UNIVERSIDAD AMERICANA DE ACAPULCO

“EXCELENCIA PARA EL DESARROLLO”

FACULTAD DE INGENIERIA EN COMPUTACIÓN
INCORPORADA A LA UNIVERSIDAD NACIONAL
AUTÓNOMA DE MÉXICO

CLAVE. 8852 - 58

ESTUDIO Y ANÁLISIS DEL USO DE ANCHO DE BANDA EN LA RED DE LA DIRECCIÓN LOCAL GUERRERO DE LA COMISIÓN NACIONAL DEL AGUA

T E S I S

QUE PARA OBTENER EL TITULO DE :
INGENIERO EN TELECOMUNICACIONES
P R E S E N T A :

ROMMEL NORIEGA GUZMÁN

DIRECTOR DE TESIS: ING. JUAN CARLOS CAÑIZARES MACÍAS.

ACAPULCO, GRO. MARZO DEL 2008

AGRADECIMIENTOS

Gracias a Dios por haberme ayudado a encontrar la paz y la tranquilidad necesaria para superar cada uno de los problemas que he enfrentado a lo largo de toda mi vida.

Doy gracias a mi familia. A mis padres, por su amor, su apoyo y confianza que me han brindado para lograr alcanzar esta meta.

A mi asesor, el Ing. Juan Carlos Cañizares Macías por haberme brindado su apoyo y tomarse el tiempo necesario para corregirme y guiarme durante la realización de esta tesis.

Agradezco de forma especial a la Lic. Cristina García González, jefe del Depto. de Informática y Telecomunicaciones de la Dirección Local Guerrero de la CONAGUA; ya que con su ayuda y cooperación fue posible la realización de este proyecto.

A todos mis profesores, gracias por compartir sus conocimientos, brindarme su apoyo y comprensión durante mis estudios en esta institución.

ÍNDICE

AGRADECIMIENTOS.

INTRODUCCIÓN.

RESUMEN.

CAPITULO I. PRESENTACIÓN.

1.1. Planteamiento del problema 1
1.2. Justificación 2
1.3. Objetivo 3
1.4. Hipótesis 3
1.5. Alcances 4

CAPITULO II. MARCO TEORICO.

2.1. Descripción de redes 5
2.1.1. Topologías 8
2.1.2. Medios de transmisión 14
2.2. Ethernet 22
2.2.1. Historia 22
2.2.2. Objetivos de Ethernet 24
2.2.3. Características de Ethernet 25

2.2.4. Tipos de Ethernet 27
2.3. Internet 28
2.4. Intranet 32
2.4.1. ¿Para qué sirve? 33
2.4.2. Alcances operativos 34
2.4.3. Servicios para el usuario de Intranet 35
2.4.4. Ventajas de Intranet 35
2.5. Ancho de banda 36
2.6. Dependencia Federal Comisión Nacional del Agua 38
2.6.1. Misión 42
2.6.2. Visión 43
2.6.3. Estructura Orgánica 44
2.7. Infraestructura de la red de la Dirección Local Guerrero de la C. N. A. 45
2.7.1. Servicios 47
2.7.2. Página de Intranet 49

CAPITULO III. GESTIÓN DE REDES.

3.1. Gestión de redes 55
3.1.1. ¿Qué es Gestión de Redes? Necesidad de la Gestión 55
3.2. Sistemas de Gestión. Clasificación 58
3.3. Tipos de Gestión 61
3.3.1. Gestión de la contabilidad 61
3.3.2. Gestión de la seguridad 63
3.4. Herramientas de Gestión 68

3.4.1. Tipos de herramientas 69
3.4.2. Equipos de pruebas de cableado 70
3.4.3. Monitoreo de red 71
3.4.4. Analizador de red 72
3.4.5. Analizadores de protocolos 73

CAPITULO IV. SOFTWARE DE MONITOREO.

4.1. Prueba y evaluación de las herramientas del software de monitoreo de las redes de computadoras 76
4.1.1. Monitoreo de computadoras 78
4.1.2. Monitoreo en capas 81
4.1.3. Agentes integrados 82
4.1.4. Agentes externos 86
4.1.5. Parámetros de evaluación 88
4.2. Monitorizadores de red 89
4.2.1. Observer 89
4.2.2. Ethereal 91
4.2.3. Capsa 96
4.3. Software de monitoreo seleccionado 102

CAPITULO V. MONITOREO EN LA RED DE LA DIRECCIÓN LOCAL GUERRERO DE LA C. N. A.

5.1. Monitoreo en la red de la Dirección Local Guerrero de la C. N. A. 103

5.2. Páginas más visitadas 104
5.2.1. Las 10 páginas más vistas 107
5.3. Páginas visitadas con contenido para adultos 109
5.4. Accesos a Internet por área 112
5.5. Accesos a Intranet por área 114
5.6. Páginas accesadas por día 116

CAPITULO VI. POSIBLES SOLUCIONES.

