UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERIA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERIA ELECTRONICA Y COMUNICACIONES

Seminario de Graduación "Proyectos de Conectividad y Redes de Comunicación, Administración de Redes y Servicios, Seguridad Industrial, Normativas de Calidad y Automatización Robótica (Mecatrónica)"

TEMA

SISTEMA DE ANÁLISIS Y MONITOREO PARA LA RED INALÁMBRICA DE LA EMPRESA "DISTRY-TEX"

Proyecto de Investigación, presentado previo a la obtención del título de Ingeniero Electrónico y Comunicaciones

AUTOR (A): Segundo Danilo Barrera Morales

AMBATO – ECUADOR

Septiembre - 2009

APROBACIÓN DEL TUTOR

En mi calidad de tutor del trabajo de investigación sobre el tema: **Sistema de Análisis y Monitoreo para la Red Inalámbrica de la empresa DISTRY-TEX** , de Segundo Danilo Barrera Morales, estudiante de la Carrera de Ingeniería en Electrónica y Comunicaciones, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el Art. 45 del Capítulo III Seminarios, del Reglamento de Graduación de Pregrado de la Universidad Técnica de Ambato.

Ambato Septiembre, 2009

EL TUTOR

Ing. Iván Aldás

AUTORÍA

El presente trabajo de investigación titulado: Sistema de Análisis y Monitoreo para la Red Inalámbrica de la empresa DISTRY-TEX. Es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato Septiembre, 2009

Danilo Barrera
180366218-6

DEDICATORIA:

Con el alma rebosante de gratitud y cariño, dedico el presente trabajo a mi Madre y Hermanos quienes con incomparables sacrificios me han ayudado y alentado en cada momento de mi vida estudiantil, aunque haya tenido caídas y tropiezos, gracias por atreverse a confiar en mí, es obvio que sin ustedes este sueño nunca hubiera podido ser completado.

DANILO BARRERA

AGRADECIMIENTO:

Quiero expresar un sincero y profundo agradecimiento a todas las personas que me han apoyado en el transcurso de mi carrera, así como también a la Universidad Técnica de Ambato, a la Facultad de Ingeniería en Sistemas Electrónica e Industrial por permitirme culminar con éxito esta última etapa de mi vida universitaria.

A cada uno de los profesores que me apoyaron y compartieron todo su conocimiento, pero de una manera especial al Ing. Iván Aldás, tutor del presente trabajo por su valioso tiempo y paciencia durante todo el proceso de elaboración. Y por último a mis amigos y compañeros de carrera que siempre he podido contar con ellos en todo momento.

DANILO BARRERA

INDICE

A. PAGINAS PRELIMINARES

B. TEXTO: INTRODUCCION

Capítulo I

RESUMEN EJECUTIVO

Este presente proyecto está desarrollado, y se divide en seis capítulos que se detallan a continuación:

El Capitulo I, enfoca el **PROBLEMA.** Este apartado se plantea el Tema de Investigación, el planteamiento del problema, la respectiva justificación y por último se presenta los Objetivos tonto General como Específicos.

El Capitulo II, trata sobre el **MARCO TEORICO.** Se desglosa los Antecedentes Investigativos, Fundamentación Legal y Categorías Fundamentales, en este apartado, se describe la investigación teórica que nos servirán en los capítulos siguientes del cual se tomara en cuenta para el desarrollo del sistema de Análisis y Monitoreo se redes inalámbricas; también en este capítulo, se describe la Hipótesis con sus respectivas variables.

El Capítulo III, da a conocer la **METODOLOGIA** con el cual se enfoca nuestro tema, para poder tener una modalidad básica de investigación; así poder definir el modelo de investigación conjuntamente con la población y muestra, también se realiza la correspondiente Operacionalización de las Variables, para así recolectarla información necesaria para realizar un buen procesamiento y análisis del sistema.

El Capítulo IV, se presenta las **CONCLUSIONES Y RECOMENDACIONES,** tomadas de las experiencias obtenidas durante el estudio del sistema. Así demostrando el cumplimiento tanto de la Hipótesis como los Objetivos mencionados anteriormente.

El Capitulo V, se describe los antecedentes de la Propuesta, y por ultimo Anexos y la correspondiente Bibliografía.

INTRODUCCION

Las redes inalámbricas es una de las principales actualizaciones de la tecnología.
La red es un conjunto de dispositivos electrónicos inteligentes interconectados entre sí, esto quiere decir, maquinas que procesen y/o manipulen información.
Las redes inalámbricas de área local o WLAN (Wireless Local Area Networks) están transformando la forma de comunicarnos. No solo son más flexibles y escalables que las redes de área local cableadas, también nos permiten armar redes en lugares en donde el cableado es un limitante.
Además de sus diversas ventajas, las redes WLAN tienen un gran inconveniente, su vulnerabilidad a ataques de seguridad.
El objetivo de este proyecto es crear un procedimiento para evaluar el problema de inseguridad de la red inalámbrica para de la empresa DISTRY-TEX, estableciendo el desarrollo de un sistema de Análisis y Monitoreo poder saber lo que está pasando dentro de esta en tiempo real.
También presenta sugerencias de posibles implementaciones que refuerzan la seguridad de la red logrando erradicar sus inseguridades.
En la actualidad, los sistemas de control y monitoreo se han convertido en factor común para la seguridad.
Son muchos los motivos para preocuparnos por la seguridad de la red inalámbrica de la empresa DISTRY-TEX. Por ejemplo, queremos evitar compartir nuestro ancho de banda públicamente y también evitar la pérdida de información. Como todos sabemos que las redes inalámbricas utilizan un medio inseguro para su comunicación y esto tiene sus repercusiones en la seguridad. También debemos tener en cuenta que las tramas circulan de forma pública y en consecuencia cualquiera que estuviera en el espacio cubierto por la red, y con unos medios simples, podría capturar las tramas y ver el tráfico de la red.

Para resolver los problemas de seguridad que presenta esta red inalámbrica tendremos que poder, por un lado, garantizar el acceso mediante algún tipo de credencial a la red y por otro garantizar la privacidad de las comunicaciones aunque se hagan a través de un medio inseguro.

El monitoreo de la red inalámbrica comienza seleccionando la interfaz de red que desea monitorear. La selección de la interfaz correcta de red es fundamental para lograr los resultados de monitoreo deseados. Para realizar el proceso de análisis y monitoreo de la red inalámbrica de la empresa DISTRY-TEX utilizaremos un software simple y fácil de usar como es Observer que es un analizador de protocolos. Mediante este software podremos visualizar el Control de desempeño, Control de Múltiples Instalaciones, Control de Solución de Problemas, Control de Información de la red inalámbrica de la empresa entre otras.

También en este proyecto se realizara una breve descripción de los métodos de seguridad existentes para las redes inalámbricas y sus respectivas ventajas.

TEMA:

Sistema de análisis y monitoreo para Redes Inalámbricas de la empresa "DISTRY-TEX"

CAPITULO I

EL PROBLEMA

1. PLANTEAMIENTO DEL PROBLEMA

1.1 CONTEXTUALIZACION

En la actualidad a nivel mundial las empresas están utilizando cada vez más las redes inalámbricas, las cuales permiten la comunicación entre diversos equipos, sin utilizar un medio de propagación físico.

Pero no todo podía ser perfecto, una de las preocupaciones en cuanto a la utilización de estas redes recae en la seguridad de la información que viaja por la red y de los equipos que forman parte de ella, y que cualquier persona con el equipo adecuado dentro del área de alcance de la red puede acceder a ella. Por este motivo el uso de sistemas de análisis y monitoreo es algo más que opcional para saber cuando una persona no autorizada ha penetrado nuestra red inalámbrica.

En el Ecuador la implementación de redes inalámbricas se está aplicando en la mayoría de las grandes empresas, las mismas que brindan velocidad de transmisión y bajo costo en su implementación, dando soluciones a varios

inconvenientes, pero la mayor parte de estas poseen deficiencias en la seguridad y monitoreo.

En la empresa “DISTRY-TEX” ubicada en la ciudad de Pelileo, tiene implementada una red inalámbrica y esta no tiene un sistema de seguridad es por eso que se requiere de un sistema de análisis y monitoreo, para poder evitar que personas no autorizadas accedan a la información privada esta red.

1.2 ANÁLISIS CRÍTICO.

Los problemas se iniciaron cuando personas ajenas a esta empresa accedían a la red inalámbrica para obtener información de ella o para beneficiarse de los servicios que esta dispone.

La pérdida de información se da continuamente siendo otro problema en la empresa “DISTRY-TEX”, la cual tiene implementada una red inalámbrica y no cuenta con un sistema de seguridad.

Otro de los problemas que afectan a la red inalámbrica en es la lentitud en la entrega de servicios, debido a que personas no autorizadas están utilizando para aplicaciones desconocidas o mal intencionadas, con el desarrollo de un sistema de análisis y monitoreo podríamos detectar el origen que causa los problemas y lograr tener un mejor servicio.

1.3 PROGNOSIS

De continuar los problemas de inseguridad en las red inalámbrica de la empresa“DISTRY-TEX” por la falta de monitoreo estos seguirán creciendo y las pérdidas de información serán más continuas.

Al analizar y monitorear la red inalámbrica se tendrá un panorama claro de lo que está pasando dentro de ella.

1.4 FORMULACIÓN DEL PROBLEMA

¿Cómo desarrollar un sistema de análisis y monitoreo para redes inalámbricas en la empresa “DISTRY-TEX”?

1.4.1 PREGUNTAS DIRECTRICES

1.4.1.1 ¿Cuál es la infraestructura de la red de la empresa?

1.4.1.2 ¿Con que tipos de equipos cuenta la empresa?

1.4.1.2 ¿Qué tipos de sistemas de análisis y monitoreo serian más apropiadas para este desarrollo?

1.4.1.3 ¿Qué pasos se seguiría para el desarrollo de este sistema?

1.4.1.4 ¿Qué beneficios presenta el análisis y monitoreo de la red inalámbrica en la empresa?

1.4.2 DELIMITACIÓN DEL PROBLEMA

El presente proyecto de “Sistemas de análisis y monitoreo para Redes Inalámbricas de la empresa “DISTRY-TEX” tendrá una duración de cinco meses, desde el diez de noviembre del 2008 al treinta de marzo del 2009.

1.5 JUSTIFICACIÓN

En este mundo que va evolucionando a la par con la tecnología y donde la demanda de redes inalámbricas es mas continuo, es necesario tener un Sistema de análisis y monitoreo para la seguridad de Redes Inalámbricas, y así poder brindar mayor confiabilidad a los usuarios de estas.

El desarrollo de este proyecto será de vital importancia ya que ayudara a las empresas pequeñas que disponen de redes inalámbricas a mantener la seguridad en su red, para evitar que personas ajenas a esta puedan acceder sin permisos.

Este proyecto de desarrollo de un sistema de análisis y monitoreo de una red inalámbrica aportará con una buena forma de comunicación interna y segura en las empresa.

1.6 OBJETIVOS DE LA INVESTIGACIÓN

1.6.1 OBJETIVO GENERAL

Desarrollo de un sistema de análisis y monitoreo para la Red Inalámbrica de la empresa “DISTRY-TEX”

1.6.2 OBJETIVOS ESPECÍFICOS

1.6.2.1. Analizar la infraestructura de redes existente en la empresa y los diferentes tipos de equipos que dispone.

1.6.2.2. Determinar los sistemas apropiados para el análisis y monitoreo de la red inalámbrica.

1.5.2.3. Explicar cómo funcionan los Protocolos y sistemas de seguridad en las red inalámbrica y como se pueden usar para monitorear la misma.

1.6.2.4. Determinar los pasos apropiados para el desarrollo de este sistema.

1.5.2.5. Establecer los beneficios que presenta el análisis y monitoreo de las redes inalámbricas.

CAPITULO II

MARCO TEORICO

2.1 ANTECEDENTES INVESTIGATIVOS

Al revisar los archivos en la biblioteca de la Facultad de Ingeniería en Sistemas Electrónica e Industrial se ha encontrado los siguientes trabajos investigativos que está relacionado con las redes inalámbricas, las cuales fueron desarrolladas por Alex Salazar con el título “Diseño de una red comunitaria basada en tecnologías WLAN para la facultad de Ingeniería en Sistemas Electrónica e Industrial” en el periodo Abril Septiembre del 2005, también un perfil presentado por Karina Zagal en el periodo Septiembre-febrero del 2007-2008 la cual lleva por título " Sistema de monitoreo de la Red Inalámbrica en la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato", cuyas conclusiones se refieren a la seguridad que se puede obtener con el monitoreo de las redes inalámbricas.

2.2 FUNDAMENTACION

2.2.1 FUNDAMENTACIÓN LEGAL

La fundamentación legal de éste proyecto se basa el acceso a las redes y recursos asociados e interconexión Artículo # 11.

Y también en las leyes y reglamentos del espectro de frecuencia a nivel mundial. Leyes que rigen las Telecomunicaciones en el Ecuador, Ley No. 184

2.3CATEGORÍAS FUNDAMENTALES

RED DE COMPUTADORES

¿Qué es una red**?**

Una red de computadoras (también llamada red de ordenadores o red informática) es un conjunto de equipos (computadoras y/o dispositivos) conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información (archivos), recursos (CD-ROM, impresoras, etc.) y servicios (acceso a internet, e-mail, chat, juegos), etc.

CLASIFICACIÓN DE REDES

Red de área personal (*PAN*)

Red de área personal o Personal area network es una red de computadoras para la comunicación entre distintos dispositivos (tanto computadoras, puntos de acceso a internet, teléfonos celulares, PDA, dispositivos de audio, impresoras) cercanos al punto de acceso. Estas redes normalmente son de unos pocos metros y para uso personal.

Red de área local (*LAN*)

Son redes privadas localizadas en un edificio o campus. Su extensión es de algunos kilómetros. Muy usadas para la interconexión de computadores personales y estaciones de trabajo. Se caracterizan por: tamaño restringido, tecnología de transmisión (por lo general broadcast), alta velocidad y topología.

Son redes con velocidades entre 10 y 100 Mbps, tiene baja latencia y baja tasa de errores.

Red de área de campus (*CAN*)

Red del área del campus (CAN): Se deriva a una red que conecta dos o más LANs los cuales deben estar conectados en un área geográfica específica tal como un campus de universidad, un complejo industrial o una base militar.

Red de área metropolitana (*MAN*)

Las redes de área metropolitana (MAN, Metropolitan Area Network) Conectan segmentos de red local de una área específica, como un campus, un polígono industrial o una ciudad, se basa en la conexión de redes locales que expande el servicio en un área metropolitana, el soporte de la conexión de las redes se basa en el servicio de líneas dedicadas o discadas de las compañías telefónicas, en la actualidad crece el interés en redes inalámbricas y redes interconectadas por troncales de Fibra Óptica. La unión a las MANs se realiza mediante el uso de enrutadores o convertidores de protocolos como los Gateways o pasarelas. Puede ser pública o privada. Una MAN puede soportar tanto voz como datos.

Red de área amplia (*WAN*)

Son redes que cubren una amplia región geográfica, a menudo un país o un continente. Este tipo de redes contiene máquinas que ejecutan programas de usuario llamadas hosts o sistemas finales. Los sistemas finales están conectados a una subred de comunicaciones. La función de la subred es transportar los mensajes de un host a otro. En este caso los aspectos de la comunicación pura (la subred) están separados de los aspectos de la aplicación (los host), lo cual simplifica el diseño. En la mayoría de las redes de amplia cobertura se pueden distinguir dos componentes: Las líneas de transmisión y los elementos de intercambio (Conmutación). Las líneas de transmisión se conocen como circuitos,

canales o truncales. Los elementos de intercambio son computadores especializados utilizados para conectar dos o más líneas de transmisión.

CLASIFICACIÓN DE LAS REDES SEGÚN LA TECNOLOGÍA DE TRANSMISIÓN

Redes de Broadcast. Aquellas redes en las que la transmisión de datos se realiza por un sólo canal de comunicación, compartido entonces por todas las máquinas de la red. Cualquier paquete de datos enviado por cualquier máquina es recibido por todas las de la red.

Unicast: el proceso por el cual se envía un paquete de un host a un host individual.

Redes Point-To-Point. Aquellas en las que existen muchas conexiones entre parejas individuales de máquinas. Para poder transmitir los paquetes desde una máquina a otra a veces es necesario que éstos pasen por máquinas intermedias, siendo obligado en tales casos un trazado de rutas mediante dispositivos routers.

Multicast: el proceso por el cual se envía un paquete de un host a un grupo seleccionado de hosts.

CLASIFICACIÓN DE LAS REDES SEGÚN EL TIPO DE TRANSFERENCIA DE DATOS QUE SOPORTAN

Redes de transmisión simple. Son aquellas redes en las que los datos sólo pueden viajar en un sentido.

Redes Half-Duplex. Aquellas en las que los datos pueden viajar en ambos sentidos, pero sólo en uno de ellos en un momento dado. Es decir, sólo puede haber transferencia en un sentido a la vez.

Redes Full-Duplex. Aquellas en las que los datos pueden viajar en ambos sentidos a la vez.

COMPONENTES DE UNA RED

Servidor*:* este ejecuta el sistema operativo de red y ofrece los servicios de red a las estaciones de trabajo.

Estaciones de Trabajo*:* Cuando una computadora se conecta a una red, la primera se convierte en un nodo de la ultima y se puede tratar como una estación de trabajo o cliente. Las estaciones de trabajos pueden ser computadoras personales con el DOS, Macintosh, Unix, OS/2 o estaciones de trabajos sin discos.

Tarjetas o Placas de Interfaz de Red: Toda computadora que se conecta a una red necesita de una tarjeta de interfaz de red que soporte un esquema de red específico, como Ethernet, ArcNet o Token Ring. El cable de red se conectara a la parte trasera de la tarjeta.

Sistema de Cableado: El sistema de la red está constituido por el cable utilizado para conectar entre si el servidor y las estaciones de trabajo.

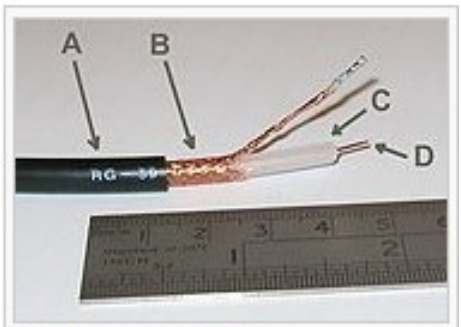
Recursos y Periféricos Compartidos: Entre los recursos compartidos se incluyen los dispositivos de almacenamiento ligados al servidor, las unidades de discos ópticos, las impresoras, los trazadores y el resto de equipos que puedan ser utilizados por cualquiera en la red.

TIPOS DE CABLES

Medios guiados

Cable coaxial.

El cable coaxial es un cable utilizado para transportar señales eléctricas de alta frecuencia que posee dos conductores concéntricos, uno central, llamado positivo o vivo, encargado de llevar la información, y uno exterior, de aspecto tubular, llamado malla o blindaje, que sirve como referencia de tierra y retorno de las corrientes. Entre ambos se encuentra una capa aislante llamada dieléctrico, de cuyas características dependerá principalmente la calidad del cable. Todo el conjunto suele estar protegido por una cubierta aislante.



