CAPÍTULO I. INTRODUCCIÓN

1.1 Estado del arte del monitoreo de redes de computadoras.

La palabra monitoreo no tiene una definición exacta, pero en el contexto computacional ha adquirido un auge muy grande, de manera más específica en el área de redes y de seguridad. Se ha discutido mucho sobre la definición de la palabra monitoreo se han hecho estudios sobre la mejor definición y se enfocará en uno muy particular que es "una función que busca conocer cómo se están realizando las tareas definidas en el plan operativo y de presupuesto" [16].

Aunque la definición anterior, no aplica exactamente en el área estudiada, nos proporciona un panorama en donde se puede extender más en una definición concreta para nuestra investigación.

En el área tecnológica el concepto de monitoreo debe tener un enfoque más práctico, en materia de redes, por ejemplo, todas las acciones que se realizan son activas y se necesita tener constante acción con el equipo involucrado, conexiones y es el caso de este tema a desarrollar, supervisar todas las funciones que implica el trabajo de una red de computadoras. El monitoreo se encuentra muy ligado con el concepto de Inteligencia Competitiva la cual se define como: "conocimiento generado a partir del análisis resultante de la integración de información sobre el entorno de la organización, que está disponible lícitamente" [17].

En base a este conocimiento generado, se pueden realizar acciones específicas en el caso de que una infraestructura de redes pueda tener algún tipo de problema, se puede que esta sería la diferencia entre el simple análisis de datos y monitorear una red. En caso del monitoreo además de realizar un análisis detallado acerca de las acciones que se suceden en la red, también se realizan las acciones de supervisar y reaccionar ante algún imprevisto.

Estos imprevistos se pueden traducir en eventos como es el caso de "problemas de ruido en la línea de transmisión y que crean situaciones que no existen como tales

como direcciones de computadoras que no pertenecen a ninguno de los nodos, errores en la información, por mencionar algunos” [10].

A grandes rasgos lo que se pretende en el proyecto de tesis es “una verificación sobre la información contenida en un paquete que viaja a lo largo de toda la red, además de los protocolos manejados en la red, si esta información no es válida por alguna razón, se declara inválido el paquete escribiendo una bandera de error” [10].

Lo que ocurre en todo caso es que si esto sucede con cada una de las computadoras conectadas a la red que se encuentra bajo análisis “se llevará cuenta de los errores que están ocurriendo en la red, de tal forma que si una computadora se da cuenta de que el número de errores excedió a la cuenta permitida, le informa a la computadora que está "monitoreando" a la red, a fin de que pueda declararse una condición de error y mostrarla en el servidor de toda la red” [10].

La estructura general para el monitoreo se muestra a continuación:

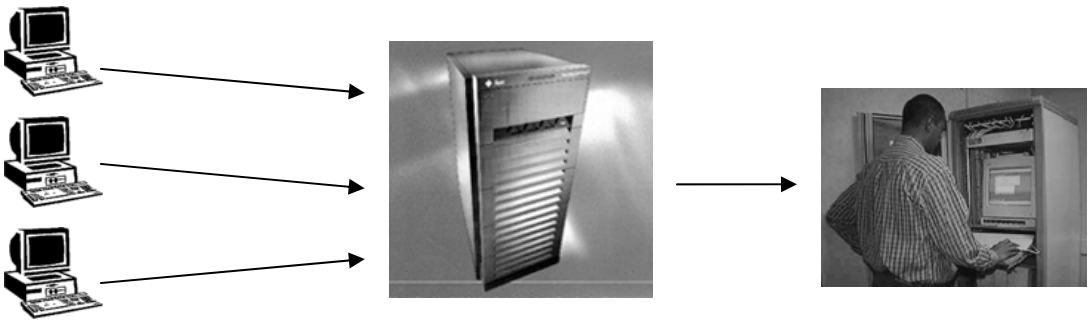

Figura 1.1 Estructura general para el monitoreo de redes LAN.

En esta estructura se tienen limitantes y funciones específicas importantes las cuales se muestran más adelante. Otro aspecto importante para resaltar en la definición de monitoreo es que al momento de mostrar el error en el servidor encargado de monitorear la red, el administrador deberá tener una reacción a este acontecimiento, el cual es dar seguimiento al error y restaurar la infraestructura de la red para su correcto funcionamiento, es decir tener una respuesta a los eventos inesperados del sistema.