6.1. Posibles soluciones 118
6.1.1. PacketShaper y Sitara 118
6.2. PacketShaper 119
6.2.1. Detecta y clasifica las aplicaciones de red 120
6.2.2. Analiza la conducta de la red 120
6.2.3. Refuerza el reparto del ancho de banda basado en Políticas 121
6.2.4. Realiza informes de funcionamiento de las Aplicaciones 122
6.3. Sitara 124
6.3.1. QoSWorks 124
6.3.2. Características de QoSWorks 126
6.3.3. Política inteligente de Web Caching 126
6.3.4. Administrador de tráfico Sitara AccúRate 128
6.3.5. La solución QoSWorks 130
6.3.6. Clasificación Wire-Speed 131
6.3.7. Política de administración flexible e intuitiva 132

6.3.8. Monitorización y obtención de informes en tiempo real 133
6.4. Equipo seleccionado 134

CAPÍTULO VII. CONCLUSIONES Y RECOMENDACIONES.

7.1. Conclusiones 135
7.2. Recomendaciones 137

ANEXOS

GLOSARIO 139
BIBLIOGRAFIA 145

INTRODUCCION

Con la creación de redes de computadoras, el compartir información y el uso de los servicios que brindan las redes permiten una mejora en el desempeño de las actividades de los usuarios, pues se coordinan esfuerzos a grandes distancias. Los primeros pasos fueron lograr la comunicación entre varios equipos de cómputo dentro de un mismo edifico de una empresa o institución, posteriormente el uso de las redes se volvió común para las instituciones, y el alcance de las redes se incrementó con el desarrollo de la tecnología, por lo que ahora las redes de una empresa o dependencia, pueden abarcar un conjunto de edificios o inclusive conectar oficinas o edificios en diferentes países y continentes.

Hoy se habla de Internet, la red de redes, de las intranets de muchas instituciones, inclusive de las redes en casa u oficinas. Estos tipos de redes tienen un objetivo común que es el permitir el intercambio de información y el brindar servicios como compartir archivos, correo electrónico, etc. Todo esto con el fin de permitir un mejor desempeño de las actividades diarias de las personas.

En la Comisión Nacional del Agua, El director y los subdirectores utilizan Internet para enviar instrucciones, disposiciones, acciones a tomar a la Dirección Local Guerrero y/o cualquiera de las otras direcciones locales del país.

La Dirección Local Guerrero utiliza Internet para enviar al director y los subdirectores de la CONAGUA avances de obras, estimaciones, soluciones a las instrucciones recibidas e intercambio de información con la Dirección General, Direcciones de Organismos de Cuencas.

Las redes han ido evolucionando con los avances tecnológicos, desde sus arquitecturas y topologías, así como los servicios que se han ido generando, por ejemplo, la Comisión Nacional del Agua cuenta con el servicio de videoconferencias, las cuales son utilizadas para dar información de los diferentes programas, revisión de las actividades que se desarrollan e informar al personal de nuevas disposiciones. Esta aplicación requiere un uso considerable del ancho de banda de la red, pues las transmisiones de audio y video generan mucho más paquetes que el envío de texto e imágenes; además de que, para garantizar un buen desempeño de estas aplicaciones, se necesita que el envío de paquetes sea a una tasa de transferencia constante. El uso de estas aplicaciones y los volúmenes de información tanto laborales como personales generan un gasto de ancho de banda.

No es suficiente el tener una red con la mejor tecnología, es necesario saber administrar de manera correcta, equitativa y eficiente los recursos con los que cuenta la red.

RESUMEN

Los temas a abordar en la siguiente tesis, tienen por objetivo el estudio del monitoreo de redes, por lo que a continuación se describen los capítulos que la conforman.

En el capítulo II se describe los conceptos básicos para esta tesis, estos temas son: Descripción de redes, en el cual se dará a conocer ¿Cómo funciona una red?, ¿Qué propósitos tiene una red?, Medios de transmisión, entre otros. Otro tema de importancia es el Internet, se dará a conocer: ¿Cómo surgió?, ¿Por qué surgió?, ¿Qué es? Y ¿Cómo funciona?. Intranet y Ancho de Banda son temas incluidos en este trabajo como parte del marco teórico. Se dará conocer los principios, misión, visión, facultades, página de intranet de la Comisión Nacional del Agua, así como la estructura de la red de la Dirección Local.

En el capítulo III se explica el concepto de gestión de redes, los tipos de gestión existentes, las herramientas de gestión, tales como: Equipos de pruebas de cableado, Monitoreo de red, analizador de red y analizador de protocolo, en este caso se utilizará el monitoreo de red.

El capítulo IV se abordan como se realizan las pruebas y evaluaciones a los software de monitoreo. En este capítulo se escogió el software que cumplió con las características deseadas para que los datos que se muestran fueran confiables para el estudio.

Las estadísticas obtenidas con el software elegido se muestran en el capítulo V, se analizaron para dar solución al problema planteado.

Ya en el capítulo VI se muestran posibles soluciones para mejorar el gasto de ancho de banda.