Cable coaxial RG-59.
A: Cubierta protectora de plástico
B: Malla de cobre
C: Aislante
D: Núcleo de cobre

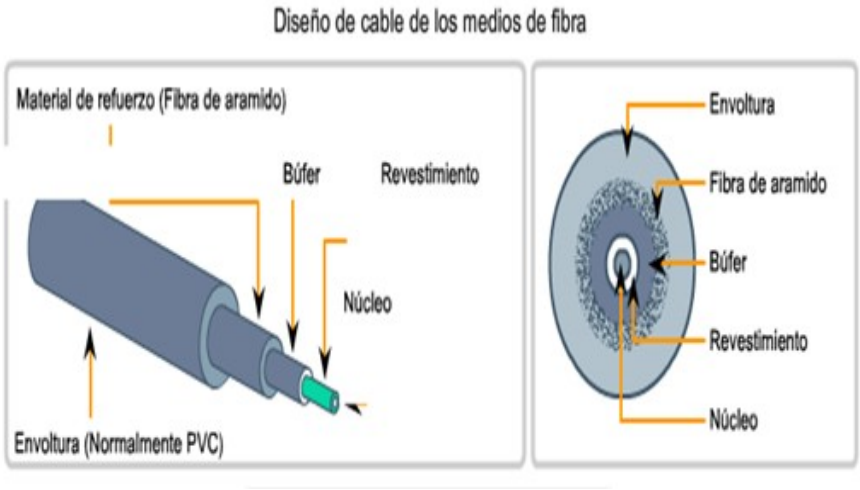
Cable de par trenzado

Los hilos se encuentran trenzados por pares, de forma que cada par forma un circuito. Existen dos categorías de pares trenzados que son: El par trenzado sin pantalla (UTP, unshielder twisted pair) usado en telefonía, y el par trenzado apantallado (STP, shielded twisted pair) proporciona protección frente a la diafonía. El trenzado de los pares permite la eliminación de las interferencias, siendo de esta manera posible la transmisión a velocidades elevadas hasta 100 Mbs.

Fibra óptica

El cable de fibra óptica consta de un núcleo de vidrio central a través del cual se propagan las ondas luminosas. Este núcleo se rodea por un revestimiento de vidrio que fundamentalmente refleja la luz, este tipo de cable se puede extender sobre distancias mucho más grandes que el cable de cobre, no es susceptible a interferencias electromagnéticas, además no radia señales que puedan interferir a

los demás medios de transmisión.



Medios no guiados:

Red por radio

La Red por radio es aquella que emplea la radiofrecuencia como medio de unión de las diversas estaciones de la red.

Es un tipo de red muy actual, usada en distintas empresas dedicadas al soporte de redes en situaciones difíciles para el establecimiento de cableado, como es el caso de edificios antiguos no pensados para la ubicación de los diversos equipos componentes de una Red de ordenadores.

Red por infrarrojos

Las redes por infrarrojos permiten la comunicación entre dos nodos, usando una serie de leds infrarrojos para ello. Se trata de emisores/receptores de las ondas infrarrojas entre ambos dispositivos, cada dispositivo necesita "ver" al otro para realizar la comunicación por ello es escasa su utilización a gran escala.

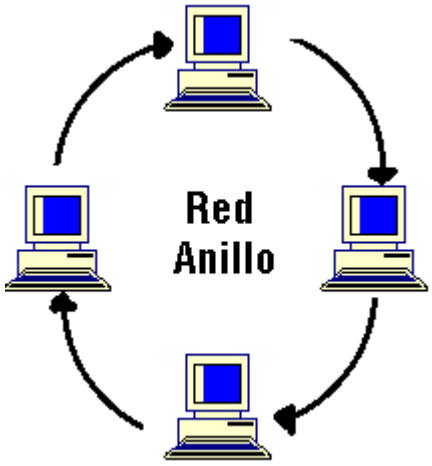
Red por microondas

Una red por microondas es un tipo de red inalámbrica que utiliza microondas como medio de transmisión. El protocolo más frecuente es el IEEE 802.11b y transmite a 2.4 GHz, alcanzando velocidades de 11 Mbps (Megabits por segundo).

TOPOLOGÍA DE RED:

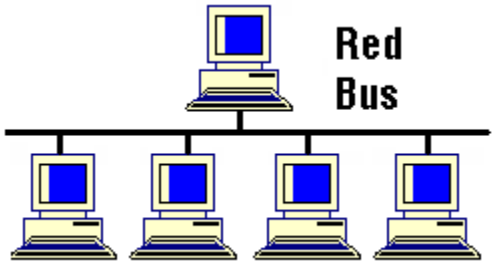
Anillo

En ésta, las computadoras se conectan en un circuito cerrado formando un anillo por donde circula la información en una sola dirección, con esta característica permite tener un control de recepción de mensajes, pero si el anillo se corta los mensajes se pierden.



Bus

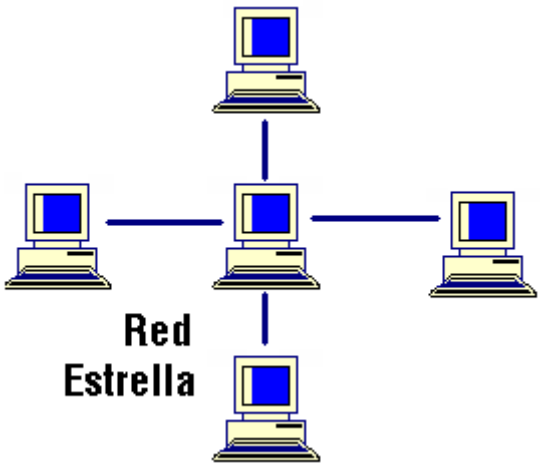
Su funcionamiento es similar a la de red anillo, permite conectar las computadoras en red en una sola línea con el fin de poder identificar hacia cual de todas las computadoras se esté eligiendo.



E

strella

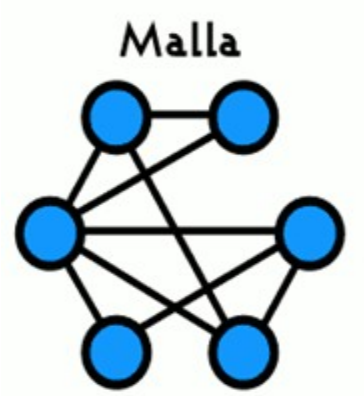
Aquí una computadora hace la función de Servidor y se ubica en el centro de la configuración y todas las otras computadoras o estaciones de trabajo se conectan a él.



Malla

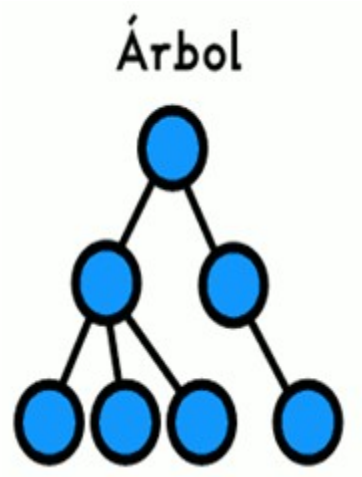
En la topología malla cada computador se conecta a otro casi directamente.

La topología malla se utiliza en redes pequeñas y no se utilizada frecuentemente debido a que es muy costosa.



Árbol

Topología de red en la que los nodos están colocados en forma de árbol. Desde una visión topológica, la conexión en árbol es parecida a una serie de redes en estrella interconectadas salvo en que no tiene un nodo central. En cambio, tiene un nodo de enlace troncal, generalmente ocupado por un hub o switch, desde el que se ramifican los demás nodos. Es una variación de la red en bus, la falla de un nodo no implica interrupción en las comunicaciones. Se comparte el mismo canal de comunicaciones.



PROTOCOLOS DE REDES

El Protocolo de red o también Protocolo de Comunicación es el conjunto de reglas que especifican el intercambio de datos u órdenes durante la comunicación entre las entidades que forman parte de una red.

Estándares de redes

- IEEE 802.3, estándar para Ethernet
- IEEE 802.5, estándar para Token Ring
- IEEE 802.11, estándar para Wi-Fi
- IEEE 802.15, estándar para Bluetooth.

TCP/IP**:**

Se refiere a los dos protocolos que trabajan juntos para transmitir datos: el Protocolo de Control de Transmisión (TCP) y el Protocolo Internet (IP). Cuando envías información a través de una Intranet, los datos se fragmentan en pequeños paquetes. Los paquetes llegan a su destino, se vuelven a fusionar en su forma original. El Protocolo de Control de Transmisión divide los datos en paquetes y los reagrupa cuando se reciben. El Protocolo Internet maneja el encaminamiento de los datos y asegura que se envían al destino exacto.

COMPONENTES BÁSICOS DE LAS REDES DE ORDENADORES

El ordenador

La mayoría de los componentes de una red media son los ordenadores individuales, generalmente son sitios de trabajo (incluyendo ordenadores personales) o servidores.

Tipos de sitios de trabajo

Hay muchos tipos de sitios de trabajo que se pueden incorporar en una red particular, algo de la cual tiene exhibiciones high-end, sistemas con varios CPU, las cantidades grandes de RAM, las grandes cantidades de espacio de almacenamiento en disco duro, u otros componentes requeridos para las tareas de proceso de datos especiales, los gráficos, u otros usos intensivos del recurso.

POSIBLES PROBLEMAS **QUE PRESENTA UNA RED A RAÍZ DE UNA MALA CONFIGURACIÓN EN LOS EQUIPOS ESTABLECIDOS.**

Perdida de las Datos:

La pérdida de datos es producida por algún virus o por otro tipo de incidencia, los más comunes son mal manejo por parte del usuario o personas inescrupulosas que acceden al sistema o mediante Internet, estos puede incidentes pueden evitarse de tal manera que en las estaciones de trabajo se instalan códigos para que así tengan acceso solo personal autorizado, en cuanto a Internet hay muchos software en el

mercado mejor conocidos como Muros de fuego, que sirve para detener a los intrusos.

Caídas Continuas de la Red:

La caída continua en una Red se debe en la mayoría de los casos a una mala conexión Servidor > Concentrador o la conexión existente con el proveedor de Internet.

En el procesamiento de la información es muy lento:

Cuando el procesamiento de información de una Red es muy lento tenemos que tomar en cuenta el tipo de Equipos que elegimos, Servidor, Cableado, Concentrador, Estaciones de Trabajo y otros, ya que si tomamos una decisión errónea perderemos tanto tiempo como dinero.

SERVICIOS DE RED.

Acceso

Los servicios de acceso a la red comprenden tanto la verificación de la identidad del usuario (para determinar cuáles son los recursos de la misma que puede utilizar) como servicios para permitir la conexión de usuarios de la red desde lugares remotos.

Control de acceso

El usuario debe identificarse con un servidor, el cual se autentifica por medio de un nombre de usuario y una clave de acceso. Si ambos son correctos, el usuario puede conectarse a la red.

Acceso remoto.

La red de la organización está conectada con redes públicas que permiten la conexión de estaciones de trabajo situadas en lugares distantes. Según el método utilizado para establecer la conexión, el usuario podrá acceder a unos u otros recursos.

Ficheros

El servicio de ficheros consiste en ofrecer a la red grandes capacidades de almacenamiento para descargar o eliminar los discos de las estaciones. Esto permite almacenar tanto aplicaciones como datos en el servidor, reduciendo los requerimientos de las estaciones. Los ficheros deben ser cargados en las estaciones para su uso.

Impresión

Permite compartir impresoras de alta calidad, capacidad y costo entre múltiples usuarios, lo que reduce el gasto, Existen equipos servidores con capacidad de almacenamiento propio donde se almacenan los trabajos en espera de impresión, lo cual permite que los clientes se descarguen de esta información con más rapidez.

Correo

El correo electrónico es la aplicación de red más utilizada. Permite mejoras en la comunicación frente a otros sistemas, tales como comodidad, costo y rapidez.

Información

Los servidores de información pueden bien servir de ficheros en función de sus contenidos, tales como los documentos hipertexto, o bien, pueden servir información dispuesta. Tal es el caso de los servidores de bases de datos y otras aplicaciones.

DISEÑO DE REDES INFORMÁTICAS

El diseño de una red informática es determinar la estructura física la red. Un buen diseño de la red informática es fundamental para evitar problemas de pérdidas de datos, caídas continuas de la red, problemas de lentitud en el procesamiento de la información y problemas de seguridad informática.

En todo diseño de la red se ha de determinar los equipos a utilizar en la red informática: número de switch, switch intermedios ó para grupos, routers, tarjetas Ethernet, así como la disposición de los conectores RJ45.

Se debe determinar:

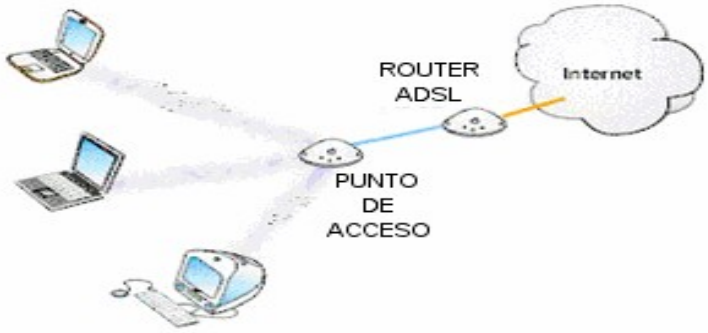
- Tipo de hardware que tiene cada ordenador.

- Elegir el servidor o servidores para las conexiones entre ordenadores.
- Determinar el tipo de adaptadores de red que se necesitan.
- El hardware necesario: modems, routers, switchs, hub, tipo de cable, canaletas.
- Medición del espacio entre los ordenadores y el servidor.

REDES INALÁMBRICAS

En los últimos años las redes de área local inalámbricas (WLAN, Wireless Local Area Network) están ganando mucha popularidad, que se ve acrecentada conforme sus prestaciones aumentan y se descubren nuevas aplicaciones para ellas.

Por red inalámbrica entendemos una red que utiliza ondas electromagnéticas como medio de transmisión de la información que viaja a través del canal inalámbrico enlazando los diferentes equipos o terminales móviles asociados a la red.



- Una conexión funcional a internet con Router ADSL
- Un punto de acceso (Access Point) o antena receptora que deberá conectarse físicamente al router ADSL.
- Un accesorio Wi-fi para cada dispositivo que queramos conectar a la red (equipo portátil, PC, PDA…), y así incorporarle el estándar 802.11, siempre que el dispositivo no lleve Wi-fi integrado de fábrica.

Estos enlaces se implementan básicamente a través de tecnologías de microondas y de infrarrojos, definiéndola como aquella red que provee la funcionalidad y los beneficios que ofrecen las redes como Ethernet, pero sin la limitante de los cables.

Las redes inalámbricas ingresan dentro de varias categorías, dependiendo del tamaño del área física de cobertura

- Red Inalámbrica de Área Personal (Wireless Personal-Area Network / PAN)
- Red Inalámbrica de Área Local (Wireless Local-Area Network / LAN)
- Red Inalámbrica de Área Metropolitana (Wireless Metropolitan-Area Network /MAN)
- Red Inalámbrica de Área Amplia (Wireless Wide-Area Network /WAN)

COMPONENTES DE LAS REDES INALÁMBRICAS

Tarjeta de red inalámbrica o conexión inalámbrica (Wi-Fi).

Cada PC que quieras usar en una red inalámbrica de computadoras necesitará una tarjeta de red inalámbrica o una conexión inalámbrica. Las computadoras portátiles más modernas incluyen conexión inalámbrica.

Punto de acceso (Access point)

Los puntos de acceso tipo puente ("bridge") actúan como switches, permitiendo a los usuarios acceder a la red inalámbrica y estableciendo también conexión con

computadoras alambricamente. Estos se conectan con cable a un ruteador o a un switch.

Ruteador con access point

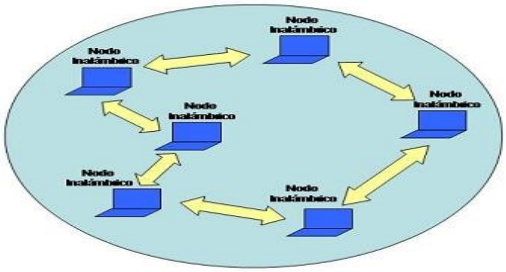
Estos ruteadores realizan la misma función que los ruteadores alambricos e incluyen un puerto WAN (Internet) con conector RJ45, varios puertos LAN con conector RJ45 para conectarse con cable a otras computadoras o periféricos así como un punto de acceso inalámbrico integrado.

Redes Inalámbricas "Bluetooth"

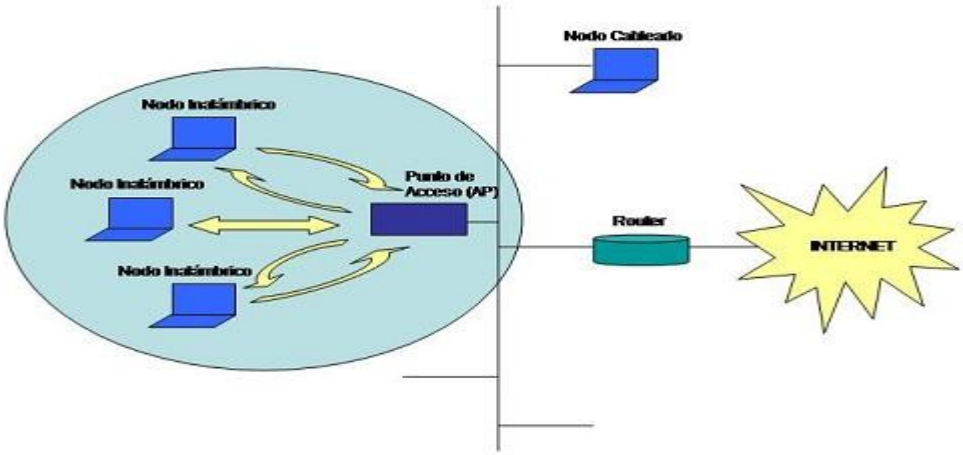
Existe una nueva tecnología de redes que permite a algunos teléfonos celulares y Asistentes Personales Digitales (PDA's) utilizar una red inalámbrica de corta distancia. Esta tecnología se llama Bluetooth y puede recibir y enviar información desde y hasta 10 metros de distancia. Algunas computadoras PC de escritorio y computadoras portátiles incluyen puerto Bluetooth.

TIPOS DE CONFIGURACION DE REDES INALAMBRICAS

Ad-hoc: Cada ordenador dispone de un adaptador inalámbrico y así se comunican todos ellos entre sí, manteniendo una topología punto a punto. Si sólo necesitamos que los ordenadores se "vean" entre sí, nos bastará este modo.



Infraestructura: Cada ordenador dispone de un adaptador inalámbrico que sirve para comunicarse con un router o punto de acceso (AP) inalámbrico central. De esta forma podemos compartir una conexión a Internet, conectando el router Wi-Fi al módem o router de nuestro proveedor de acceso a Internet, o comunicarnos a través del AP con otras LAN o WAN.



VENTAJAS DE WLANS SOBRE LAS REDES FIJAS

Movilidad: las redes inalámbricas proporcionan a los usuarios de una LAN acceso a la información en tiempo real en cualquier lugar dentro de la

organización o el entorno público (zona limitada) en el que están desplegadas. Simplicidad y rapidez en la instalación: la instalación de una WLAN es rápida y fácil y elimina la necesidad de tirar cables a través de paredes y techos. Flexibilidad en la instalación. La tecnología inalámbrica permite a la red llegar a puntos de difícil acceso para una LAN cableada.