Vistos todos los aspectos anteriormente mencionados se puede dar una definición de monitoreo en el área de redes y es: “Análisis detallado que surge a partir del estudio sobre la red supervisada y que nos da un conocimiento de su funcionamiento y en caso de tener algún error dar acción inmediata a su reestablecimiento”.

La situación actual en el tema de monitoreo de redes no se encuentra establecida del todo, ya que existen pocas herramientas que le dan seguimiento al error a la red analizada, existen algunos productos como son: Solarwinds, ActiveXperts, AdvenNet y eEye todas de GIA Software las cuales en conjunto son herramientas de alto nivel que sirven para la administración, monitoreo y corrección de errores en la red. La desventaja es que son herramientas de alto nivel, la cual tienen un costo bastante elevado y que sólo ofrecen soluciones de manera local, es decir, estando en un servidor en el mismo lugar físico de la red supervisada.

La aportación en este proyecto de tesis será una herramienta de menor costo, fácil de usar y que el administrador lo utilice de manera remota, todos estos detalles del proyecto se mencionarán más adelante en el apartado de objetivo general y objetivos específicos.

En esta parte se puede concluir que el tema de monitoreo de redes es apenas un desarrollo que no se ha explotado del todo y que puede tener muchas variantes, para cuestiones de nuestro proyecto de monitoreo de redes se realizará mediante una aplicación Web de manera remota.

1.2 Objetivo general.

Establecer la interfaz para el sistema de monitoreo de redes de datos mediante una aplicación Web para la detección de problemas en la red y así el administrador pueda tener un diagnóstico de estado de la infraestructura y el funcionamiento de la red y en todo caso dar una solución mediante sus conocimientos de la red constituida.

El objetivo del proyecto es proporcionar una interfaz para el monitoreo de redes vía web, en el cual el administrador de ésta tendrá la posibilidad de conocer el estado de la red en forma remota y de la misma forma poder detectar posibles problemas en la comunicación, para que el usuario o administrador tenga la posibilidad de conocer y dar acción de manera inmediata al reestablecimiento de la comunicación entre los equipos involucrados.

1.3 Objetivos específicos.

- Mediante una interfaz desarrollada, monitorear el tráfico de la red y detectar los problemas que puedan presentarse entre dos o más equipos conectados e involucrados en la misma red mediante una aplicación Web y que se pueda tener una acción inmediata en el reestablecimiento de la misma red.

- Esto, con la ayuda de herramientas ya existentes, tal es el caso de un programa o dispositivo que monitorea el viaje de los datos a través de una red llamado sniffer[3] y así realizar estudios para saber la confiabilidad de nuestra aplicación y así ofrecer una solución estable a las necesidades de quienes administren una red de computadoras y así obtener una mejor eficiencia.

1.4 Justificación.

En la actualidad, a pesar de que la comunicación entre equipos, puede ser muy confiable si no se tiene una correcta administración de la misma, los errores pueden aparecer de manera continua y los administradores a pesar de tener un diseño detallado de la red tardan en detectar el posible fallo mediante una serie de pasos.

Por eso, la necesidad de la comunicación efectiva y confiable es muy importante, para esto existen herramientas, como las Web, que pueden ser utilizados por los administradores para realizar diagnósticos, en cualquier tiempo y lugar. Esta

herramienta puede ser aplicada al aspecto comercial y que a la vez, no se necesite una licencia demasiado cara y difícil de usar para que se pueda conocer el estado de una red.

La importancia de revisar el tráfico sobre una red, su seguridad y mantenerla funcionando de manera eficaz, es algo que los administradores tienen como objetivos principales, además que es vital que los sistemas se encuentren funcionando todo el tiempo, para el servicio al usuario final.

Se necesitan herramientas eficientes para la detección de posibles errores y que puedan incrementar la productividad del sistema administrado y aquí la importancia de realizar un "análisis y monitoreo de redes que se ha convertido en una labor cada vez mas importante y de carácter pro-activo para evitar problemas" [6].

