes probar

https://apser.es/3-herramientas-para-monitorizar-la-red-que-debes-probar/

Mejores analizadores tráfico de red y Sniffers para Windows y Linux Gratis

https://www.solvetic.com/page/recopilaciones/s/programas/mejores-analizadores-protocolos-de-red-y-sniffers-para-windows-y-linux-gratis

Monitorización de redes - NetBrain en ZOOstock

https://www.zoostock.com/netbrain?gclid=Cj0KCQjwmuiTBhDoARIsAPiv6L8xZniU2sAHIRp4HWhjxGohwYkZvyUAth7G2hTUl1TVUpla69KCJ2YaAl6aEALw_wcB

3) Explica las herramientas de diagnóstico más utilizadas en Unix, Windows, para redes cableadas como inalámbricas.

8 herramientas gratuitas para el diagnóstico de redes Wi-Fi

https://revistaitnow.com/8-herramientas-gratuitas-para-el-diagnostico-de-redes-wi-fi/

Mapeador simultáneo de redes cableadas e inalámbricas

https://www.instaladoresdetelecomhoy.com/mapeador-simultaneo-de-redes-cableadas-e-inalambricas/

Las 10 mejores herramientas de diagnóstico de red gratuitas y de pago para organizaciones pequeñas y grandes

https://geekflare.com/es/best-network-diagnostics-tools/

Las 30 mejores herramientas de prueba de red (herramientas de diagnóstico del rendimiento de la red)

https://es.myservername.com/top-30-network-testing-tools

16 comandos de Linux para el diagnóstico de redes

https://ismarodriguez14.wordpress.com/2018/12/19/10-comandos-de-linux-para-el-diagnostico-de-redes/

Las 7 herramientas más populares de Kali Linux para hackear Wi-Fi

https://www.1000tipsinformaticos.com/2016/09/las-7-herramientas-mas-populares-de-kali-linux-para-hackear-wifi.html

Las 6 herramientas fundamentales para auditorías Wi-Fi instaladas en Kali Linux

https://www.redeszone.net/2017/04/08/las-6-herramientas-fundamentales-auditorias-wi-fi-instaladas-kali-linux/