Escalabilidad: los sistemas de WLAN pueden ser configurados en una variedad de topologías para satisfacer las necesidades de las instalaciones y aplicaciones específicas. Las configuraciones son muy fáciles de cambiar y además resulta muy fácil la incorporación de nuevos usuarios a la red.

SEGURIDAD DE LAS REDES

¿Qué es la seguridad de redes?

La seguridad de redes es un nivel de seguridad que garantiza que el funcionamiento de todas las máquinas de una red sea óptimo y que todos los usuarios de estas máquinas posean los derechos que les han sido concedidos:

Esto puede incluir:

- Evitar que personas no autorizadas intervengan en el sistema con fines malignos
- Evitar que los usuarios realicen operaciones involuntarias que puedan dañar el sistema
- Asegurar los datos mediante la previsión de fallas
- Garantizar que no se interrumpan los servicios

LAS CAUSAS DE INSEGURIDAD

Un estado de inseguridad activo, es decir, la falta de conocimiento del usuario acerca de las funciones del sistema, algunas de las cuales pueden ser dañinas para el sistema (por ejemplo, no desactivar los servicios de red que el usuario no necesita)

Un estado pasivo de inseguridad; es decir, cuando el administrador (o el usuario) de un sistema no está familiarizado con los mecanismos de seguridad presentes en el sistema

EL OBJETIVO DE LOS INTRUSOS

- Los atacantes (también denominados "piratas" o "hackers") pueden tener muchos motivos:
- La atracción hacia lo prohibido
- El deseo de obtener dinero (por ejemplo, violando el sistema de un banco)
- La reputación (impresionar a sus amigos)
- El deseo de hacer daño (destruir datos, hacer que un sistema no funcione)

Frecuentemente, el objetivo de los atacantes es controlar una máquina para poder llevar a cabo acciones deseadas.

Existen varias formas de lograr esto:

- Obteniendo información que puede utilizarse en ataques
- Explotando las vulnerabilidades del sistema
- Forzando un sistema para irrumpir en él

PROTOCOLOS DE SEGURIDAD EN REDES INALÁMBRICAS

WEP

Características y funcionamiento

WEP (*Wired Equivalent Privacy*, privacidad equivalente al cable) es el algoritmo opcional de seguridad incluido en la norma IEEE 802.11. Los objetivos de WEP, según el estándar, son proporcionar confidencialidad, autentificación y control de acceso en redes WLAN. WEP utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso. El estándar no contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de red. Esto genera varios inconvenientes. Por un lado, la clave está almacenada en todas las estaciones, aumentando las posibilidades de que sea comprometida. Y por otro, la distribución manual de claves provoca un aumento de mantenimiento por parte del administrador de la

red, lo que conlleva, en la mayoría de ocasiones, que la clave se cambie poco o nunca.

WPA

WPA (*Wi-Fi Protected Access*, acceso protegido Wi-Fi) es la respuesta de la asociación de empresas Wi-Fi a la seguridad que demandan los usuarios y que WEP no puede proporcionar.

Debido a la tardanza, Wi-Fi decidió, en colaboración con el IEEE, tomar aquellas partes del futuro estándar que ya estaban suficientemente maduras y publicar así WPA. WPA es, por tanto, un subconjunto de lo que será IEEE 802.11i. WPA se está ofreciendo en los dispositivos actuales.

WPA soluciona todas las debilidades conocidas de WEP y se considera suficientemente seguro. Puede ocurrir incluso que usuarios que utilizan WPA no vean necesidad de cambiar a IEEE 802.11i cuando esté disponible.

WPA incluye las siguientes tecnologías:

- **IEEE 802.1X**. Estándar del IEEE de 2001 para proporcionar un control de acceso en redes basadas en puertos.
- **EAP** definido en la RFC 2284, es el protocolo de autentificación extensible para llevar a cabo las tareas de autentificación, autorización y contabilidad.
- **MIC** (*Message Integrity Code*). Código que verifica la integridad de los datos de las tramas.

WPA2 (IEEE 802.11i)

802.11i es el nuevo estándar del IEEE para proporcionar seguridad en redes WLAN. Wi-Fi está haciendo una implementación completa del estándar en la especificación WPA2.

WPA2 incluye el nuevo algoritmo de cifrado AES (*Advanced Encryption Standard*), desarrollado por el NIS. Se trata de un algoritmo de cifrado de bloque (RC4 es de flujo) con claves de 128 bits. Requerirá un hardware potente para

realizar sus algoritmos. Este aspecto es importante puesto que significa que dispositivos antiguos sin suficientes capacidades de proceso no podrán incorporar WPA2. Para el aseguramiento de la integridad y autenticidad de los mensajes, WPA2 utiliza CCMP (Counter-Mode / Cipher Block Chaining / Message Authentication Code Protocol) en lugar de los códigos MIC.

MONITOREO

Existen varias clases diferentes de herramientas de monitoreo, cada una le muestra un aspecto diferente de lo que "está pasando", desde la interacción física del radio a las formas en que las aplicaciones de los usuarios interactúan entre ellas. Al observar el desempeño de la red a través del tiempo se puede tener una idea de lo que es "normal" para ella, y ser notificado automáticamente cuando las cosas están fuera de orden.

SISTEMA DE MONITOREO

DETECCIÓN DE REDES

Las herramientas de monitoreo comunes, simplemente proveen una lista de redes disponibles con información básica como intensidad de la señal y canal. Le permiten detectar rápidamente redes cercanas y determinar si están dentro de su alcance o si están causando interferencia.

Las incorporadas en el cliente

- **Netstumbler.-.** Es la herramienta más popular para detectar redes inalámbricas utilizando Microsoft Windows. Detecta redes abiertas y encriptadas, pero no puede detectar redes inalámbricas "cerradas".
- **Ministumbler.**-Provee muchas de las mismas funcionalidades que la versión de Windows, pero funciona en las plataformas Pocket PC.
  Ministumbler se puede correr en PDAs portátiles con una tarjeta inalámbrica para detectar puntos de acceso en la zona.
- **Macstumbler.**- Brinda muchas de sus funcionalidades pero para la plataforma Mac OS X. Funciona con todas las tarjetas Apple Airport.

- **Wellenreiter.-**Es un buen detector gráfico de redes inalámbricas para Linux. Requiere Perl y GTK, y soporta tarjetas inalámbricas Prism2, Lucent, y Cisco.

ANALIZADORES DE PROTOCOLOS

Los analizadores de protocolos de redes permiten inspeccionar paquetes individualmente ya que una gran cantidad de detalles de la información fluyen por una red. Para las redes inalámbricas, se puede inspeccionar información hasta las tramas 802.11. Existen varios analizadores de protocolos de redes populares tales como:

- **Ethereal.-** Es un analizador de protocolos que funciona con Linux, Windows, Mac OS X, y con varios sistemas SSD, capturara los paquetes directamente "del cable" y los despliega en una interfaz gráfica intuitiva. Puede decodificar más de 750 protocolos, desde las tramas 802.11 a los paquetes HTTP.
- **Kismet.-**Es un poderoso analizador de protocolos inalámbrico para Linux, Mac OS X, y la distribución Linux embebida OpenWRT. Funciona con cualquier tarjeta inalámbrica que soporte el modo monitor pasivo.
- **KisMAC.-** Desarrollado exclusivamente para la plataforma Mac OS X, puede hacer mucho de lo que Kismet hace, pero con una interfaz gráfica Mac OS X muy elaborada. Es un rastreador pasivo que registra datos al disco en un formato PCAP compatible con Ethereal. No soporta un rastreo pasivo con tarjetas AirportExtreme por las limitaciones en el manejador inalámbrico, pero soporta el modo pasivo con una variedad de tarjetas inalámbricas USS.

- **Driftnet y Etherpeg.-** Estas herramientas decodifican datos gráficos como los archivos GIF y JPEG y los despliegan como un collage. Esta herramienta tiene un uso limitado en la resolución de problemas, pero tienen mucho valor para demostrar la inseguridad de los protocolos sin

encriptación.

MONITOREO DEL ANCHO DE BANDA

Utilizando una buena herramienta de monitoreo se puede determinar fácilmente la fuente que inunda la red de correo no deseado y de virus.

Dichas herramientas también ayudan a planificar los incrementos de capacidad requeridos para mantener los usuarios satisfechos. Al mismo tiempo dan una representación visual de cómo fluye el tráfico en la red.

- **MRTG.-** Es una herramienta para supervisar la carga de tráfico en los enlaces de red, genera páginas de HTML que contienen imágenes gráficas que proporcionan una representación visual VIVA de este tráfico.
  Utilizando Perl y C, construye una página web llena de gráficos detallando el tráfico saliente y entrante en un dispositivo de red en particular.
- **RRDtool.- E**s una aplicación de monitoreo genérica más poderosa. RRD es una abreviatura de base de datos de recorrido circular (Round-Robin Database). Este es un formato de datos genérico que le permite seguir cualquier punto de datos como un conjunto promediado en el tiempo. Si bien rrdtool no monitorea directamente interfaces o dispositivos, muchos paquetes de monitoreo confían en él para almacenar y desplegar los datos que colectan.
- **Ntop.-** Se utiliza para realizar un análisis histórico del tráfico y del uso de la red, este programa construye un reporte detallado en tiempo real de lo que observa en el tráfico de la red, y lo despliega en su navegador web. Se integra con rrdtool, y realiza gráficos y cuadros visuales que representan cómo está siendo usada la red. Funciona en Linux, BSO, Mac OS X, y Windows.
- **Iptraf.-** Se utiliza para realizar un análisis de la actividad de la red en un sistema Linux. Brinda en segundos una mirada sobre las conexiones y el flujo de la red, incluyendo puertos y protocolos. Puede ser muy buena para determinar quién está usando un enlace inalámbrico en particular, y cuanta carga se le está imponiendo.

SALUD DE LA RED

Siguiendo la información a través del tiempo, usted puede tener una idea general de la salud de la red y sus servicios. Estas herramientas muestran las tendencias de la red y pueden incluso notificar a las personas cuando se presenten problemas.

- **Cacti.**-Es una herramienta que utiliza RROtool como programa de soporte (back-end) para armar gráficos con los datos que ellas recolectan. Es una herramienta de gestión de redes basada en PHP que simplifica la recolección de datos y la generación de gráficos. Cacti hace muy sencillo el mapeo de todos los dispositivos en su red y monitorea todo, desde el flujo de la red hasta la carga del CPU.
- **SmokePing.**- Está escrita en Perl y muestra la pérdida de paquetes y la latencia en un único gráfico. Es muy útil correr SmokePing en un servidor con buena conectividad a toda su red. Con el tiempo, revela tendencias que pueden apuntar a todo tipo de problemas de red.
- **Nagios.-** Es una herramienta de monitoreo de servicio. Además de seguir el desempeño de simples contactos como con SmokePing, Nagios puede observar el desempeño de los servicios reales en varias máquinas. Puede consultar periódicamente su servidor web, y estar seguro de que devuelve una página web válida.

2.4 HIPOTESIS

La implementación de sistemas de análisis y monitoreo en redes inalámbricas en la empresa “DISTRY-TEX”, permitirá tener mayor seguridad y confiabilidad en la información y en los servicios que esta posee.

2.5 VARIABLES

2.5.1 VARIABLE INDEPENDIENTE

Redes Inalámbricas

2.5.2 VARIABLE DEPENDIENTE

Sistemas de Análisis y Monitoreo

CAPITULO III

METODOLOGIA

3.1 MODALIDAD BÁSICA DE LA INVESTIGACIÓN

3.1.1 INVESTIGACIÓN BIBLIOGRÁFICA - DOCUMENTAL

Se realizó una investigación bibliográfica - documental para poder obtener información más profunda con respecto al problema y a su solución, de esta manera recopilar información valiosa que servirá de apoyo en la realización del proyecto.

3.2 NIVEL O TIPO DE INVESTIGACIÓN

3.2.1 EXPLORATORIO

Fue exploratorio porque será necesario realizar el estudio donde abarcará el nivel investigativo acerca del problema, para poder establecer el origen del mismo, además de investigar las causas del problema, y el porqué se dio el mismo

3.2.2 DESCRIPTIVO

Fue descriptivo porque analizará al problema, cuales son las causas, consecuencias y dificultades por lo que está atravesando el problema.

3.3 POBLACIÓN Y MUESTRA

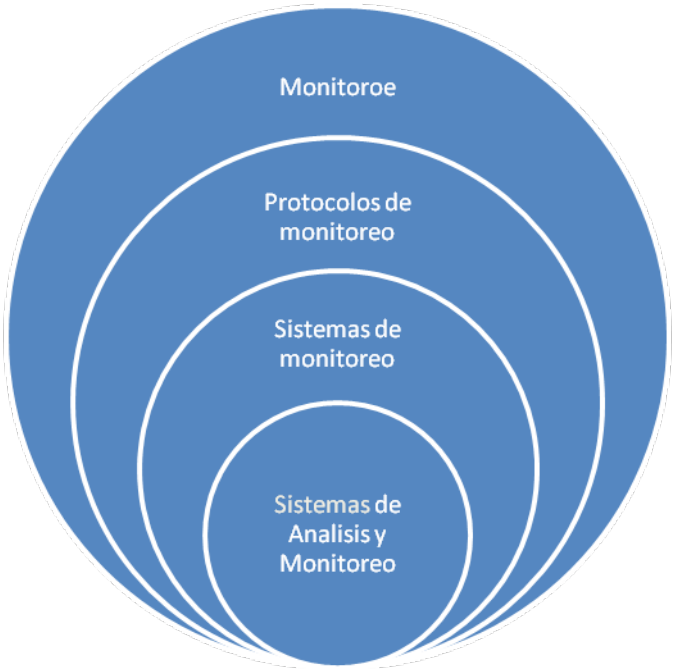
3.3.1 POBLACIÓN

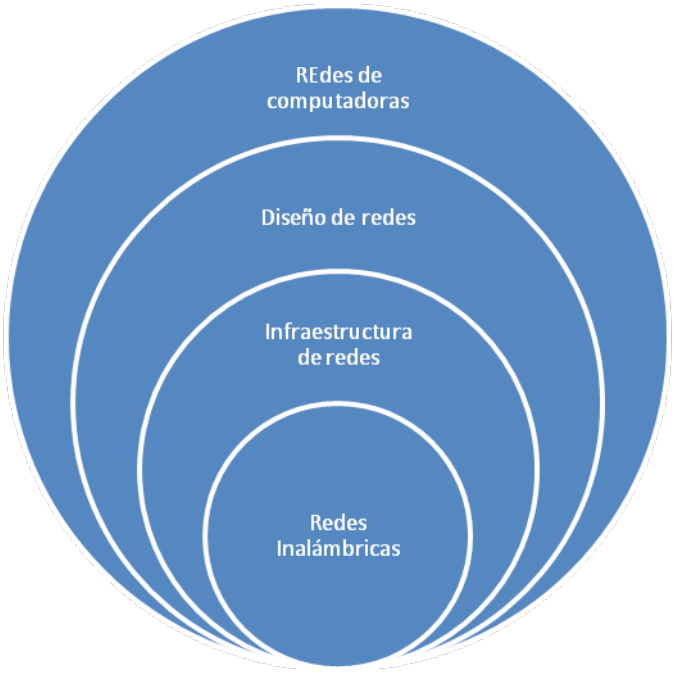
Se trabajará con una población integrada por siete docentes.

3.3.2 MUESTRA

Como la población es pequeña se trabajará con todo el universo.

3.4 OPERACIONALIZACIÓN DE LAS VARIABLES


Monitoroe
Protocolos de monitoreo
Sistemas de monitoreo
Sistemas de Analisis y Monitoreo


REdes de computadoras
Diseño de redes
Infraestructura de redes
Redes Inalámbricas

CAPITULO IV

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- La seguridad en las redes inalámbricas es una necesidad, dadas las características de la información que por ellas se transmite. Sin embargo, la gran cantidad de las redes inalámbricas actualmente instaladas no tienen

configurada seguridad alguna, o poseen un nivel de seguridad muy débil, con lo cual se está poniendo en peligro la confidencialidad e integridad de dicha información.

- La restricción de acceso mediante direcciones MAC es insuficiente para cualquier red, dado el gran número de herramientas disponibles libremente para cambiar la dirección MAC de una tarjeta cualquiera.

- Los datos deben viajar cifrados por el aire, para evitar que equipos ajenos a la red puedan capturar datos mediante escucha pasiva.

- El uso de las VPN (Red Virtual Privada) es una alternativa interesante cuando ya se tiene una red inalámbrica, y no se posee hardware inalámbrico que soporte el protocolo 802.1x. Requiere de la instalación de software especializado en los clientes inalámbricos, y de un servidor o una serie de servidores que manejen las tareas de cifrado de datos, autenticación y autorización de acceso.

- Una red puede tornarse inoperativa como resultado de ataques de Negación de servicio o software malicioso, pero también debido a nodos ocultos de los que no tenemos idea de su existencia, y problemas de interferencia. Solo mediante el monitoreo de tráfico en la red, se pueden encontrar las causas reales de un problema.

- Las ondas de radio deben confinarse tanto como sea posible. Esto es difícil de lograr totalmente, pero se puede hacer un buen trabajo empleando antenas direccionales y configurando adecuadamente la potencia de transmisión de los puntos de acceso.

RECOMENDACIONES

- No hay una solución estándar de seguridad para todas las redes inalámbricas. Es necesario tener una idea clara de los requisitos de seguridad, y la solución depende de cada escenario:
    - Habilitar todas las capacidades de seguridad de los dispositivos
    - Monitorear constantemente la red si existen sospechas de ataques

- Debe existir algún mecanismo de autenticación en doble vía, que permita al cliente verificar que se está conectando a la red correcta, y a la red constatar que el cliente está autorizado para acceder a ella.

- El método mediante WEP con clave estática es el mínimo nivel de protección que existe. En una red casera puede ser suficiente; en una corporativa, el uso de WEP está formalmente desaconsejado, por la facilidad con la que se pueden romper las claves WEP en un entorno de alto tráfico.

- El sistema WEP, incluido en la norma IEEE 802.11 para proporcionar seguridad, tiene distintas debilidades que lo hacen no seguro, por lo que deben buscarse otras alternativas para la seguridad.

CAPITULO V

PROPUESTA

5.1. DATOS INFORMATIVOS

- Universidad Técnica de Ambato
- Facultad de Ingeniería en Sistemas, Electrónica e Industrial
- Carrera de Ingeniería en Electrónica y Comunicaciones

- Tutor: Ing. Iván Aldás.
- Desarrollador Segundo Danilo Barrera Morales
- Correo Electrónico danilobarrera91@yahoo.es
- Empresa: DISTRY-TEX

5.2. ANTECEDENTES DE LA PROPUESTA

Al revisar los archivos en la biblioteca de la Facultad de Ingeniería en Sistemas Electrónica e Industrial se ha encontrado los siguientes trabajos investigativos que está relacionado con las redes inalámbricas, las cuales fueron desarrolladas por Alex Salazar con el título “Diseño de una red comunitaria basada en tecnologías WLAN para la facultad de Ingeniería en Sistemas Electrónica e Industrial” en el periodo Abril Septiembre del 2005, también un perfil presentado por Karina Zagal en el periodo Septiembre-febrero del 2007-2008 la cual lleva por título " Sistema de monitoreo de la Red Inalámbrica en la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato", cuyas conclusiones se refieren a la seguridad que se puede obtener con el monitoreo de las redes inalámbricas.