CAPITULO I. PRESENTACIÓN.

1.1. PLANTEAMIENTO DEL PROBLEMA.

La red de la Dirección Local Guerrero de la Comisión Nacional del Agua ofrece servicios como telefonía IP, Videoconferencias, correo electrónico, Internet entre otros. Pero que tanto se usan estos servicios y con que fines. Un ejemplo es el uso de la Internet, donde el uso de dicho recurso debe ser con fines laborales y de consulta. El uso de algunas aplicaciones como la mensajería instantánea puede utilizarse en forma inadecuada, pues permite tanto la opción de comunicarse con otras personas relacionadas a un proyecto de trabajo, como para comunicarse con amigos para fines personales. La opción de descargar archivos de Internet, es otra situación en la que se tiene incertidumbre de las intenciones del usuario, pues tanto se puede bajar información necesaria para actividades laborales como información de uso personal; los cuales pueden contener virus, que pueden afectar el buen funcionamiento de la red. El uso de los servicios de la red genera competencia por el ancho de banda, es por eso la necesidad de conocer si en realidad estos recursos son únicamente para laborar o no.

De lo anterior se desprende el siguiente cuestionamiento:

¿Cómo verificar el gasto del ancho de banda de la red de la Dirección Local Guerrero de la Comisión Nacional del agua en Chilpancingo, Gro.?

1.2. JUSTIFICACIÓN.

El uso de redes que comuniquen a todos los equipos de cómputo es un área determinada es ya una práctica común desde hace varias décadas. Estas redes permiten el intercambio de información y el brindar servicios específicos tales como compartir archivos, correo electrónico, etc. Todas estas aplicaciones requieren un uso en mayor o menor medida del ancho de banda, donde la competencia de este recurso se mide en términos de considerables factores, como el número de usuarios conectados a la red, la capacidad de los dispositivos de red para manejar el flujo de información y el tipo de servicios que se solicitan a la red. Por lo tanto el ancho de banda juega un papel fundamental en el desempeño de la red.

Su importancia radica en que es un recurso finito y en un momento dado, los usuarios y las aplicaciones que se trabajen puede generar que la transferencia de información se ejecute a velocidades por debajo de la capacidad de la red y la disponibilidad de los servicios se ve afectada.

Un estudio de la red de la Dirección Local Guerrero de la Comisión Nacional del Agua permitirá conocer el uso del ancho de banda, para posteriormente decidir si es necesario mejorar la red en todos sus aspectos (infraestructura y aumento de ancho de banda, en caso de que se requiera).

1.3. OBJETIVO.

El objetivo que persigue este proyecto, es analizar la utilidad que se le da al ancho de banda de la red de la Dirección Local Guerrero de la Comisión Nacional del Agua en Chilpancingo, Gro., utilizando herramientas que hagan posible esta labor. Una vez teniendo las estadísticas se buscará posibles soluciones que sean favorables para cumplir con la optimización del ancho de banda.

1.4. HIPÓTESIS.

Dar uso de la red con fines personales puede disminuir el desempeño de la red y ocasionar problemas a todos los usuarios que también utilicen dicha red. En cuanto al uso de aplicaciones hace que el ancho de banda vaya en incremento, lo cual provocará la disminución de su capacidad de respuesta a las peticiones de servicio por parte de los usuarios que sí utilicen la red con fines de la Dirección Local Guerrero.

Con el uso de monitorizadores de red, se puede detectar las aplicaciones a las cuales ingresan los usuarios de una red, así tomar las medidas necesarias para mejorar el uso de esta.

El análisis de gasto del ancho de banda permitirá conocer la situación real del uso de la red.

1.5. ALCANCES.

- Se realizará un análisis de la red de la Dirección Local Guerrero de la Comisión Nacional del Agua en Chilpancingo, Gro.
- Se conocerá el uso que se le da al ancho de banda, en base a los resultados obtenidos del análisis.
- Se mostrará la utilidad del ancho de banda en forma de estadísticas.
- Se darán a conocer propuestas que mejoren el uso del gasto del ancho de banda de la Dirección Local Guerrero de la Comisión Nacional del Agua en Chilpancingo, Gro.

CAPITULO II. MARCO TEORICO.

2.1. DESCRIPCIÓN DE REDES.

Una red es una interconexión de dos o más computadoras con el propósito de compartir información y recursos a través de un medio de comunicación.

Las primeras redes de datos se basaban en una arquitectura mainframe (figura 1) con terminales muy sencillos conectados remotamente.

