

Unidad III: Análisis y Monitoreo

3.1 Protocolos de administración de red (SNMP)

Protocolo de administración de red simple (SNMP) es un sistema de administración basado en el protocolo de red. Se utiliza para administrar redes basadas en TCP/IP y IPX. Puede encontrar información sobre SNMP en la solicitud de Internet de comentarios (RFC 1157).

3.2 Bitácoras

Bitácoras.com es un sitio de alojamiento de blogs en español, así como una red social para blogueros.

El sistema incorpora un filtro social que recoge la información de miles de bitácoras, y la presenta de forma organizada y catalogada pudiendo ser valorada por los usuarios.

3.3 Analizadores de protocolos

Un analizador de protocolos es una herramienta que sirve para desarrollar y depurar protocolos y aplicaciones de red. Permite al ordenador capturar diversas tramas de red para analizarlas, ya sea en tiempo real o después de haberlas capturado. Por analizar se entiende que el programa puede reconocer que la trama capturada pertenece a un protocolo concreto (TCP, ICMP...) y muestra al usuario la información decodificada. De esta forma, el usuario puede ver todo aquello que en un momento concreto está circulando por la red que se está analizando. Esto último es muy importante para un programador que esté desarrollando un protocolo, o cualquier programa que transmita y reciba datos en una red, ya que le permite comprobar lo que realmente hace el programa. Además de para los programadores, estos analizadores son muy útiles a todos aquellos que quieren experimentar o comprobar cómo funcionan ciertos protocolos de red, si bien su estudio puede resultar poco ameno, sobre todo si se limita a la estructura y funcionalidad de las unidades de datos que intercambian. También,

gracias a estos analizadores, se puede ver la relación que hay entre diferentes protocolos, para así, comprender mejor su funcionamiento.

3.4 Planificadores

El análisis del tráfico de red se basa habitualmente en la utilización de sondas de red, funcionando en modo promiscuo. Las sondas capturan el tráfico a analizar y constituyen la plataforma en la que se ejecutarán, de forma continua, aplicaciones propietarias o de dominio público, con las que se podrá determinar el tipo de información que circula por la red y el impacto que pudiera llegar a tener sobre la misma. El análisis de tráfico permite determinar las capacidades y métricas bajo las cuales se está comportando la red, y evitar tener problemas de desempeño. Por ejemplo podríamos determinar la existencia de virus o el uso excesivo de aplicaciones p2p que comúnmente degradan las prestaciones de la red, sobre todo si hablamos de los enlaces principales que dan acceso a Internet.

3.5 Análisis de desempeño de la red: Tráfico y Servicios

Las tecnologías de transmisión de datos a través de redes de computadores son el eje central del funcionamiento de un entorno informático que presta servicios de tipo cliente/servidor. Un excelente desempeño de la red trae como consecuencia un aumento de la productividad informática. El ingreso de nuevos equipos a la red, la existencia de protocolos no necesarios, la mala configuración de equipos activos de red o las fallas presentadas en el sistema de cableado pueden causar degradación del desempeño de la red. Por medio de pruebas, captura de paquetes, análisis de flujo de información y verificación de la configuración de equipos activos (switch, routers), se puede mejorar el desempeño de la red.