5.3. JUSTIFICACION

En este mundo que va evolucionando a la par con la tecnología y donde la demanda de redes inalámbricas es mas continuo, es necesario tener un Sistema de análisis y monitoreo para la seguridad de Redes Inalámbricas, y así poder brindar mayor confiabilidad a los usuarios de estas.

El desarrollo de este proyecto será de vital importancia ya que ayudara a las empresas pequeñas que disponen de redes inalámbricas a mantener la seguridad en su red, para evitar que personas ajenas a esta puedan acceder sin permisos.

El monitoreo de la red inalámbrica de la empresa permite conocer un medio de seguridad cada vez más relevante y permitir una mayor comodidad en los usuarios de esta red.

Este proyecto de desarrollo de un sistema de análisis y monitoreo de una red inalámbrica aportará con una buena forma de comunicación interna y segura en las empresa.

5.4. OBJETIVOS

5.4.1 OBJETIVO GENERAL

Desarrollo de un sistema de análisis y monitoreo para la Red Inalámbrica de la empresa “DISTRY-TEX”

5.4.2 OBJETIVOS ESPECÍFICOS

5.4.2.1. Analizar la infraestructura de red existente en la empresa y los diferentes tipos de equipos que dispone.

5.4.2.2. Explicar cómo funcionan los Protocolos y sistemas de seguridad en las red inalámbrica y como se pueden usar para monitorear la misma.

5.4.2.3. Determinar los pasos apropiados para el desarrollo de este sistema.

5.4.2.4. Establecer los beneficios que presenta el análisis y monitoreo de las redes inalámbricas.

5.5. ANALISIS DE FACTIVILIDAD

5.5.1 Análisis de Factibilidad Económica.

El Sistema de de análisis y monitoreo de la red inalámbrica de la empresa DISTRY-TEX, se presenta como un proyecto económicamente factible debido a que la empresa cuenta ya en la actualidad con un adecuado equipamiento, siendo pocos y accesibles los dispositivos nuevos a adquirir.

5.5.2. Análisis de Factibilidad Operativa.

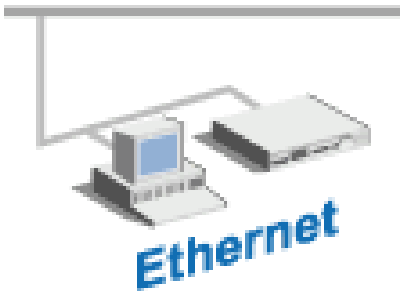
La Factibilidad Operativa se basa en la capacidad de operar el sistema de Monitoreo de la red inalámbrica de una manera correcta, segura y fiable, no cabe duda que posee el personal idóneo para sobrellevar y operar el sistema aprovechando todas sus utilidades y corrigiendo posibles errores que se presenten en dicha red.

5.6. FUNDAMENTACION

TOPOLOGÍAS QUE CONTEMPLAN LAS HERRAMIENTAS DE ANÁLISIS Y MONITOREO DE REDES

LAN Control

- Decodifica y analiza más de 450 protocolos en tiempo real
- Es posible configurar alarmas de notificación sobre eventos específicos que ocurran en las redes
- Es posible rastrear el uso de internet para replantear sus políticas de utilización

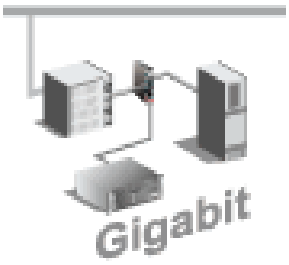


Wireless LAN Control

- Monitoreo y Análisis completo de 802.11 a/b/g.
- Planee el rendimiento de sus redes inalámbricas con base a estadísticas de uso.
- Monitoree redes inalámbricas desde consolas fijas, laptops o Tabletas PC.
- Proteja redes inalámbricas con alertas reforzando las políticas de seguridad.

Gigabit Control

- Monitorea enlaces Gigabit a velocidades de full-duplex
- Integra el análisis de Gigabit y de redes 10/100
- Observe el flujo de todos los datos Gigabit sin generar ruido en su red



WAN Control

- Examina el uso del ancho de banda para monitorear la eficiencia de la red, el rendimiento QoS y SLA
- Reporta problemas de la WAN y tendencias de la red en detalle
- Resuelve problemas de la WAN con herramientas de análisis experto

5.7. METODOLOGIA

Al analizar la infraestructura de la empresa se obtuvo la siguiente información: Cuenta con dos maquinas de escritorio, una portátil, un Access point, y un router, los esquemas utilizados para la seguridad son filtrado de MAC address, y encripción de tráfico vía WEP, pero estas seguridades no son suficientes por que existen gran cantidad de herramientas que permiten evadir, por esta razón es que

se necesita un sistema de análisis y monitoreo de la red inalámbrica de la red de la empresa para poder saber que pasa y quienes están ocupando la misma.

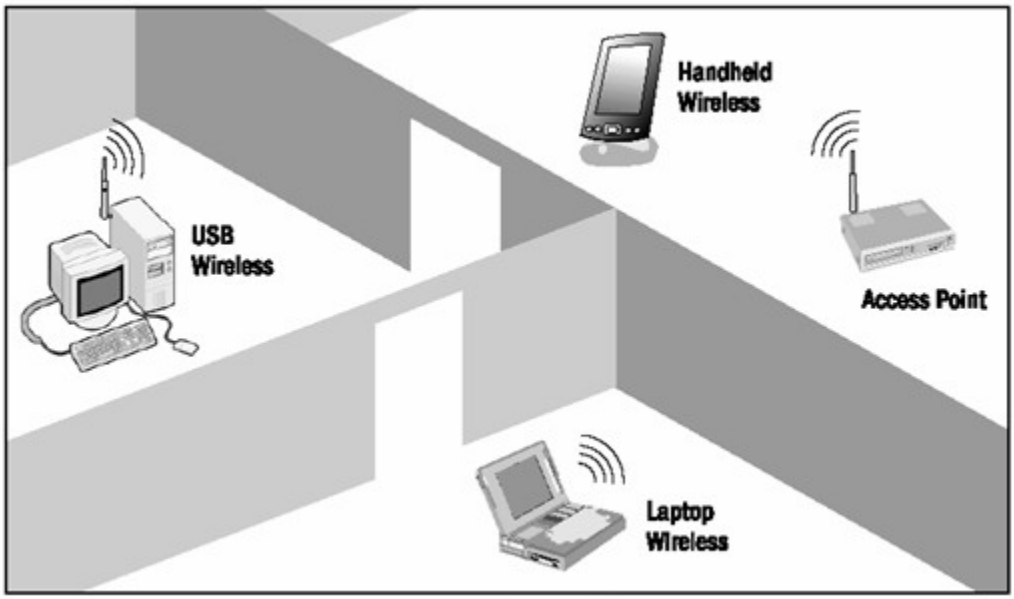


FIGURA 1. ESQUEMA DE RED INALAMBRICA

PROTOCOLOS Y SISTEMAS DE SEGURIDAD EN LA RED INALÁMBRICA

La falta de seguridad en las redes inalámbricas es un problema que, a pesar de su gravedad, no ha recibido la atención debida por parte de los administradores de redes y los responsables de la información. Este proyecto presenta las tecnologías existentes para mejorar el nivel de análisis y monitoreo en las redes inalámbricas para lograr una mayor seguridad.

Existen varios métodos para lograr la configuración segura de una red inalámbrica; cada método logra un nivel diferente de seguridad y presenta ciertas ventajas y desventajas. En el desarrollo de este proyecto realizaremos una explicación de cada uno:

- **Filtrado de direcciones MAC**

Este método consiste en la creación de una tabla de datos en cada uno de los puntos de acceso a la red inalámbrica. Dicha tabla contiene las direcciones MAC (Media Access Control) de las tarjetas de red inalámbricas que se pueden conectar

al punto de acceso. Como toda tarjeta de red posee una dirección MAC única, se logra autenticar el equipo. Este método tiene como ventaja su sencillez, por lo cual se puede usar para redes caseras o pequeñas. Sin embargo, posee muchas desventajas que lo hacen impráctico para uso en redes medianas o grandes:

• No escala bien, porque cada vez que se desee autorizar o dar de baja un equipo, es necesario editar las tablas de direcciones de todos los puntos de acceso. Después de cierto número de equipos o de puntos de acceso, la situación se torna inmanejable.

• El formato de una dirección MAC no es amigable (normalmente se escriben como 6 bytes en hexadecimal), lo que puede llevar a cometer errores en la manipulación de las listas.

• Las direcciones MAC viajan sin cifrar por el aire. Un atacante podría capturar direcciones MAC de tarjetas matriculadas en la red empleando un sniffer, y luego asignarle una de estas direcciones capturadas a la tarjeta de su computador, empleando programas tales. De este modo, el atacante puede hacerse pasar por un cliente válido.

• En caso de robo de un equipo inalámbrico, el ladrón dispondrá de un dispositivo que la red reconoce como válido. En caso de que el elemento robado sea un punto de acceso el problema es más serio, porque el punto de acceso contiene toda la tabla de direcciones válidas en su memoria de configuración. Debe notarse además, que este método no garantiza la confidencialidad de la información transmitida, ya que no prevé ningún mecanismo de cifrado.

- **Wired Equivalent Privacy (WEP)**

El algoritmo WEP forma parte de la especificación 802.11, y se diseñó con el fin de proteger los datos que se transmiten en una conexión inalámbrica mediante cifrado. WEP opera a nivel 2 del modelo OSI y es soportado por la gran mayoría de fabricantes de soluciones inalámbricas.

El algoritmo WEP cifra de la siguiente manera:

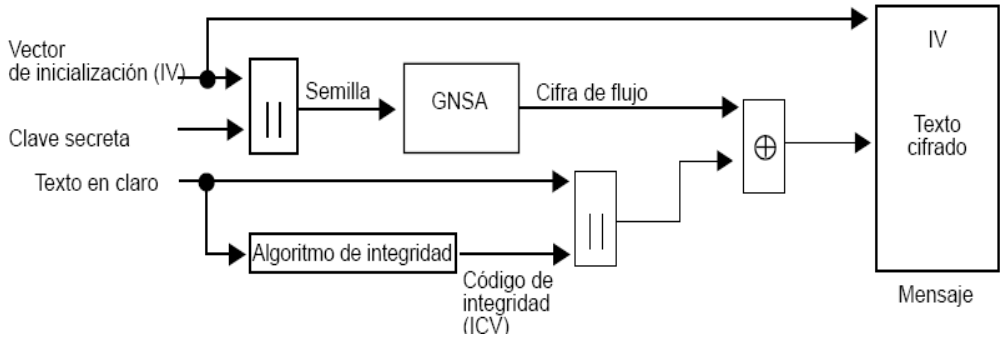


FIGURA 2. FUNCIONAMIENTO DEL ALGORITMO WEP EN MODALIDAD DE CIFRADO

• A la trama en claro se le computa un código de integridad (Integrity Check Value, ICV) mediante el algoritmo CRC-32. Dicho ICV se concatena con la trama, y es empleado más tarde por el receptor para comprobar si la trama ha sido alterada durante el transporte.

• Se escoge una clave secreta compartida entre emisor y receptor. Esta clave puede poseer 40 ó 128 bits.

• Si se empleara siempre la misma clave secreta para cifrar todas las tramas, dos tramas en claro iguales producirían tramas cifradas similares. Para evitar esta eventualidad, se concatena la clave secreta con un número aleatorio llamado vector de inicialización (IV) de 24 bits. El IV cambia con cada trama.

• La concatenación de la clave secreta y el IV (conocida como semilla) se emplea como entrada de un generador RC4 de números seudo- aleatorios. El generador RC4 es capaz de generar una secuencia seudo-aleatoria (o cifra de flujo) tan larga como se desee a partir de la semilla.

• El generador RC4 genera una cifra de flujo, del mismo tamaño de la trama a cifrar más 32 bits (para cubrir la longitud de la trama y el ICV).

• Se hace un XOR bit por bit de la trama con la secuencia de clave, obteniéndose como resultado la trama cifrada.

• El IV y la trama se transmiten juntos.

En el receptor se lleva a cabo el proceso de descifrado:

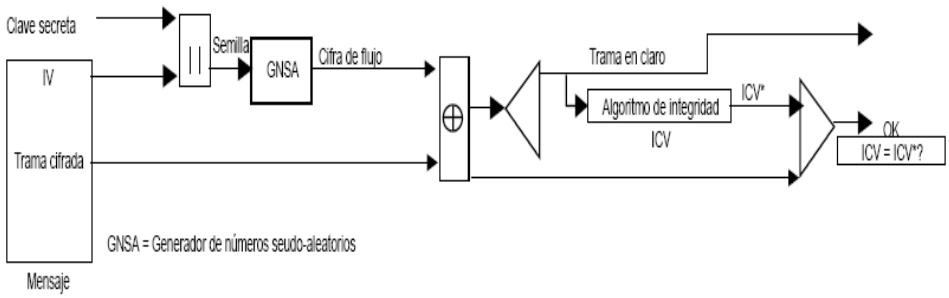


FIGURA 3. FUNCIONAMIENTO DEL ALGORITMO WEP EN MODALIDAD DE DESCIFRADO

• Se emplean el IV recibido y la clave secreta compartida para generar la semilla que se utilizó en el transmisor.

• Un generador RC4 produce la cifra de flujo a partir de la semilla. Si la semilla coincide con la empleada en la transmisión, la cifra de flujo también será idéntica a la usada en la transmisión.

• Se efectúa un XOR bit por bit de la cifra de flujo y la trama cifrado, obteniéndose de esta manera la trama en claro y el ICV.

• A la trama en claro se le aplica el algoritmo CRC-32 para obtener un segundo ICV, que se compara con el recibido.

• Si los dos ICV son iguales, la trama se acepta; en caso contrario se rechaza.

El algoritmo WEP resuelve aparentemente el problema del cifrado de datos entre emisor y receptor. Sin embargo, existen dos situaciones que hacen que WEP no sea seguro en la manera que es empleado en la mayoría de aplicaciones:

• La mayoría de instalaciones emplea WEP con claves de cifrado estáticas (se configura una clave en el punto de acceso y no se la cambia nunca, o muy de vez en cuando). Esto hace posible que un atacante acumule grandes cantidades de texto cifrado con la misma clave y pueda intentar un ataque por fuerza bruta.

• El IV que se utiliza es de longitud insuficiente (24 bits). Dado que cada trama se cifra con un IV diferente, solamente es cuestión de tiempo para que se agote el espacio de 2^{24} IV distintos. Esto no es problemático en una red casera con bajo tráfico, pero en una red que posea alto tráfico se puede agotar el espacio de los IV

en más o menos 5 horas. Si el atacante logra conseguir dos tramas con IV idéntico, puede efectuar un XOR entre ellas y obtener los textos en claro de ambas tramas mediante un ataque estadístico. Con el texto en claro de una trama y su respectivo texto cifrado se puede obtener la cifra de flujo; conociendo el funcionamiento del algoritmo RC4 es posible entonces obtener la clave secreta y descifrar toda la conversación.

• WEP no ofrece servicio de autenticación. El cliente no puede autenticar a la red, ni al contrario; basta con que el equipo móvil y el punto de acceso compartan la clave WEP para que la comunicación pueda llevarse a cabo. Existen en este momento diversas herramientas gratuitas para romper la clave secreta de enlaces protegidos con WEP.

- **Las VPN**

Una red privada virtual (Virtual Private Network, VPN) emplea tecnologías de cifrado para crear un canal virtual privado sobre una red de uso público. Las VPN resultan especialmente atractivas para proteger redes inalámbricas, debido a que funcionan sobre cualquier tipo de hardware inalámbrico y superan las limitaciones de WEP.

Para configurar una red inalámbrica utilizando las VPN, debe comenzarse por asumir que la red inalámbrica es insegura. Esto quiere decir que la parte de la red que maneja el acceso inalámbrico debe estar aislada del resto de la red, mediante el uso de una lista de acceso adecuada en un enrutador, o agrupando todos los puertos de acceso inalámbrico en una VLAN si se emplea switching. Dicha lista de acceso y/o VLAN solamente debe permitir el acceso del cliente inalámbrico a los servidores de autorización y autenticación de la VPN. Deberá permitirse acceso completo al cliente, sólo cuando éste ha sido debidamente autorizado y autenticado.

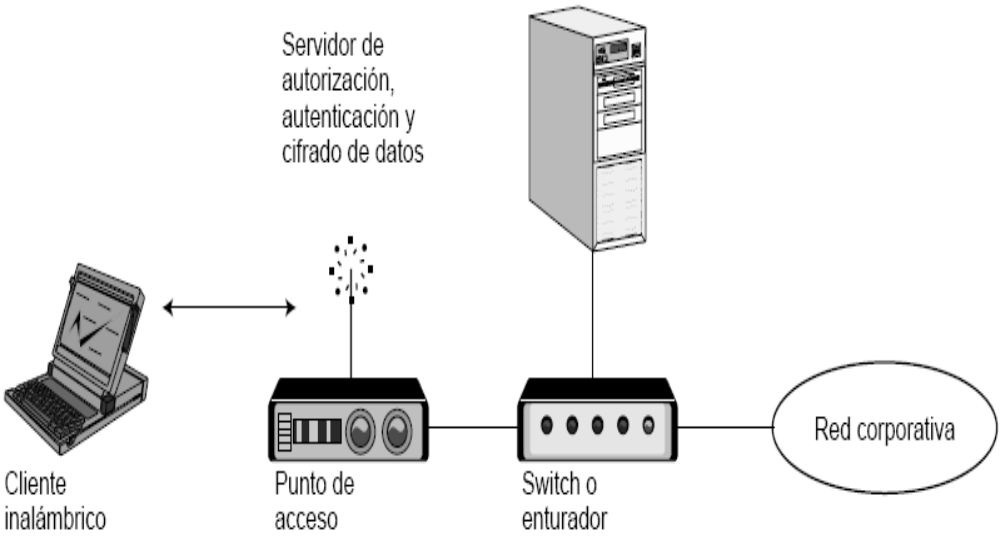


FIGURA 4. ESTRUCTURA DE UNA VPN PARA ACCESO INALÁMBRICO SEGURO.

Los servidores de VPN se encargan de autenticar y autorizar a los clientes inalámbricos, y de cifrar todo el tráfico desde y hacia dichos clientes.
Dado que los datos se cifran en un nivel superior del modelo OSI, no es necesario emplear WEP en este esquema.