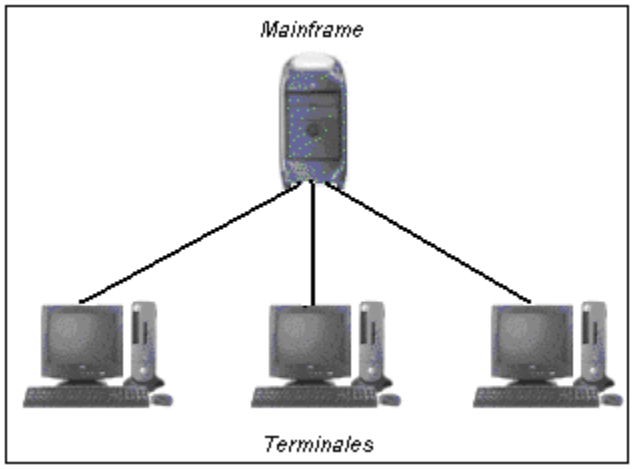


Fig. 1 Arquitectura Mainframe

La justificación de las soluciones de este tipo es bastante obvia: los primeros ordenadores resultaban muy caros y aparatosos como para que cada empleado de una empresa dispusiera de uno propio.

No sería hasta la desarrollo del PC (Personal Computer) cuando empezó a plantearse la dotación de inteligencia a los puestos de usuario.

Las redes en general, consisten en “compartir recursos”, y uno de sus objetivos es hacer que todos los programas, datos y equipo estén disponibles para cualquiera de la red que así lo solicite, sin importar la localización física del recurso y del usuario. En otras palabras, el hecho de que el usuario se encuentra a 1000 kilómetros de distancia de los datos, no debe evitar que este los pueda utilizar como si fueran originados localmente.

La comunicación de datos se ha convertido en una parte fundamental de la computación. Las redes globales reúnen datos sobre diversos temas, como las condiciones atmosféricas, la producción de cosechas o el tráfico aéreo. En el mundo científico, las redes de datos son esenciales pues permiten a los científicos enviar programas de datos hacía supercomputadoras remotas para sus procesamientos, recuperar los resultados e intercambiar información con sus colegas.

La mayor parte de las redes son entidades independientes, establecidas para satisfacer las necesidades de un solo grupo. Los usuarios escogen una tecnología de hardware apropiada a sus problemas de comunicación. De manera más importante es imposible construir una red universal desde una sola tecnología de hardware debido a que ninguna red satisface todas las necesidades de uso. Algunos usuarios necesitan una red de alta velocidad para conectar

máquinas, pero dichas redes no se pueden expandir para abarcar grandes distancias. Otros establecen una red de menor velocidad que conecta máquinas que se encuentran a miles de kilómetros de distancia.

Durante los pasados 20 años, ha evolucionado una nueva tecnología que hace posible interconectar muchas redes físicas diferentes y hacerlas funcionar como una unidad coordinada. Esta tecnología, llamada internetworking, unifica diferentes tecnologías de hardware subyacentes al proporcionar un conjunto de normas de comunicación y una forma de interconectar redes heterogéneas. La tecnología de red de redes oculta los detalles del hardware de red y permite que las computadoras se comuniquen de forma independiente de sus conexiones físicas de red.

Una red de redes consiste en un grupo de redes conectadas que actúan como un todo coordinado.

Si se realiza una conexión entre una computadora y otra o entre terminales y computadoras, la comunicación entre redes puede dividirse en dos tipos básicos: de circuitos conmutados y por conmutación de paquetes.

Las redes conmutadas de circuitos operan formando una conexión dedicada (circuito) entre dos puntos. Las redes de conmutación de paquetes, normalmente utilizadas para conectar computadoras funcionan de manera completamente diferente que las

conmutadas por circuitos. En una red de conmutación de paquetes, la información es transferida a través de la red divididas en pequeñas unidades llamadas paquetes que son multiplexados en conexiones entre maquinas.

2.1.1. Topologías.

Los diferentes componentes que van a formar una red se pueden interconectar o unir de diferentes formas, siendo la forma elegida un factor fundamental que va a determinar el rendimiento y la funcionalidad de la red. La disposición de los diferentes componentes de una red se conoce con el nombre de topología de la red. La topología idónea para una red concreta va a depender de diferentes factores, como el número de máquinas a interconectar, el tipo de acceso al medio físico que deseemos, etc.

Podemos distinguir tres aspectos diferentes a la hora de considerar una topología:

1. La topología física, que es la disposición real de las máquinas, dispositivos de red y cableado (los medios) en la red.

2. La topología lógica, que es la forma en que las máquinas se comunican a través del medio físico. Los dos tipos más comunes de topologías lógicas son broadcast (Ethernet) y transmisión de tokens (TokenRing).

3. La topología matemática, mapas de nodos y enlaces.

La topología de broadcast simplemente significa que cada host envía sus datos hacia todos los demás hosts del medio de red. Las estaciones no siguen ningún orden para utilizar la red, sino que cada máquina accede a la red para transmitir datos en el momento en que lo necesita. Esta es la forma en que funciona Ethernet.

En cambio, la transmisión de tokens controla el acceso a la red al transmitir un token eléctrico de forma secuencial a cada host. Cuando un host recibe el token significa que puede enviar datos a través de la red. Si el host no tiene ningún dato para enviar, transmite el token hacia el siguiente host y el proceso se vuelve a repetir.