El monitoreo del estado de una red es un tema de actualidad en el cual todas las empresas o administradores de redes están involucrados de alguna manera, ya que en materia de seguridad y de efectividad en transmisión de datos siempre hay obstáculos que impiden el buen desempeño de la red por lo cual:

> Monitorear el estado de la red es una actividad que no puede considerarse secundaria. Las herramientas de monitoreo permiten saber con anticipación sobre posibles caídas del sistema, así como tiempos de respuesta, fluctuación en la velocidad de transmisión de datos y un sinfín de elementos que resultan oro molido para el administrador de la red [12].

Mencionado todo lo anterior se debe tener un enfoque en la creación de "programas para el control remoto de computadoras o sistemas de monitoreo, los cuales te permiten controlar una máquina mediante un enlace a través de un medio de comunicación, ya sea en una Red de Área Local o en la más grande red existente que es Internet" [8].

Las empresas de gran talla desarrollan sus propias herramientas para la detección de problemas en la red, además ninguna empresa ya sea pequeña o grande, está exenta de comprar alguno de esos productos, además que depende mucho del tipo

de uso que la empresa tenga para su red y su finalidad que es lo más importante es que desempeñe el trabajo para el cual fue adquirido.

Estos softwares, tienen un costo bastante alto, además que no son comercializables, ese es el gran problema que se tiene en el contexto del monitoreo de redes, por lo cual no se tiene un desarrrollo pleno en esta área, viendo estos puntos anteriormente mencionados, se necesita:

1. Una herramienta que se pueda comercializar para que cualquier administrador que lo necesite pueda realizar el manejo de su red en cualquier tiempo y lugar.

2. Y la posibilidad que la misma pueda tener una gran demanda comercial y la cual puede significar una entrada económica importante, para la empresa o entidad que lo desarrolle, por su significado y propósitos antes mencionados.

El administrador necesita una herramienta que le dé seguridad en el funcionamiento de su red y así evitar grandes pérdidas tanto de información como de dinero.

Por lo tanto se planea desarrollar una aplicación que no sea de uso tan avanzado y que requiera la combinación de hardware y software y que permite que el usuario tenga "accesibilidad desde cualquier navegador y que prometa aumentar la productividad y precisión en el mantenimiento de redes por medio del monitoreo y la grabación constante del estado de la conexión" [12], por lo que le ofrecerá al administrador mayor conocimiento acerca de su red de manera remota.

El tema "Interfaz para el monitoreo de redes de comunicaciones mediante una aplicación Web" se enfoca en el tipo de herramienta antes mencionada ya que da una solución de manejo mucho más simple para el administrador.

1.5 Limitaciones.

- Desarrollar y establecer una herramienta que sea confiable 100%.

- La infraestructura de una red puede variar de manera considerable, por eso, se trabajará con una red de computadoras no muy amplia para el inicio del desarrollo de la aplicación, después conforme la aplicación se amplíe empezará a aumentar el número de equipos y así sacar el mayor provecho posible de la herramienta.
- La realización del proyecto también se limitará por las características y el tipo de equipo con el cual se cuente.
- La red a monitorear cuenta con un número limitado de usuarios y con los siguientes servicios:
    - Impresión
    - Internet
    - Carpetas compartidas

1.6 Desarrollo.

En primer lugar, se realiza la investigación sobre las herramientas necesarias para el monitoreo de redes y el manejo de su interfaz, en este caso se lleva a cabo la búsqueda de un sniffer en el cual se encuentra soportada nuestra herramienta, ya que los datos que deduce, se pueden utilizar para los objetivos establecidos, mencionados con anterioridad y se instala en la computadora encargada del monitoreo.

Después se procede a hacer un estudio sobre el sniffer, en este estudio abarca el familiarizarse con la herramienta, aprender a manejarla, los fines para los que se utiliza y la relación que puede tener para con otras herramientas, como los servicios Web.

A continuación se hace la construcción del ambiente Web, con sus análisis correspondientes y que tenga las utilidades que el administrador necesita, después se pasará a la parte en donde se conectará nuestro sniffer con el mismo ambiente Web y atrapar las variables que contienen los datos que nos interesan y presentarlas de una manera fácil.