- **802.1x**

802.1x es un protocolo de control de acceso y autenticación basado en la arquitectura cliente/servidor, que restringe la conexión de equipos no autorizados a una red. El protocolo fue inicialmente creado por la IEEE para uso en redes de área local alambradas, pero se ha extendido también a las redes inalámbricas. Muchos de los puntos de acceso que se fabrican en la actualidad ya son compatibles con 802.1x.
El protocolo 802.1x involucra tres participantes:

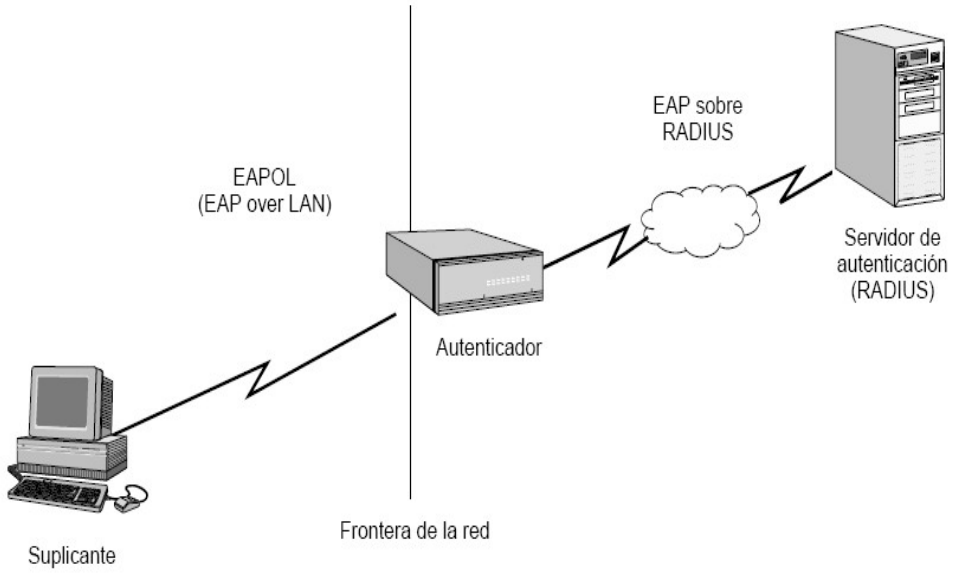


FIGURA 5. ARQUITECTURA DE UN SISTEMA DE AUTENTICACIÓN 802.1X.

• **El suplicante**, o equipo del cliente, que desea conectarse con la red.

• **El servidor de autorización/autenticación**, que contiene toda la información necesaria para saber cuáles equipos y/o usuarios están autorizados para acceder a la red. 802.1x fue diseñado para emplear servidores RADIUS (Remote Autenticación Dial-In User Service). Estos servidores fueron creados inicialmente para autenticar el acceso de usuarios remotos por conexión vía telefónica; dada su popularidad se optó por emplearlos también para autenticación en las LAN.

• **El autenticador**, que es el equipo de red (switch, enrutador, servidor de acceso remoto...) que recibe la conexión del suplicante. El autenticador actúa como intermediario entre el suplicante y el servidor de autenticación, y solamente permite el acceso del suplicante a la red cuando el servidor de autenticación así lo autoriza.

La autenticación del cliente se lleva a cabo mediante el protocolo EAP (Extensible Authentication Protocol) y el servicio RADIUS, de la siguiente manera:

• El proceso inicia cuando la estación de trabajo se enciende y activa su interfaz de red (en el caso alambrado) o logra enlazarse o asociarse con un punto de acceso (en el caso inalámbrico). En ese momento, la interfaz de red tiene el acceso

bloqueado para tráfico normal, y lo único que admite es el tráfico EAPOL (EAP over LAN), que es el requerido para efectuar la autenticación.

• La estación de trabajo envía un mensaje EAPOL-Start al autenticador, indicando que desea iniciar el proceso de autenticación.

• El autenticador solicita a la estación que se identifique, mediante un mensaje EAP-Request/Identity.

• La estación se identifica mediante un mensaje EAP-Response/ Identity.

• Una vez recibida la información de identidad, el autenticador envía un mensaje RADIUS Access- Request al servidor de autenticación, y le pasa los datos básicos de identificación del cliente.

• El servidor de autenticación responde con un mensaje RADIUS Access-Challenge, en el cual envía información de un desafío que debe ser correctamente resuelto por el cliente para lograr el acceso.

Dicho desafío puede ser tan sencillo como una contraseña, o involucrar una función criptográfica más elaborada. El autenticador envía el desafío al cliente en un mensaje EAP-Request.

• El cliente da respuesta al desafío mediante un mensaje EAP-Response (Credentials) dirigido al autenticador. Este último reenvía el desafío al servidor en un mensaje RADIUS-Access-Response.

• Si toda la información de autenticación es correcta, el servidor envía al autenticador un mensaje RADIUS-Access-Accept, que autoriza al autenticador a otorgar acceso completo al cliente sobre el puerto, además de brindar la información inicial necesaria para efectuar la conexión a la red.

• El autenticador envía un mensaje EAP-Success al cliente, y abre el puerto de acuerdo con las instrucciones del servidor RADIUS.

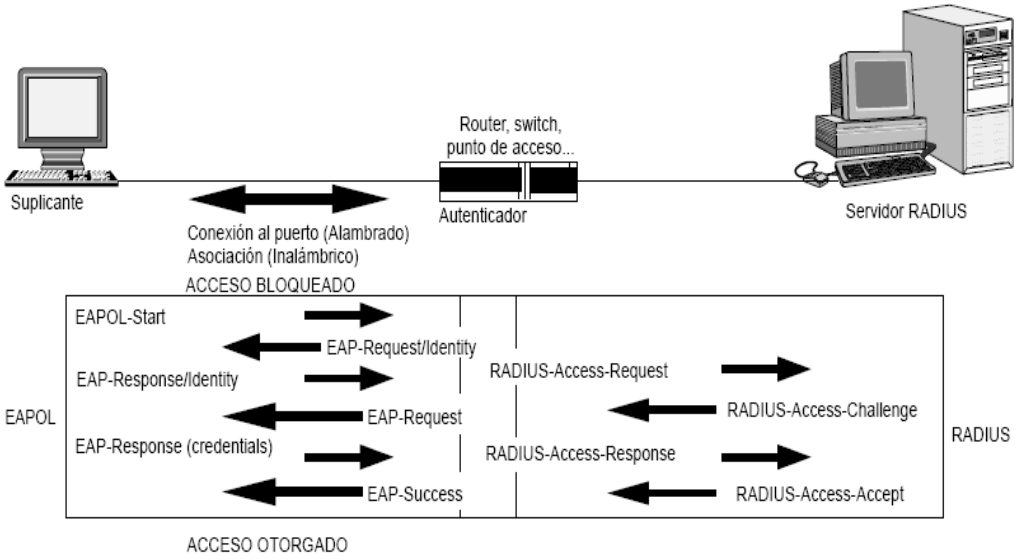


Figura 6. Diálogo EAPOL-RADIUS.

En el caso del acceso inalámbrico, el servidor RADIUS despacha en el mensaje RADIUS-Access-Accept un juego de claves WEP dinámicas, que se usarán para cifrar la conexión entre el cliente y el punto de acceso. El servidor RADIUS se encarga de cambiar esta clave dinámica periódicamente (por ejemplo, cada cinco minutos), para evitar el ataque de rompimiento de la clave descrito en la sección referente a WEP.

Existen varias variantes del protocolo EAP, según la modalidad de autenticación que se emplee. Se puede hablar de dos grupos de variantes: las que emplean certificados de seguridad, y las que utilizan contraseñas.

Las variantes de EAP que emplean certificados de seguridad son las siguientes:

• EAP-TLS: Requiere de instalación de certificados en los clientes y en el servidor. Proporciona autenticación mutua fuerte (es decir, el servidor autentica al cliente y viceversa) y soporta el uso de claves dinámicas para WEP. La sesión de autenticación entre el cliente y el autenticador se cifra empleando el protocolo TLS (Transparent Layer Substrate).

• EAP-TTLS: Desarrollada por Funk Software y Certicom. Proporciona servicios similares a EAP-TLS, con la diferencia de que requiere solamente la instalación de un certificado en el servidor.

Esto garantiza la autenticación fuerte del servidor por parte del cliente; la autenticación del cliente por parte del servidor se efectúa una vez que se establece la sesión TLS, utilizando otro método tal como PAP, CHAP, MS-CHAP ó MS-CHAP v2.

• PEAP: Desarrollado por Microsoft, Cisco y RSA Security. Funciona de manera parecida a EAPTTLS, en el sentido de que solamente requiere de certificado de seguridad en el servidor. Provee protección a métodos más antiguos de EAP, mediante el establecimiento de un túnel seguro TLS entre el cliente y el autenticador.

El empleo de certificados permite una autenticación fuerte entre cliente y servidor, sin embargo posee también varias desventajas:

• La administración de los certificados de seguridad puede ser costosa y complicada, especialmente en los esquemas donde se necesitan certificados en los clientes y en el servidor. Es necesario comprar los certificados a una autoridad de certificación (CA) conocida, o montar una CA propia.

• El diálogo de autenticación es largo.

Esto ocasiona que el proceso sea algo demorado, siendo especialmente molesto para usuarios que tienen que reautenticarse con mucha frecuencia (por ejemplo, usuarios en movimiento que cambien de un punto de acceso a otro).

• La manipulación del certificado puede ser engorrosa para el usuario.

En muchos casos se elige instalar el certificado en la terminal del usuario, con lo cual, si la terminal es robada y el certificado es el único nivel de seguridad que se posee, la seguridad de la red estaría en riesgo. Otra solución sería llevar el certificado en una tarjeta inteligente (smart card), lo que obligaría a instalar hardware adicional en las terminales para leer dichas tarjetas.

Las variantes de EAP que utilizan contraseñas son las siguientes:

• EAP-MD5: Emplea un nombre de usuario y una contraseña para la autenticación. La contraseña se transmite cifrada con el algoritmo MD5. Su gran inconveniente consiste en el bajo nivel de seguridad que maneja, ya que es susceptible a ataques de diccionario (un atacante puede ensayar a cifrar múltiples contraseñas con MD5 hasta que encuentre una cuyo texto cifrado coincida con la contraseña cifrada capturada anteriormente).

Además, el cliente no tiene manera de autenticar al servidor (no se podría garantizar que el cliente se está conectando a la red adecuada), y el esquema no es capaz de generar claves WEP dinámicas. Por estos problemas, EAP-MD5 ha caído en desuso.

• LEAP: Esta variante es propietaria de Cisco. Emplea un esquema de nombre de usuario y contraseña, y soporta claves dinámicas WEP. Al ser una tecnología propietaria, exige que todos los puntos de acceso sean marca Cisco, y que el servidor RADIUS sea compatible con LEAP.

• EAP-SPEKE: Esta variante emplea el método SPEKE (Simple Password-authenticated Exponential Key Exchange), que permite verificar que tanto cliente como servidor comparten una información secreta (en este caso, una contraseña) a través de un medio inseguro. Se ha comprobado que el método es muy seguro, aun con contraseñas cortas. Ofrece protección contra ataques de diccionario, así como el servicio de autenticación mutua sin necesidad de certificados. Muchos proveedores lo implementan por ser un método de autenticación robusto y sencillo.

- **WPA (WI-FI Protected Access)**

WPA es un estándar propuesto por los miembros de la Wi-Fi Alliance (que reúne a los grandes fabricantes de dispositivos para WLAN) en colaboración con la IEEE. Este estándar busca subsanar los problemas de WEP, mejorando el cifrado de los datos y ofreciendo un mecanismo de autenticación.

Para solucionar el problema de cifrado de los datos, WPA propone un nuevo protocolo para cifrado, conocido como TKIP (Temporary Key Integrity Protocol). Este protocolo se encarga de cambiar la clave compartida entre punto de acceso y cliente cada cierto tiempo, para evitar ataques que permitan revelar la clave. Igualmente se mejoraron los algoritmos de cifrado de trama y de generación de los IVs, con respecto a WEP.

El mecanismo de autenticación usado en WPA emplea 802.1x y EAP, que fueron discutidos en la sección anterior. Según la complejidad de la red, un punto de acceso compatible con WPA puede operar en dos modalidades:

• Modalidad de red empresarial: Para operar en esta modalidad se requiere de la existencia de un servidor RADIUS en la red. El punto de acceso emplea entonces 802.1x y EAP para la autenticación, y el servidor RADIUS suministra las claves compartidas que se usarán para cifrar los datos.
• Modalidad de red casera, o PSK (Pre-Shared Key): WPA opera en esta modalidad cuando no se dispone de un servidor RADIUS en la red. Se requiere entonces introducir una contraseña compartida en el punto de acceso y en los dispositivos móviles. Solamente podrán acceder al punto de acceso los dispositivos móviles cuya contraseña coincida con la del punto de acceso. Una vez logrado el acceso,
TKIP entra en funcionamiento para garantizar la seguridad del acceso. Se recomienda que las contraseñas empleadas sean largas (20 o más caracteres), porque ya se ha comprobado que WPA es vulnerable a ataques de diccionario si se utiliza una contraseña corta.
La norma WPA data de abril de 2003, y es de obligatorio cumplimiento para todos los miembros de la Wi-Fi Alliance a partir de finales de 2003. Según la Wi-Fi Alliance, todo equipo de red inalámbrica que posea el sello “Wi- Fi Certified” podrá ser actualizado por software para que cumpla con la especificación WPA.

Análisis y Monitoreo de Redes

Las redes de cómputo de las organizaciones, se vuelven cada vez más complejas y la exigencia de la operación es cada vez más demandante. Las redes, cada vez más, soportan aplicaciones y servicios estratégicos de las organizaciones. Por lo cual el análisis y monitoreo de redes se ha convertido en una labor cada vez mas importante y de carácter pro-activo para evitar problemas.

Anteriormente, cuando no se disponía de las herramientas que hoy existen, era necesario contratar a una empresa especializada para esta labor, con un costo muy elevado. Existen herramienta, que permiten, realizar esta importante labor, y contar un sistema experto como aliado que le ayuda en la interpretación de los

resultados obtenidos que se quedan con Ud. todo el tiempo y pasa a ser parte de su activo.

COMO SE INTEGRAN ESTAS HERRAMIENTAS DE ANÁLISIS Y MONITOREO DE REDES

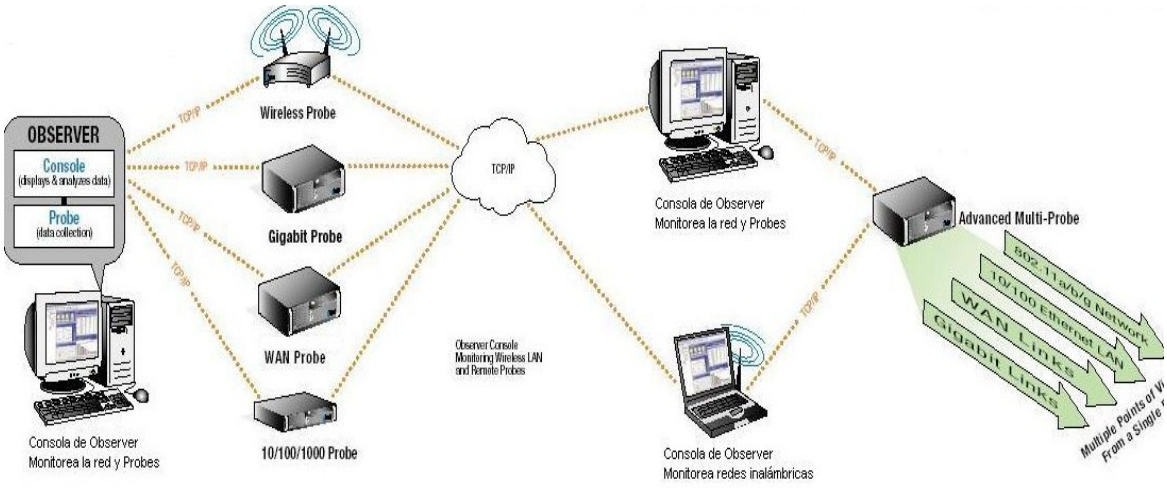


FIGURA 7. Herramientas de Análisis y Monitoreo

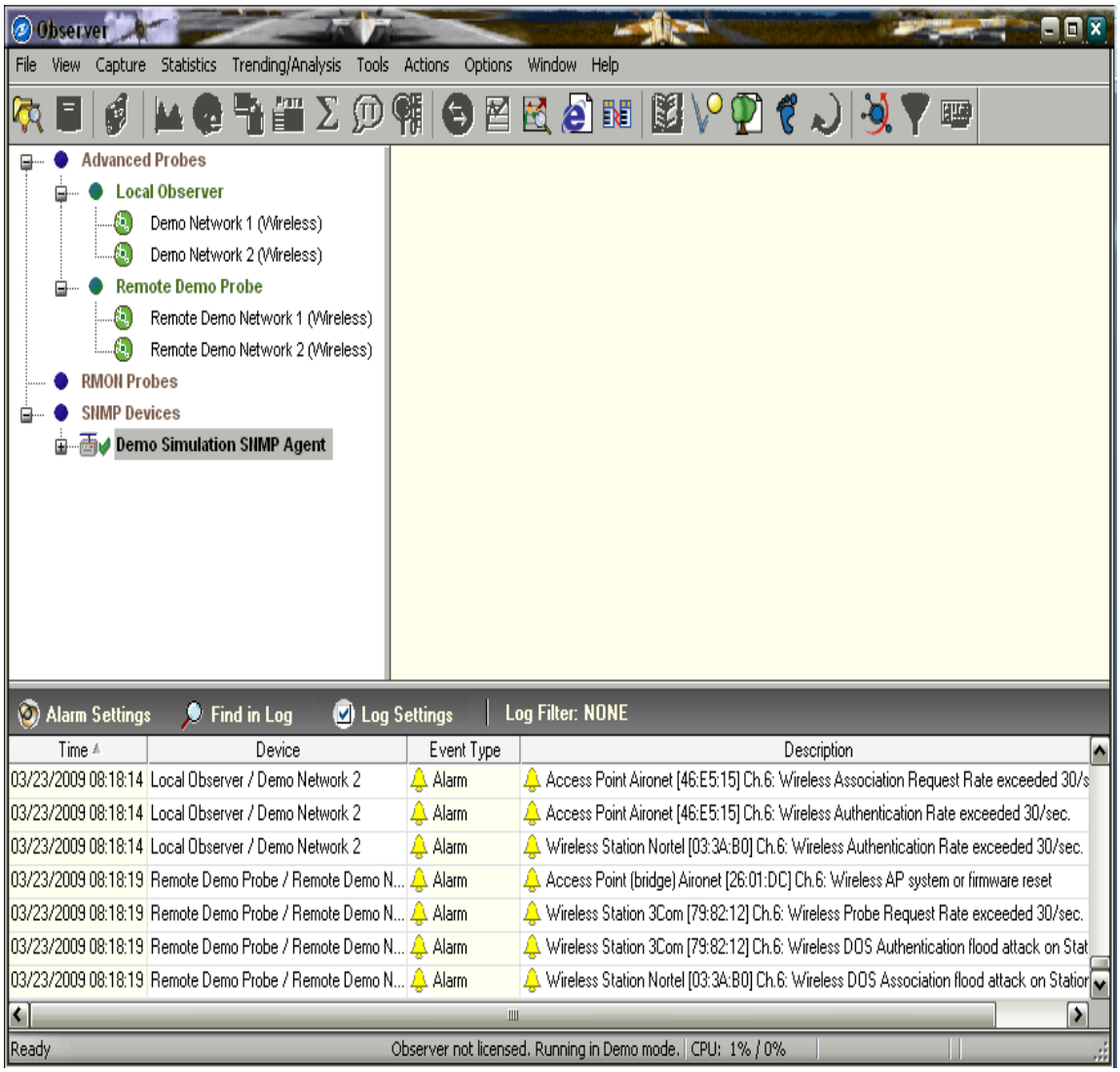
PASOS APROPIADOS PARA EL DESARROLLO DE ESTE SISTEMA

- El primer paso para el estudio y desarrollo de este proyecto fue analizar la infraestructura de la red inalámbrica y conocer los equipos que posee la empresa, también se conoció que seguridades dispone la misma.
- Una vez conocido esto se analizaron los protocolos de seguridad y con esto poder elegir el mejor método de análisis y monitoreo de la red de esta empresa.
- También se analizaron los herramientas de análisis y monitoreo, de esto se eligió un software que permite realizar las funciones necesarias para el monitoreo de la red inalámbrica para poder saber qué es lo que pasa en la misma.
- Por último se describirá las características y funciones que permite realizar el software elegido:

DEMOSTRACION DE SOFTWARE ELEGIDO PARA EL ANALISIS Y MONITOREO DE LA RED INALAMBRICA.