Las principales modelos de topología son:

Topología de bus: La topología de bus (figura 2) tiene todos sus nodos conectados directamente a un enlace y no tiene ninguna otra conexión entre nodos. Físicamente cada host está conectado a un cable común, por lo que se pueden comunicar directamente, aunque la ruptura del cable hace que los hosts queden desconectados.

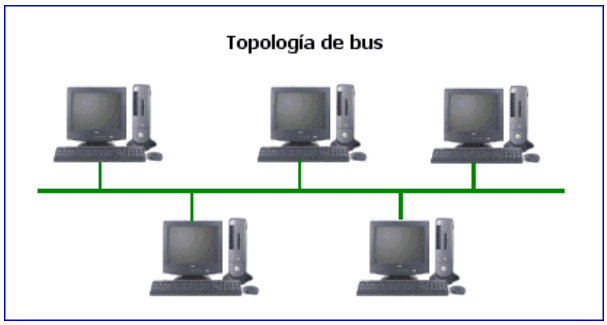


Fig. 2 Topología de bus

La topología de bus permite que todos los dispositivos de la red puedan ver todas las señales de todos los demás dispositivos, lo que puede ser ventajoso si desea que todos los dispositivos obtengan esta información. Sin embargo, puede representar una desventaja, ya que es común que se produzcan problemas de tráfico y colisiones, que se pueden paliar segmentando la red en varias partes.

Topología de anillo: Una topología de anillo (figura 3) se compone de un solo anillo cerrado formado por nodos y enlaces, en el que cada nodo está conectado solamente con los dos nodos adyacentes.

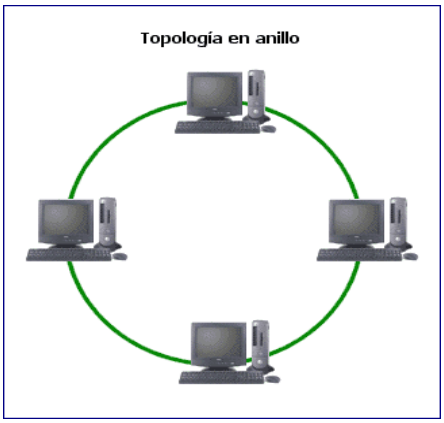


Fig. 3 Topología de anillo

Los dispositivos se conectan directamente entre sí por medio de cables en lo que se denomina una cadena margarita. Para que la información pueda circular, cada estación debe transferir la información a la estación adyacente.

Topología en estrella: La topología en estrella (figura 4) tiene un nodo central desde el que se irradian todos los enlaces hacia los demás nodos. Por el nodo central, pasa toda la información que circula por la red.

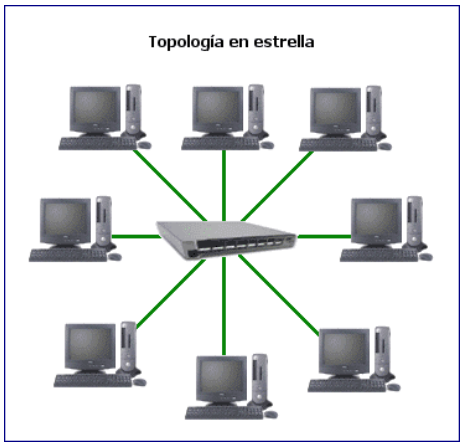


Fig. 4 Topología en estrella

La ventaja principal es que permite que todos los nodos se comuniquen entre sí de manera conveniente. La desventaja principal es que si el nodo central falla, toda la red se desconecta.

Topología en árbol: La topología en árbol (figura 5) es similar a la topología en estrella extendida, salvo en que no tiene un nodo central. En cambio, un nodo de enlace troncal, generalmente ocupado por un hub o switch, desde el que se ramifican los demás nodos.

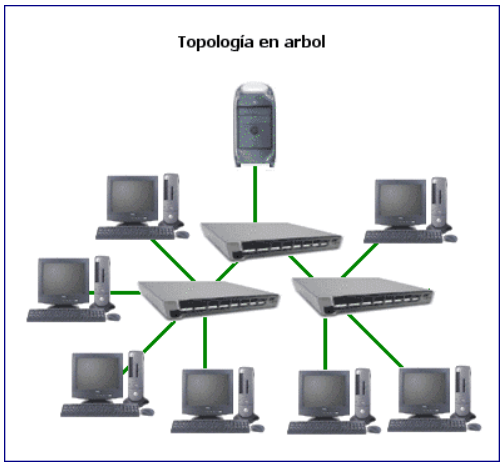


Fig. 5 Topología en árbol

El enlace troncal es un cable con varias capas de ramificaciones, y el flujo de información es jerárquico.

Topología en malla completa: En una topología de malla completa (figura 6), cada nodo se enlaza directamente con los demás nodos. Las ventajas son que, como cada todo se conecta físicamente a los demás, creando una conexión redundante, si algún enlace deja de funcionar la información puede circular a través de cualquier cantidad de enlaces hasta llegar a destino. Además, esta topología permite que la información circule por varias rutas a través de la red.