De manera simultánea, se redacta la parte correspondiente del desarrollo y ya con nuestra aplicación en funciones, se procede a realizar las pruebas necesarias, la

prueba se realiza con un grupo de computadoras las cuales se les asignará una dirección IP (Internet Protocol) y un número de puerto (Port), realizado lo anterior se pueden identificar los datos que cada una de las máquinas envíen y si existe un posible error.

1.7 Hardware y software a utilizar.

1.7.1 Sniffer.

Un sniffer es “un programa o dispositivo que se encarga de monitorear el viaje de los datos a través de una red” [3], de esta manera se pueden “observar los datos que, las computadoras involucradas en la red, se envían unas con otras” [1], con la finalidad de que el administrador o usuario actué de manera inmediata por algún imprevisto generado por el mismo estado de la red.

Existen diferentes tipos de sniffers entre los cuales se pueden encontrar dos tipos principales: “los sniffers comerciales y los sniffers *underground*”, [13], subterráneos o ilegales por llamarlos de otro modo. Los sniffers de uso comercial se utilizan para el monitorear y “mantener redes”[13], mientras que los sniffers de uso *underground* son los que “se utilizan para asaltar los ordenadores de una red” [13],

Para el proyecto se enfocará al *sniffer* tipo comercial, ya que además de tener fines lícitos, servirá para hacer de la red, lo más funcional posible.

La manera en la que funciona generalmente es en la cual “Un ruteador lee cada paquete de datos que pasa por él y determina de manera intencional el destino del paquete dentro de la red. Un ruteador y un sniffer, pueden leer los datos dentro del paquete así como la dirección de destino.”[11].

1.7.1.1 Etherpeek.

Es un sniffer desarrollado por la empresa AG Group el cual está basado en el sistema operativo Windows 2000 (existen versiones posteriores pero por limitaciones en la adquisición de la licencia se tiene el mencionado) y es “un software basado en redes de computadoras y una herramienta para el análisis de protocolo de redes [15].

La utilidad más importante que tiene es que “ayuda a los administradores de redes a configurar, mantener y resolver problemas en las redes Ethernet monitoreando y capturando el tráfico en la red” [15].

Los datos que captura Etherpeek son variados, con la ventaja de poder analizar características entre las cuales se encuentran: el tipo de paquetes que se envían con su respectivo tamaño, el tráfico de paquetes (paquetes enviados, recibidos y perdidos).

Además de captar los protocolos de comunicación utilizados por las distintas computadoras en la red, dirección origen y destino por donde viajan los datos en la red, además de proporcionarnos datos y gráficas que nos indican cuál es la productividad y la eficiencia en nuestra Red de Área Local (LAN).

Para efectos del proyecto de tesis, todos estos datos antes mencionados son capturados por la aplicación Web cada cierto lapso de tiempo, para tener una supervisión constante y de esta manera si se tiene algún error dar acción inmediata al reestablecimiento de la comunicación.

Además se utilizan herramientas que complementan a Etherpeek en su funcionamiento y que son de la misma empresa AG Group en su división de grupo llamado Wildpackets, entre las cuales se pueden observar a: iNetTools, NetDoppler, NetSense y RMONGrabber.

- iNetTools.- Herramienta que sirve para saber si existe comunicación entre las computadoras involucradas en la red.
- NetDoppler.- herramienta que realiza un rastreo de cada una de las máquinas de la misma red y que nos proporciona datos y gráficas para establecer la utilización del ancho de banda y el porcentaje de efectividad en el traspaso de los datos de las mismas, además de realizar un árbol con nodos IP, esto quiere decir que se construye un árbol con la dirección IP de todos los nodos involucrados en la red.
- NetSense.- aplicación la cual hace un análisis de protocolos de la red y que cargando un archivo especializado se despliega un estudio de alto nivel y en

diferentes formatos sobre el funcionamiento de la red que se encuentra supervisando.

- RMONGrabber.- aplicación de alto nivel que resuelve los problemas detectados en l red.

1.7.2 Otras herramientas.

Para el trabajo también se requieren herramientas como el sistema operativo Windows 2000, máquinas que tengan más de 256 MB en RAM de velocidad, adaptadores de red PCI Fast Ethernet conectados de la PC a la red, también se necesitará hardware para la conexión entre máquinas, es el caso de los accesorios conocidos como hubs y switches.