Una vez realizada la respectiva instalación de programa procedemos a ingresar al mismo, este le solicitara el tipo de red que necesita monitorear como muestra el grafico:

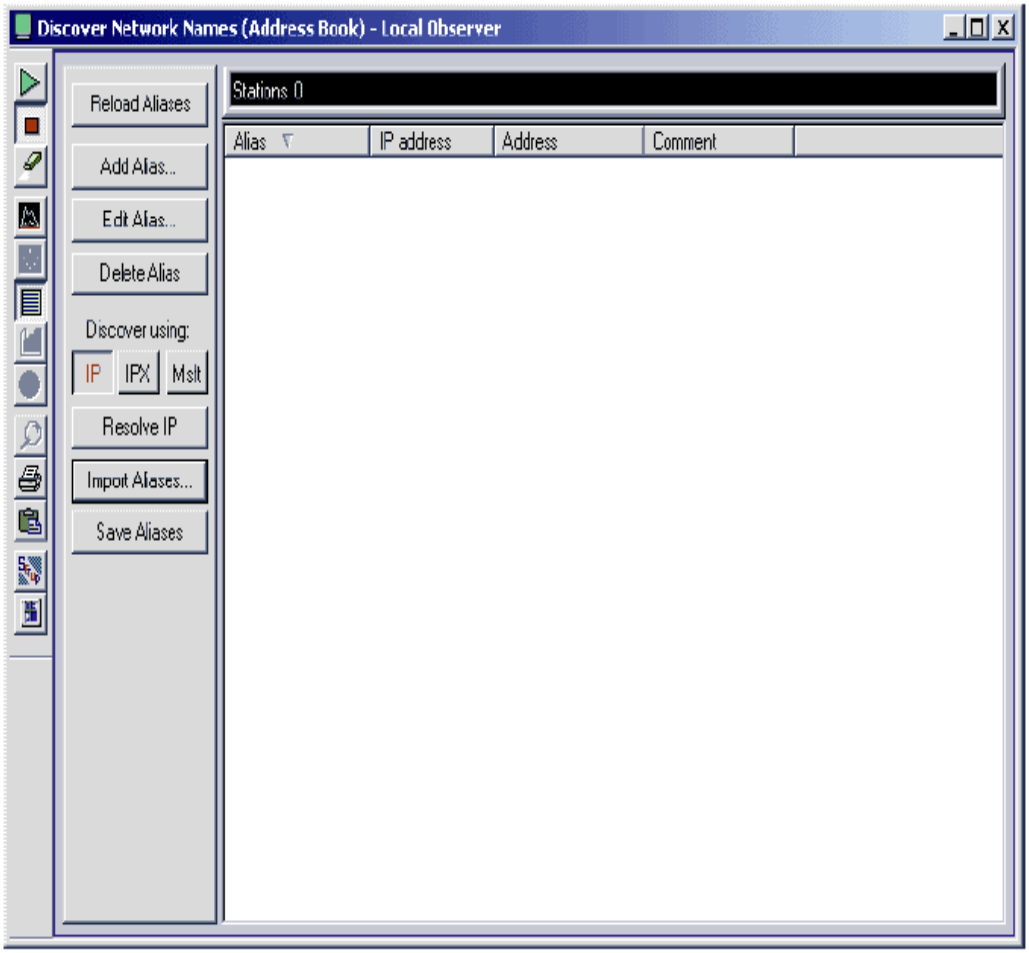
Luego presionamos OK para continuar y poder acceder al programa como se muestra en la figura:



Para realizar el mapeado de la red

Elegimos en la barra de herramientas **Tools -> Discover Network Names**:

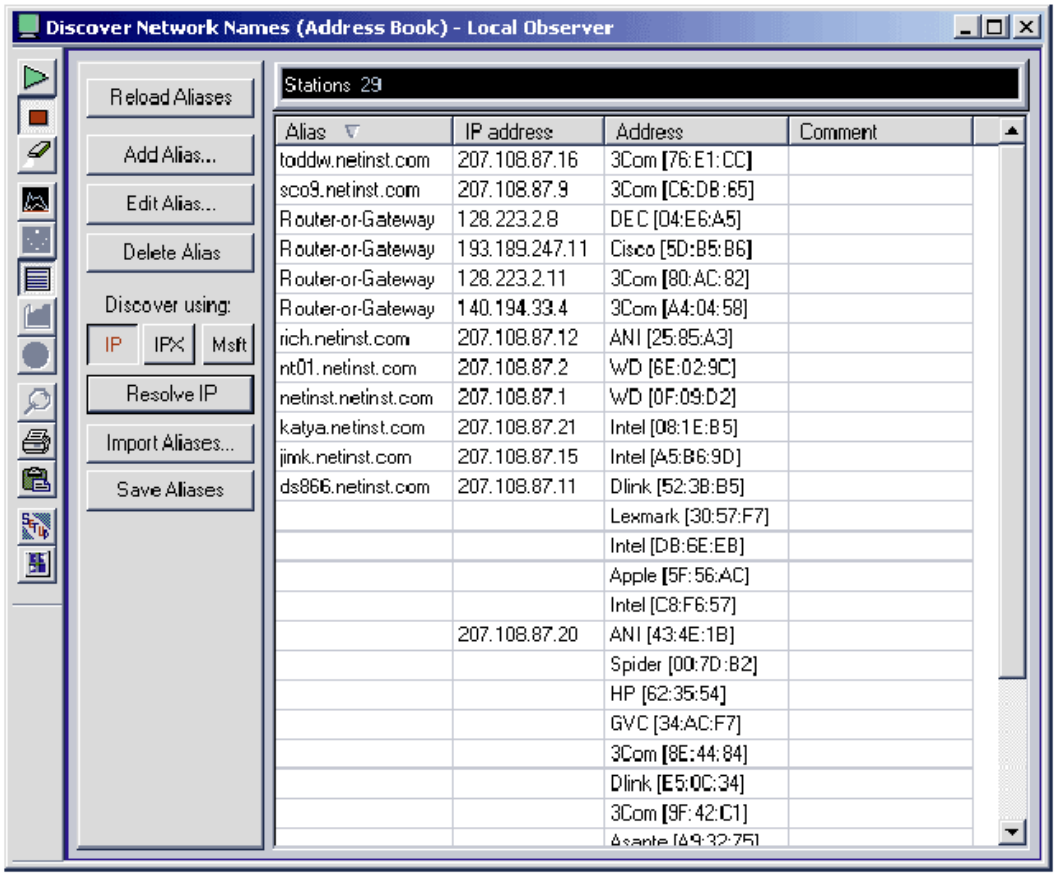
Antes de que Observer pueda decirle cualquier cosa sobre su red, necesita construir una tabla con los dispositivos que están conectados a su red, mapeando las MAC Address con 'Alias' con los cuales los identificaremos más fácilmente.



Seleccione el método de Discover Network Names. Las elecciones son IP, IPX (Novell) o Msft (Microsoft login name). En este ejemplo hemos elegido IP

Apriete el botón de Play 

. Si esta es la primera vez que ejecuta esta opción, una pantalla le preguntará por el rango de IPs a ser monitoreadas. Observer escanea su red en base a las MAC address, mostrando los dispositivos conforme los vaya encontrando como muestra la siguiente figura:



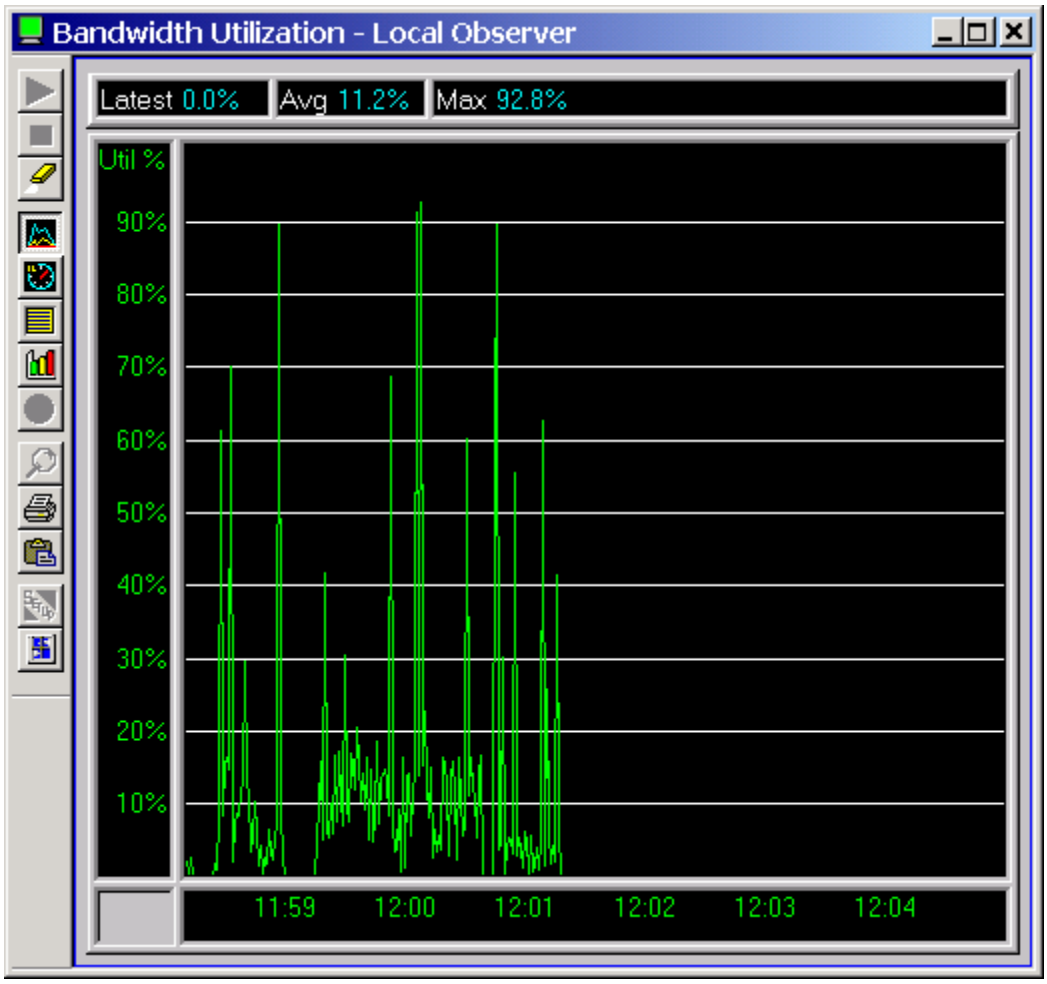
En este ejemplo, hemos elegido direcciones IP como método de búsqueda, estas direcciones IPs pueden ser resueltas a sus nombres DNS sólo tecleando el botón de Resolve IP. También, puede elegir Add, Delete o Edit alias para agregar, borrar o editar la lista de alias.

Elija el botón de Save Alias de tal modo que otras consultas tengan acceso a esta lista de dispositivos**.**

Cuanto ancho de banda estoy utilizando en la red.

Para saber cuánto ancho de banda estoy utilizando en mi red escojamos en la barra de herramientas la opción **Statistics->Bandwidth Utilization:** En la gráfica de utilización del ancho de banda (Bandwidth Utilization) nos permite fácilmente ver cuánto ancho de banda se está consumiendo por su tráfico de su red.

No es necesario elegir el botón de start, el modo de inicio (start) comienza automáticamente.



Interpretación de la gráfica

La utilización del ancho de banda, es calculada registrando el número de bytes vistos por Observer o la Sonda (Probe). Ejecutando esta gráfica varias veces en los momentos de carga normal, podrá darse una idea de la utilización "normal" de su red. Una vez que ha identificado lo que es "normal" para su red, esto será la llave para entender cualquier gráfica en el contexto correcto y con mayor facilidad podrá descubrir las anomalías cuando estas ocurran.

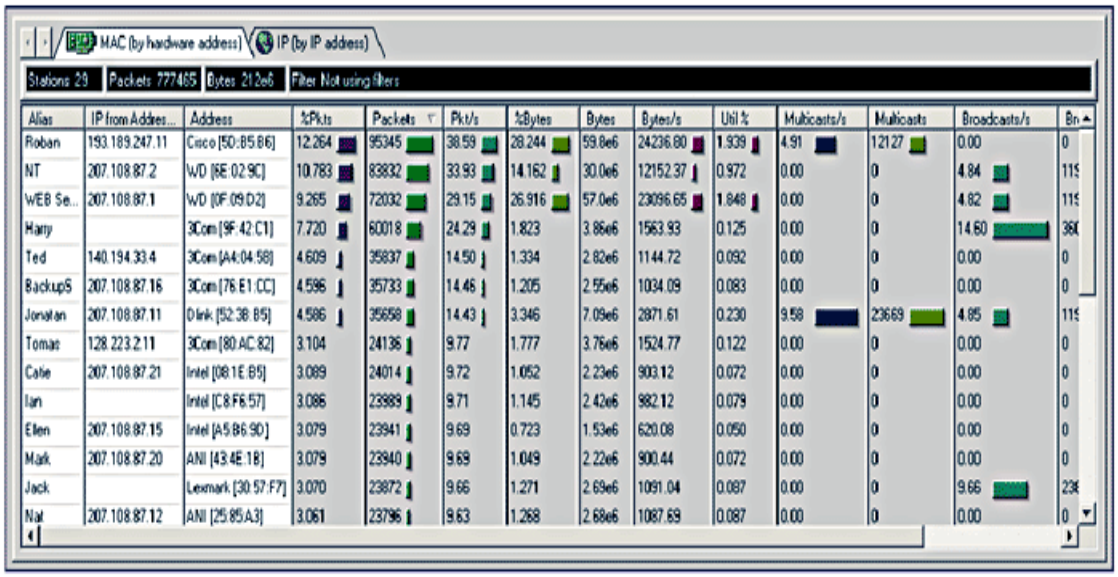
Para ver que dispositivos están utilizando más ancho de banda en la red

Escojamos la opción Statistics -> Top Talkers:

La gráfica de Top Talkers le permite ver quién está usando el mayor ancho de banda, esta gráfica le muestra al usuario, estación de trabajo o aplicación que está

consumiendo en exceso el ancho de banda. Identificando los patrones regulares de uso de la LAN, podrá detectar el dispositivo de la red que esté fallando y determinar qué porcentaje del ancho de banda están utilizando cada sistema en la red.

Iniciando la gráfica elija: **Statistics** -> **Top Talkers** y presione el botón de Play



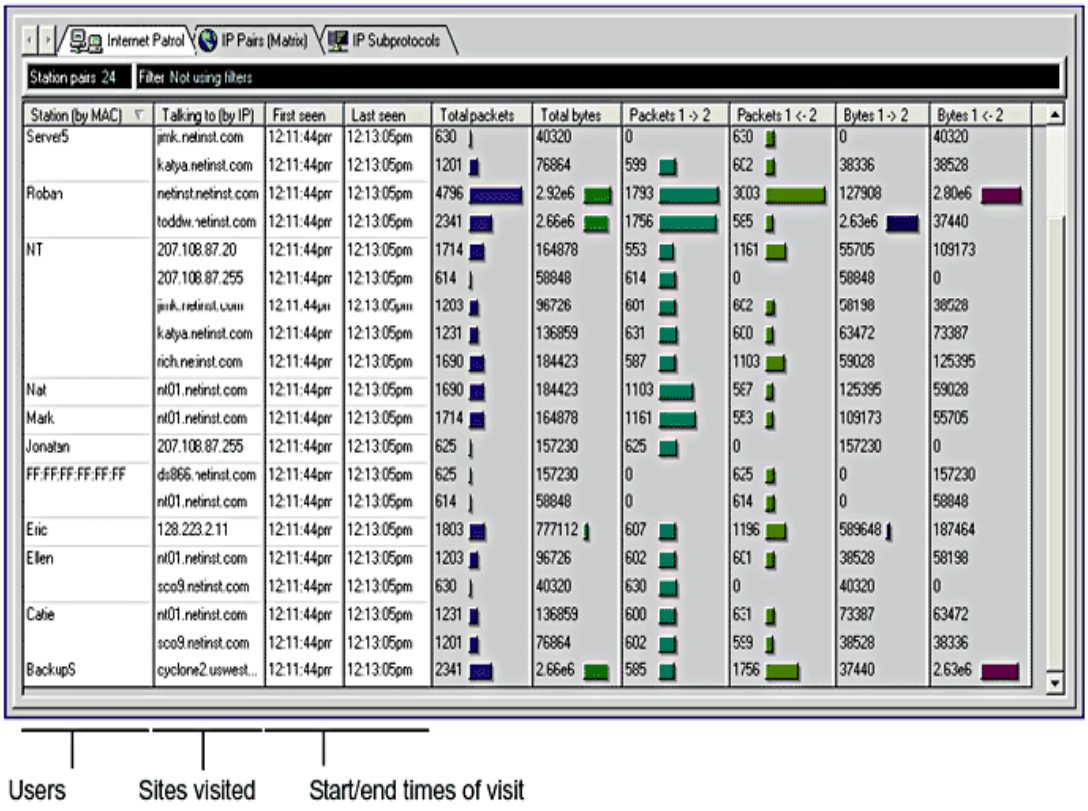
Interpretación de la gráfica.

Con la gráfica anterior, es posible identificar inmediatamente los dispositivos que están usando el mayor ancho de banda, Usted podría determinar si los sistemas que mas tráfico generan son los servidores (lo cual probablemente signifique que está bien) o estaciones de trabajo (lo cual podría indicar que existe un problema con el hardware o se trata de un uso indebido de una computadora). Usted puede iniciar un proceso de "packet capture" de cualquiera de las direcciones mostradas en la gráfica, seleccionando el registro y con un click en el botón derecho del ratón (mouse), para ver el detalle del tráfico generado por esa estación.

El uso de Internet está acaparando el ancho de banda

La pornografía que existe en Internet, la piratería de música y archivos de software no solamente atascan el ancho de banda de la red con tráfico no relacionado con su organización, también desgastan la productividad, exponen la red a virus y a posibles problemas legales. Con Observer es fácil ver donde están navegando los usuarios, cuanta información han descargado y que información fue.