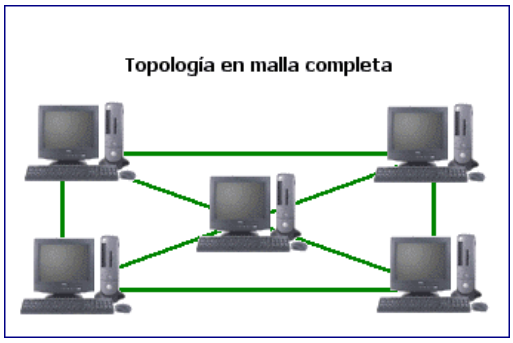


Fig. 6 Topología en malla completa

La desventaja física principal es que sólo funciona con una pequeña cantidad de nodos, ya que de lo contrario la cantidad de medios necesarios para los enlaces, y la cantidad de conexiones con los enlaces se torna abrumadora.

2.1.2. Medios de transmisión.

Por medio de transmisión se entiende el soporte físico utilizado para el envío de datos por la red.

El cable par trenzado: Es de los más antiguos en el mercado y en algunos tipos de aplicaciones es el más común. Consiste en dos alambres de cobre o a veces de aluminio, aislados con un grosor de 1 mm. aproximadamente. Los alambres se trenzan con el propósito de reducir la interferencia eléctrica de pares similares cercanos. Los pares trenzados se agrupan bajo una cubierta común de PVC (Poli cloruro de Vinilo) en cables multipares de pares trenzados (de 2, 4, 8, hasta 300 pares).

La estructura de todos los cables par trenzado no difieren significativamente, aunque es cierto que cada fabricante introduce algunas tecnologías adicionales mientras los estándares de fabricación se lo permitan. El cable está compuesto, por un conductor interno que es de alambre electrolítico recocido, de tipo circular, aislado por una capa de polietileno coloreado. Como se muestra en la figura siguiente.

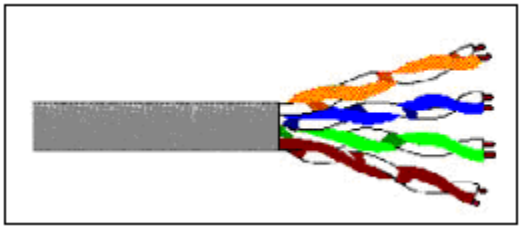


Fig. 7 Cable par trenzado

Debajo de la aislación coloreada existe otra capa de aislación también de polietileno, que contiene en su composición una sustancia antioxidante para evitar la corrosión del cable. El conducto sólo tiene un diámetro de aproximadamente medio milímetro, y más la aislación el diámetro puede superar el milímetro.

Sin embargo es importante aclarar que habitualmente este tipo de cable no se maneja por unidades, sino por pares y grupos de pares, paquete conocido como cable multipar. Todos los cables del multipar están trenzados entre sí con el objeto de mejorar la resistencia de todo el grupo hacia diferentes tipos de interferencia electromagnética externa.

Tipos de cable par trenzado (figura 8):

- Cable de par trenzado apantallado (STP): En este tipo de cable, cada par va recubierto por una malla conductora que actúa de apantalla frente a interferencias y ruido eléctrico.

Fig. 8 Tipos de cable par trenzado

El nivel de protección del STP ante perturbaciones externas es mayor al ofrecido por UTP. Sin embargo es más costoso y requiere más instalación.

Es utilizado generalmente en las instalaciones de procesos de datos por su capacidad y sus buenas características contra las radiaciones electromagnéticas, pero el inconveniente es que es un cable robusto, caro y difícil de instalar.

- Cable de par trenzado con pantalla global (FTP): En este tipo de cable como en el UTP, sus pares no están apantallados, pero sí dispone de una pantalla global para mejorar su nivel de protección ante interferencias externas.

- Cable par trenzado no apantallado (UTP): El cable par trenzado más simple y empleado, sin ningún tipo de pantalla adicional. Es el más utilizado en telefonía.

  Categorías del cable UTP:

  - *Categoría* 1: Este tipo de cable esta especialmente diseñado para redes telefónicas, es el típico cable empleado para teléfonos por las compañías telefónicas. Alcanzan como máximo velocidades de hasta 4 Mbps.
  - *Categoría 2*: De características idénticas al cable de categoría 1.
  - *Categoría 3:* Es utilizado en redes de ordenadores de hasta 16 Mbps. de velocidad.
  - *Categoría 4:* Esta definido para redes de ordenadores tipo anillo como Token Ring y con una velocidad de 20 Mbps.
  - *Categoría 5*: Es un estándar dentro de las comunicaciones en redes LAN. Es capaz de soportar comunicaciones de hasta 100 Mbps. Este tipo de cable es de 8 hilos, es decir cuatro pares trenzados. La velocidad de transmisión de datos (figura 9) de esta categoría viene dado por esta tabla referida a una distancia estándar de 100 metros:

Velocidad de transmisión de datos
4 Mbps
10 Mbps
16 Mbps
100 Mbps

Fig. 9 Tabla de velocidad de transmisión de datos

- Categoría 5e: Es una categoría 5 mejorada. Minimiza la atenuación y las interferencias.
- Categoría 6: No esta estandarizada aunque ya se está utilizando.
- Categoría 7: No esta definida y mucho menos estandarizada.