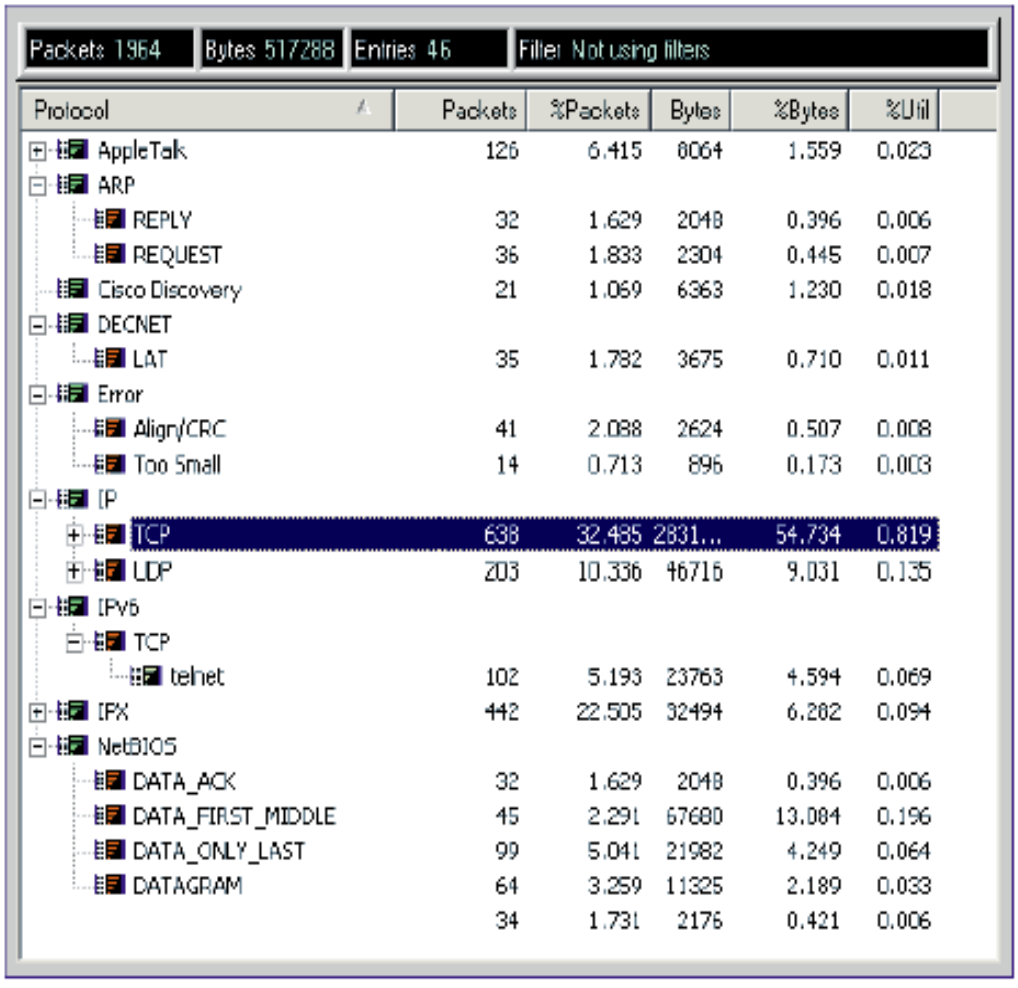
Para checar el uso de Internet elija: Statistics -> Internet Observer del menú principal. Como sucede con otras gráficas, presione el botón de "Play".



En la gráfica anterior, puede observar todas las páginas de internet por las cuales los usuarios están navegando. Ordene esta gráfica por usuarios, por los sitios visitados con los tiempos de inicio y terminación en cada sitio. Usted puede fácilmente darse cuenta si los usuarios hacen uso del internet en base a las políticas de su organización.

Que protocolos se están ejecutando en mi red

Impresoras enviando paquetes a la red de dispositivos Appletalk que no existen; ruteadores que envían mensajes de "broadcast" en protocolos que otros dispositivos no entienden. Son sólo dos ejemplos de dispositivos mal configurados que pudieran estar mal gastando el ancho de banda en su red. Con observer es fácil ver que protocolos están siendo usados en su red, y que dispositivos están utilizándolos.
Elija Statistics->Protocol Distribution y teclee el botón de "Play". Observer le mostrará un árbol de protocolos y subprotocolos que son utilizados en su red en ese momento.



Protocol	Packets	%Packets	Bytes	%Bytes	%Util
AppleTalk	126	6.415	8064	1.559	0.023
ARP					
REPLY	32	1.629	2048	0.396	0.006
REQUEST	36	1.833	2304	0.445	0.007
Cisco Discovery	21	1.069	6363	1.230	0.018
DECNET					
LAT	35	1.782	3675	0.710	0.011
Error					
Align/CRC	41	2.088	2624	0.507	0.008
Too Small	14	0.713	896	0.173	0.003
IP					
TCP	638	32.485	2831...	54.734	0.819
UDP	203	10.336	46716	9.031	0.135
IPV6					
TCP					
telnet	102	5.193	23763	4.594	0.069
IPX	442	22.505	32494	6.282	0.094
NetBIOS					
DATA_ACK	32	1.629	2048	0.396	0.006
DATA_FIRST_MIDDLE	45	2.291	67680	13.084	0.196
DATA_ONLY_LAST	99	5.041	21982	4.249	0.064
DATAGRAM	64	3.259	11325	2.189	0.033
	34	1.731	2176	0.421	0.006

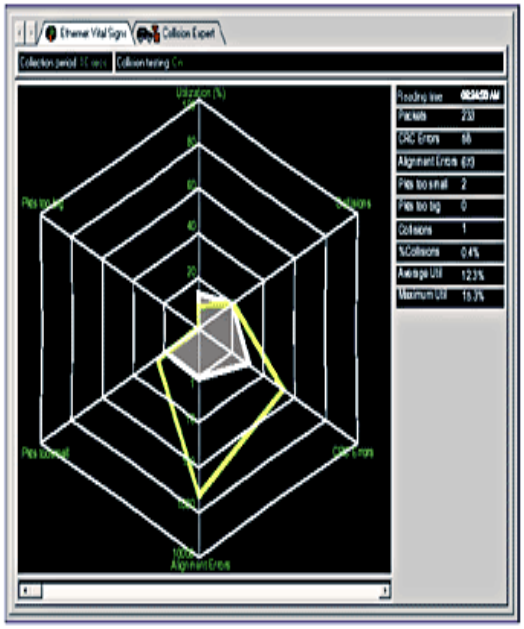
Usted puede contraer o expandir las ramas del árbol para ver los protocolos y subprotocolos. Las estadísticas le muestran el número de "bytes" brutos y el porcentaje de utilización para cada protocolo y subprotocolos. Identifique bps

protocolos que no debían estar utilizándose en su red. También puede ver si un protocolo inesperado está generando una inesperada cantidad de tráfico, lo cual podría indicar un problema de configuración de hardware o software.

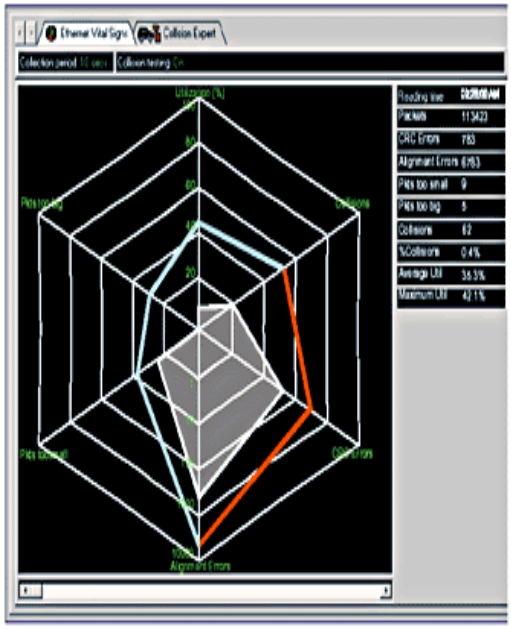
Como determinar la fuente de los errores

Observer ofrece excelentes herramientas para marcar y determinar la fuente de los errores CRC/Alineación (Bad CRC or Alignment Error) y errores del tamaño en su red. Observer le muestra un amplio resumen de la actividad de los errores en la red como signo vital. Usted puede utilizar la gráfica de Network Errors by Station (Errores en la red por estación de trabajo)" para determinar que dispositivo en su red está causando el problema de tal manera que tenga mejores posibilidades de investigar más a detalle.

Para obtener una amplia vista de la "salud" de la red junto con un resumen de los errores elija: Statistics->Network Vital Signs del menú principal de Observer. La gráfica inicia automáticamente. En la siguiente gráfica se muestra como se mostraría el cuadrante.



Network Idle



Trouble Developing

Esta gráfica le muestra las condiciones de error actuales de su red mapeadas contra el ancho de banda utilizado. La sombra gris nos muestra la lectura previa tomada inmediatamente antes de la lectura actual.

La forma y el color de la línea de la espiral le muestran todo en una solo gráfica, fácilmente reconozca la "firma" única de la actividad normal de su red.

- Aunque la forma "normal" de una red saludable es completamente variable, existen tres posibles estados generales de las líneas de la gráfica que representan: Todas las líneas en amarillo indican que no hubo suficiente actividad en la red para contar con una cuenta significativa de errores. En otras palabras, la red está básicamente inactiva.
- Todas las líneas en verde indican que la actividad de la red y la cuenta de errores están dentro del umbral de los valores que puede cambiar apretando el botón de "Display Properties".
- Una combinación de líneas rojas y azules significan problemas, las líneas rojas marcan una cuenta de errores arriba de los valores aceptables.

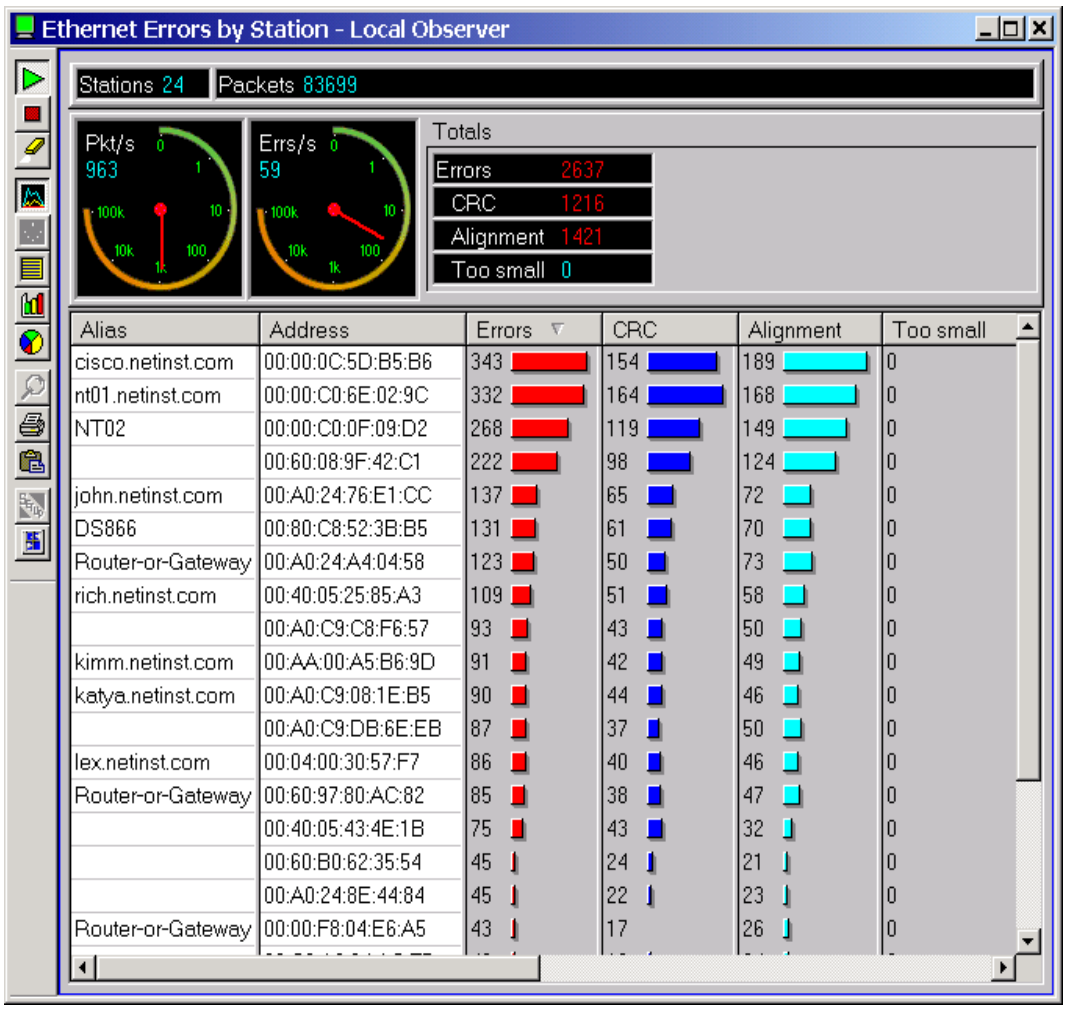
Los dos ejemplos anteriores, muestran la gráfica de dos redes. La primera muestra una red relativamente con poca actividad (todas las líneas en amarillo).

La segunda muestra algunos errores significativos involucrando errores de CRC y de alineación, pudiera desear investigar donde se están originando estos errores a través de la ejecución de la gráfica de "Network Errors by Station (Errores de Red por Estación de Trabajo)".

Una vez que se ha familiarizado con la "firma" de su red, usted estará en mejores posibilidades de notar inmediatamente picos de utilización y de error cuando estos ocurran. Si nota una inusual divergencia con su "firma" típica de su red, puede utilizar la gráfica de "Network Errors by Station (Errores de Red por Estación de Trabajo)" para localizar la fuente de la anormalidad.

Que dispositivos están generando errores en mi red

Para localizar los errores mostrados por las estadísticas de Observer, elija: Statistics->Network Errors by Station. Adelante, se muestra la estadística generada por esta aplicación.

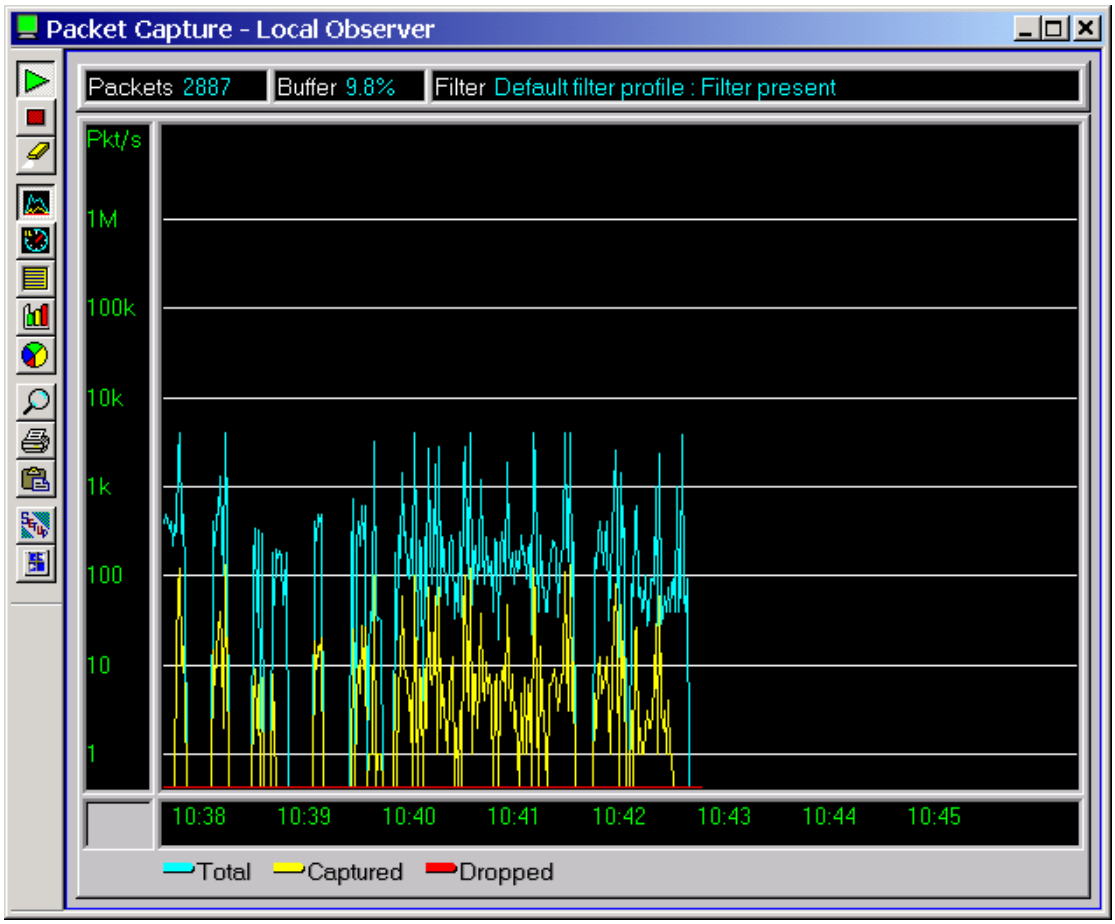


Como en las otras gráficas tabulares, puede seleccionar como ordenar la información y el criterio de selección sólo dando "click" en cualquiera de los encabezados de las columnas. Por ejemplo si hubiera detectado que los errores de CRC se están incrementando en su red y trata de investigar que dispositivo está generando la mayor cantidad de estos errores, sólo debe dar "click" en la columna de errores de CRC para ver esta estadística ordenando por los dispositivos que generen mayores errores de CRC.

En este punto, usted puede iniciar una captura de paquetes (packet capture) en cualquiera de los dispositivos conectados a la red sólo dando "click" en uno de ellos con el botón derecho del mouse, enseguida, se muestra el diálogo de

Para capturar y decodificar el tráfico de la red

Cada analizador de protocolos de red captura y decodifica el tráfico de la red. Iniciando la gráfica elija: Capture->Packet Capture del menú de Observer y presione el botón de play. La gráfica muestra la cantidad de tráfico que está siendo capturada.