El cable coaxial: Hasta hace poco, era el medio de transmisión más común en las redes locales. La construcción del cable debe de ser firme y uniforme (figura 10), por que si no es así, no se tiene un funcionamiento adecuado.

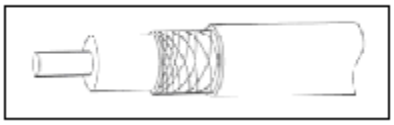


Fig. 10 Cable coaxial

Se encuentra estructurado de la siguiente manera:

- Un núcleo de cobre sólido, o de acero con capa de cobre, o bien de una serie de fibras de alambre de cobre entrelazadas dependiendo del fabricante.
- Una capa de aislante que recubre el núcleo o conductor, generalmente de material de polivinilo, este aislante tiene la función de guardar una distancia uniforme del conductor con el exterior.
- Una capa de blindaje metálico, generalmente cobre o aleación de aluminio entretejido (a veces solo consta de un papel metálico) cuya función es la de mantenerse lo mas apretado posible para eliminar las interferencias, además de que evita de que el eje común se rompa o se tuerza demasiado, ya que si el eje común no se mantiene en buenas condiciones, trae como consecuencia que la señal se va perdiendo, y esto afectaría la calidad de la señal.
- Por último, tiene una capa final de recubrimiento, de color negro en el caso del cable coaxial delgado o amarillo en el caso del cable coaxial grueso, este recubrimiento normalmente suele ser de vinilo, xelón ó polietileno uniforme para mantener la calidad de las señales.

Existen dos tipos de cable coaxial:

- Cable Thick o cable grueso: es más voluminoso, caro y difícil de instalar, pero permite conectar un mayor número de nodos y alcanzar mayores distancias.
- Cable Thin o cable fino, también conocido como cheapernet por ser más económico y fácil de instalar. Sólo se utiliza para redes con un número reducido de nodos.

Ambos tipos de cable pueden ser usados simultáneamente en una red. La velocidad de transmisión de la señal por ambos es de 10 Mb.

Fibra Óptica: Es el medio de transmisión más moderno y avanzado. Utilizado cada vez más para formar la "espina dorsal" de grandes redes. Estos cables son mucho más ligeros, de menor diámetro y repetidores que los tradicionales cables metálicos. Además, la densidad de información que son capaces de transmitir es también mucho mayor.

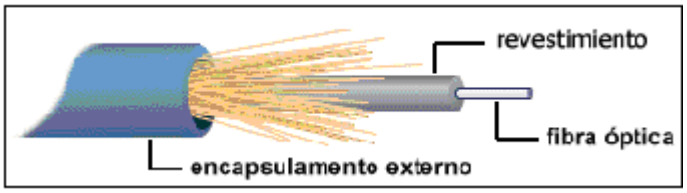


Fig. 11 Fibra óptica

En la última década la fibra óptica ha pasado a ser una de las tecnologías más avanzadas que se utilizan como medio de transmisión. Los logros con este material fueron una mayor velocidad y disminuir casi en su totalidad ruidos e interferencias.

La fibra óptica está compuesta por filamentos de vidrio de alta pureza muy compactos. El grosor de una fibra es como la de un cabello humano aproximadamente. Fabricadas a alta temperatura con base en silicio, su proceso de elaboración es controlado por medio de computadoras, para permitir que el índice de refracción de su núcleo, que es la guía de la onda luminosa, sea uniforme y evite las desviaciones.

Como características de la fibra podemos destacar que son compactas, ligeras, con bajas pérdidas de señal, amplia capacidad de transmisión y un alto grado de confiabilidad ya que son inmunes a las interferencias electromagnéticas de radio-frecuencia. Las fibras ópticas no conducen señales eléctricas, conducen rayos luminosos, por lo tanto son ideales para incorporarse en cables sin ningún componente conductivo y pueden usarse en condiciones peligrosas de alta tensión.

Los tipos de fibra óptica son:

- Fibra multimodal

En este tipo de fibra viajan varios rayos ópticos reflejándose a diferentes ángulos, los diferentes rayos ópticos recorren diferentes distancias y se desfasan al viajar dentro de la fibra. Por esta razón, la distancia a la que se puede trasmitir está limitada.

- Fibra multimodal con índice graduado

En este tipo de fibra óptica el núcleo está hecho de varias capas concéntricas de material óptico con diferentes índices de refracción. En

estas fibras el número de rayos ópticos diferentes que viajan es menor y, por lo tanto, sufren menos el severo problema de las multimodales.

- Fibra monomodal:

Esta fibra óptica es la de menor diámetro y solamente permite viajar al rayo óptico central.