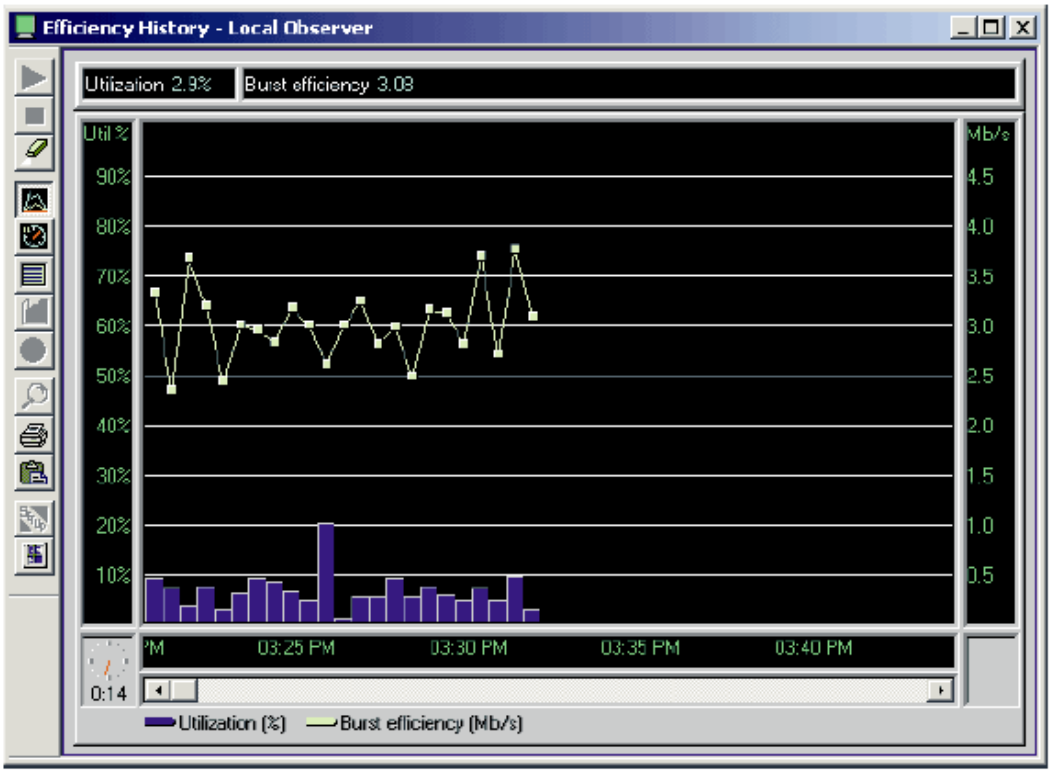
Las líneas en azul, muestran el número total de paquetes; las líneas amarillas, el número total de paquetes que son capturados. A menos que haya programado un filtro, la línea amarilla deberá cubrir a la línea azul. Esta es una manera de verificar que está capturando el tráfico que espera. La gráfica también muestra cualquier número de paquetes que se hayan extraviado durante la captura con una

línea en rojo). Los paquetes extraviados, significan que algo está mal con el sistema donde se ejecuta Observer. Ya sea que no sea lo suficientemente rápido como para manejar el tráfico o existe algún problema con la configuración.

Determinar si los cambios a la configuración han afectado

La historia de la eficiencia provee en una sola vista de la eficiencia actual de su red. Considere que esta gráfica genera una cantidad moderada de tráfico en la red.

Inicie la gráfica con Statistics->Efficiency History del menú de estadísticas. La gráfica inicia automáticamente

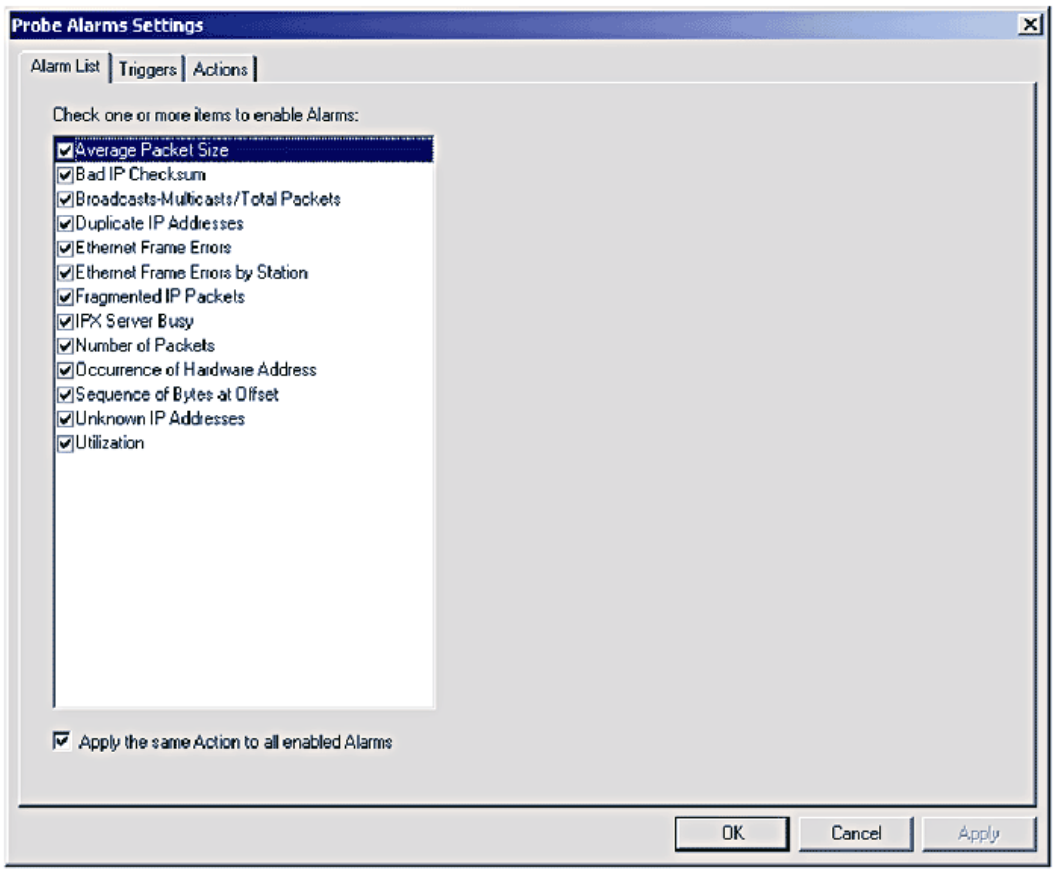


Como configurar para que me notifique de las distintas variaciones de las condiciones de la red

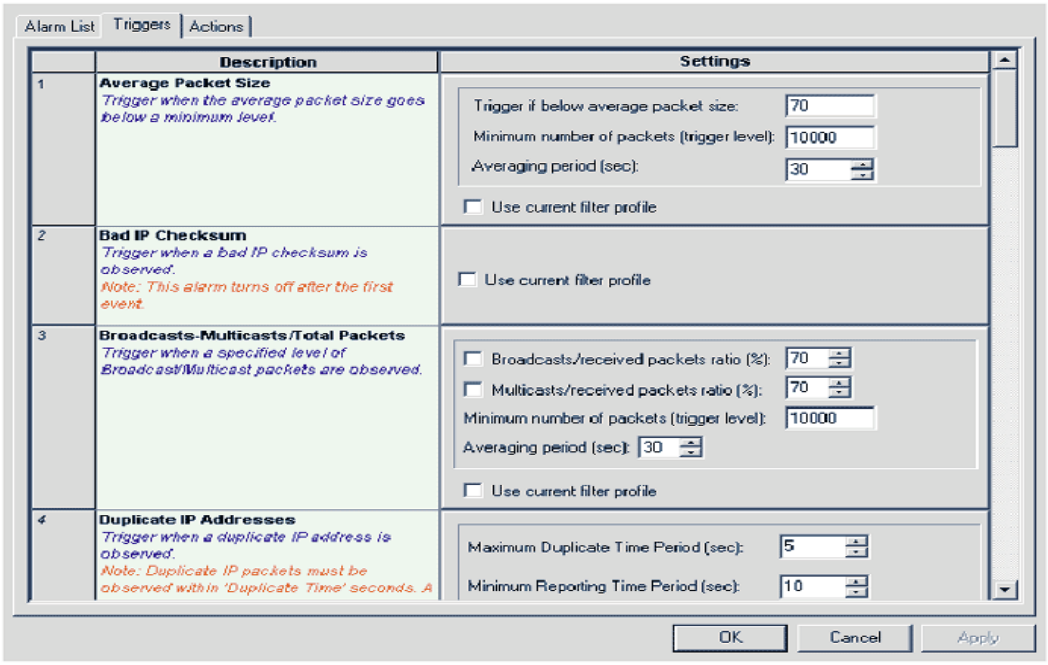
Observer puede configurarse para que automáticamente le notifique de errores y condiciones que podrían indicar un posible problema. Puede dejar que los mensajes se envíen a la consola o enviarlos por correo electrónico. Para programar el evento, selecciones Statistics->Triggers and Alarms del menú

principal.

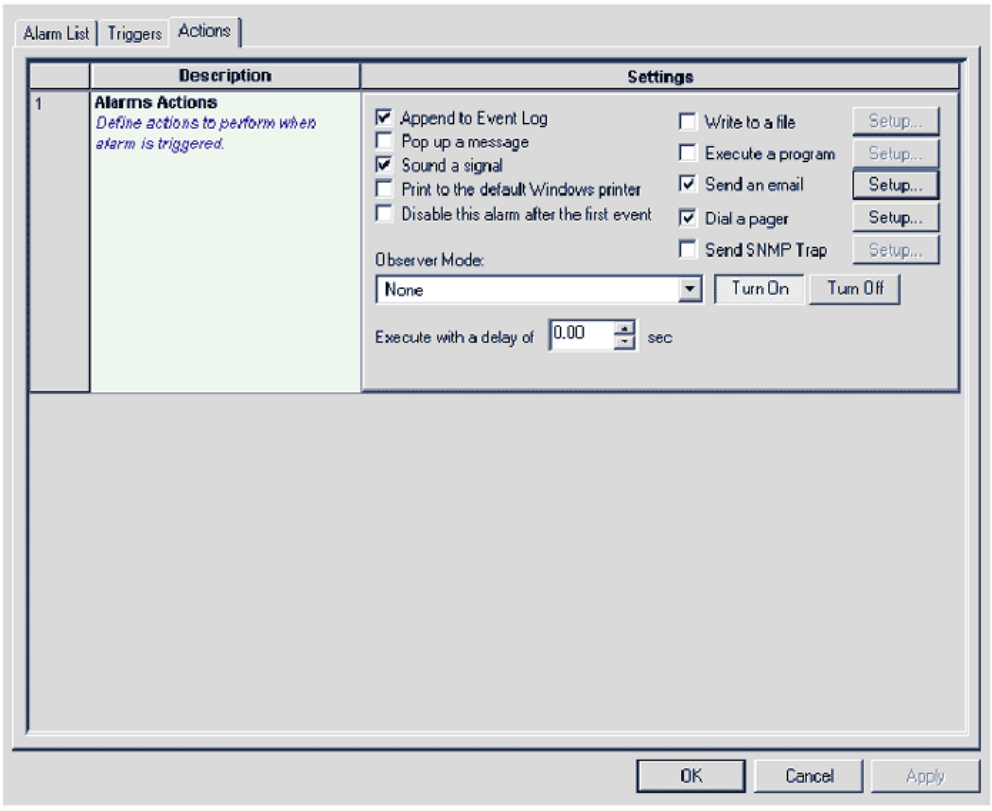
Presione el botón de Setup  para mostrar la lista de alarmas disponibles.



Elija las alarmas que están a la izquierda que quiera programar. Cuando haya terminado, elija la pestaña de eventos (Triggers) para programar los valores que 'dispararán' las alarmas elegidas.



Una vez que ha programado estos valores, presione la pestaña de Acciones (Actions) para especificar qué tipo de notificación o acción quiere que se 'dispare' cuando estos valores hayan sido excedidos.



Cuando haya terminado de especificar todas las 'pestañas' con los valores que haya elegido, presione el botón de OK para aplicar los valores y cerrar el diálogo. La ventana con el 'Log' de los eventos (Triggers) y alarmas (Alarms) se desplegará, la cual le mostrará cualquier actividad de Alarma tan pronto y como ocurra.

BENEFICIOS QUE PRESENTA EL ANÁLISIS Y MONITOREO DE LAS REDES INALÁMBRICAS.

- Determina inmediatamente la eficacia de los cambios de la red.
- Descifra protocolos.
- Filtrado de Información.
- Muestre los errores de Ethernet, del token ring y del FDDI por la estación.
- Puede monitorear desde un simple segmento hasta multisegmentos en redes LAN, Wireles LANs y WANs, una vez que se haya actualizado el software a las versiones más completas.

LO QUE PUEDE OBSERVAR Y OBTENER CON LAS HERRAMIENTAS DE ANÁLISIS Y MONITOREO DE REDES

- **Control de desempeño**
  - Revisa los signos vitales de su red en tiempo real
  - Analiza y da soporte las demandas de nuevas aplicaciones, como es VoIP.
  - Determina las tendencias de la red y por tanto predice las necesidades de incrementar la capacidad de sus equipos de manera planeada y con herramientas de modelaje.

- Obtenga mayor eficiencia de su red sin necesidad de aumentar el ancho de banda o de sus servidores.

- **Control de Múltiples Instalaciones**
  - Administra y controla redes remotas, con hardware o software sin necesidad de realizar gastos ostentosos de viaje.
  - Reporta simultáneamente a múltiples consolas del estado de su red.
  - Monitoree múltiples redes simultáneamente desde una consola.

- **Control de Solución de Problemas**
  - Responda a los asuntos que se presenten de manera rápida con un análisis unificado.
  - Mejora la atención a problemas en tiempo real.
  - Resuelva los problemas que se presenten tanto en las redes locales como en las remotas.
  - Administre la configuración de dispositivos locales y remotos con toda la funcionalidad de SNMP.

- **Control de Información**
  - Conserva y almacena datos de la red para manejar reportes y tendencias.
  - Vea y analice la red, así como el tráfico de la red a través del tiempo.
  - Monitoree el estado de la red en comparación a los reportes de análisis.

- Genere reportes sustentados para justificar las necesidades de actualización de la red.

MATERIALES DE REFERENCIA

BIBLIOGRAFIA

REFERENCIAS BIBLIOGRÁFICAS

- HUIDROBO M. José. "Redes y Servicios de Telecomunicaciones". Segunda Edición. España, Paraninfo SA 2000
- TANENBAUM, Andrew S. "Redes de Computadores". Cuarta edición. Prontica Hall, Hispanoamericana, SA México 2001.
- RANDALL K. NICHOLS – PANOS C. LEKKAS. Seguridad para Comunicaciones Inalámbricas.

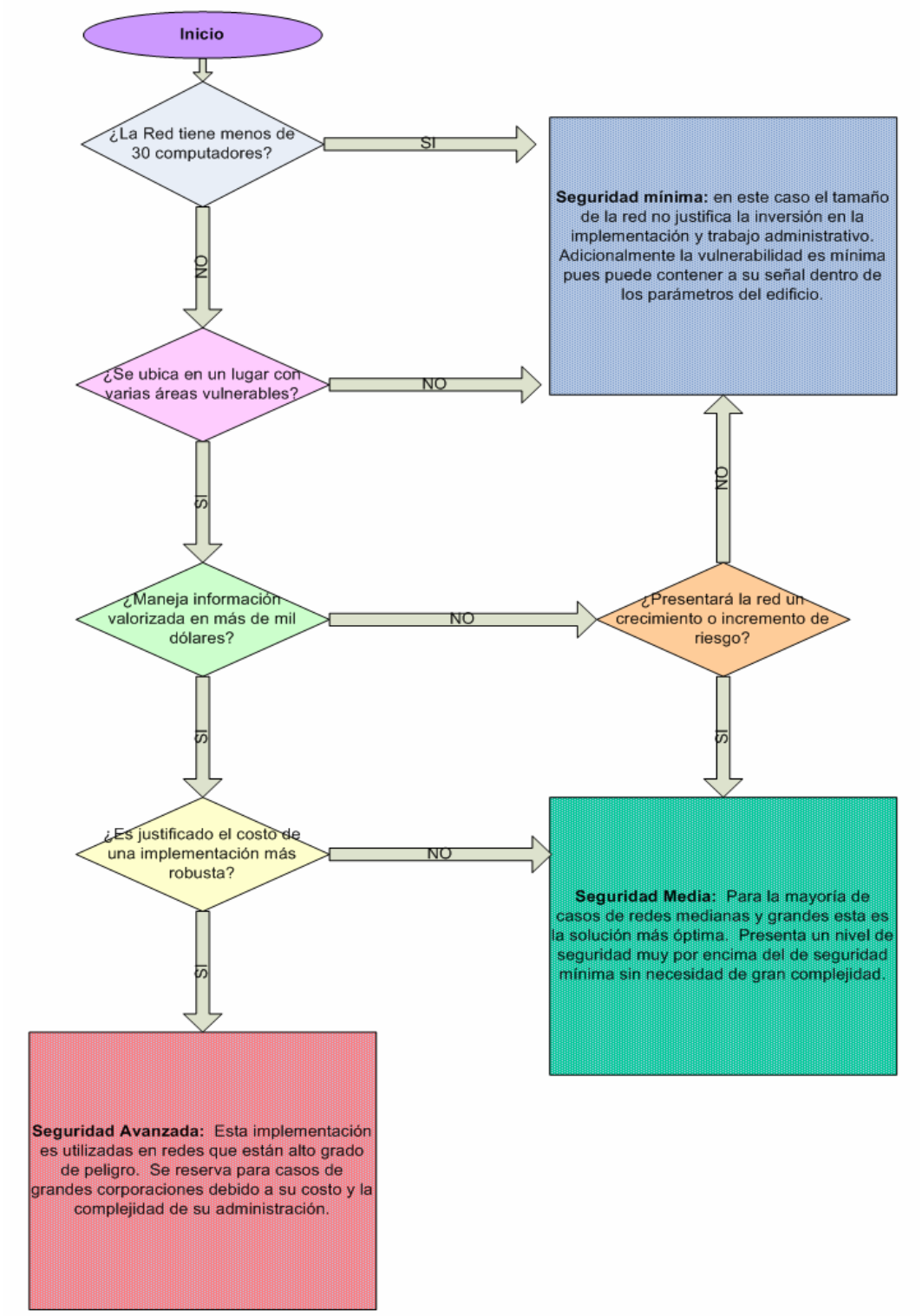
DIRECCIONES DE INTERNET

- www.ieee802.org
- http://es.wikipedia.org/wiki/Cable_coaxial
- http://es.wikipedia.org/wiki/Telecomunicaciónes
- www.cisco.com
- http://www.integracion-de-sistemas.com/analisis-y-monitoreo-de-redes/index.html#Que_es_posible_observar
- http://es.geocities.com/yeiko_6/

- http://www.atmforum.org
- http://lucypedrolucia.blog.dada.net/post/563957/MEDIOS+DE+TRANSMISION+GUIADOS
- http://www.ietf.org
- http://www.monografías.com/redesycomunicaciones
- http://es.wikipedia.org/wiki/redesycomputadoras
- http://www.atmforum.org/
- www.cisco.com
- http://www.atmforum.org
- http://www.ietf.org
- http://es.wikipedia.org/wiki/protocolosdered
- http://es.wikipedia.org/wiki/Point-toPoint_Protoco
- http://es.wikipedia.org/wiki/framerelay
- http://es.wikipedia.org/wiki/DECnet
- http://es.wikipedia.org/wiki/FDDI
- http://es.wikipedia.org/wiki/HDLC
- http://es.wikipedia.org/wiki/vozsobreip
- http://es.wikipedia.org/wiki/Comunicaci%C3%B3n_inal%C3%A1mbrica
- http://www.geocities.com/TimesSquare/Chasm/7990/clasific.htm
- http://www.monografías.com/rvozsobreip
- http://wilac.net/doc/tricalcar/materiales_abril2008/PDF_es/04_es_topologia-e-infraestructura_presentacion_v02.pdf

ANEXOS

Diagrama de flujo para selección de la implementación de seguridad



Herramientas de Análisis y Monitoreo de Redes (Hardware y Software)

Software para el Análisis y Monitoreo de Redes

Hardware para el análisis y monitoreo de redes de alta velocidad Gigabit y de redes WAN

Hardware Rackable para el análisis y monitoreo de redes de alta velocidad Gigabit y WAN

Interfaces especiales de hardware para cada necesidad