2.2. ETHERNET.

2.2.1. Historia.

En 1972 comenzó el desarrollo de una tecnología de redes conocida como Ethernet Experimental- El sistema Ethernet desarrollado, conocido en ese entonces como red ALTO-ALOHA, fue la primera red de área local (LAN) para computadoras personales (Pc´s). Esta red funcionó por primera vez en mayo de 1973 a una velocidad de 2.94 Mb/s.

Las especificaciones formales de Ethernet de 10 Mb/s fueron desarrolladas en conjunto por las corporaciones Xerox, Digital (DEC) e Intel, y se publicó en el año 1980. Estas especificaciones son conocidas como es estándar DEC-Intel-Xerox (DIX), el libro azul de Ethernet. Este documento hizo de Ethernet Experimental un estándar abierto.

La tecnología Ethernet fue adoptada para su estandarización por comité de redes locales (LAN) de la IEEE como IEEE 802.3. El estándar 802.3 fue publicado por primera vez en 1985.

El estándar IEEE 802.3 provee un sistema tipo Ethernet basado, pero no idéntico, al estándar DIX original. El nombre correcto para esta tecnología es IEEE 802.3 CSMA/CD, pero casi siempre es referido como Ethernet.

IEEE 802.3 Ethernet fue adoptado por la Organización Internacional de Estandarización (ISO), haciendo de el un estándar de redes internacional.

Ethernet continuó evolucionando en respuesta a los cambios en tecnología y necesidades de los usuarios. Desde 1985, el estándar IEEE 802.3 se actualizó para incluir nuevas tecnologías.

Ethernet es una tecnología de redes ampliamente aceptada con conexiones disponibles para PC´s, estaciones de trabajo científicas y de alto desempeño y sistemas mainframe.

2.2.2. Objetivos de Ethernet.

Los objetivos de Ethernet son:

- Simplicidad. Las características que puedan complicar el diseño de la red sin hacer una contribución substancial para alcanzar otros objetivos se han excluido.
- Bajo costo. Las mejoras tecnológicas van a continuar reduciendo el costo global de los dispositivos de conexión.
- Compatibilidad. Todas las implementaciones de Ethernet deberán ser capaces de intercambiar datos a nivel de capa de enlaces de datos. Para eliminar la posibilidad de variaciones incompatibles de Ethernet, la especificación evita características opcionales.
- Direccionamiento flexible. El mecanismo de direccionamiento debe proveer la capacidad de dirigir datos a un único dispositivo, a un grupo de dispositivos, o alternativamente, difundir (broadcast) el mensaje a todos los dispositivos conectados a la red.
- Equidad. Todos los dispositivos conectados deben tener el mismo acceso a la red.
- Mantenimiento. El diseño de Ethernet debe simplificar el mantenimiento de la red, operaciones y planeamiento.

2.2.3. Características de Ethernet.

Las siguientes son algunas de las características que definen a Ethernet:

Las especificaciones Ethernet (IEEE 802.3) también han sido adoptadas por ISO y se encuentran en el estándar internacional 8802-3.

Ethernet esta basado en la lógica de la topología bus. Originalmente, el bus era una única longitud de cable a la cual los dispositivos de red estaban conectados. En las implementaciones actuales, el bus se ha miniaturizado y puesto en un hub (concentrador) al cuál las estaciones, servidores y otros dispositivos son conectados.

Ethernet usa un método de acceso al medio por disputa (contention). Las transmisiones son difundidas en el canal compartido para ser escuchadas por todos los dispositivos conectados, solo el dispositivo destino previsto va a aceptar la transmisión. Este tipo de acceso es conocido como CSMA/CD (Acceso al Medio Múltiple con Detección de Errores).

Ethernet ha evolucionado para operar sobre una variedad de medios, cable coaxial par trenzado y fibra óptica, a múltiples tasas de transferencia. Todas las implementaciones son ínter operables, lo que simplifica el proceso de migración a nuevas versiones de Ethernet.

Ethernet fue diseñado para ser expandido fácilmente. El uso de dispositivos de interconexión tales como bridges, routers y switches permiten que redes LAN individuales se conecten entre si. Cada LAN continúa operando en forma independiente pero es capaz de comunicarse fácilmente con las otras LAN conectadas.

2.2.4. Tipos de Ethernet.

Existen una gran variedad de implementaciones de IEEE 802.3.

Algunos tipos de estas implementaciones de IEEE 802.3 y sus características se detallan a continuación (figura 12):

TECNOLOGIA	**VELOCIDAD DE TRANSMISION**	**TIPO DE CABLE**	**DISTANCIA MAXIMA**
10Base2	10 Mbps	Coaxial	185 m
10BaseT	10 Mbps	Par Trenzado	100 m
10BaseF	10 Mbps	Fibra óptica	2000 m
100BaseT4	100Mbps	Par Trenzado (categoría 3UTP)	100 m
100BaseTX	100Mbps	Par Trenzado (categoría 5UTP)	100 m
100BaseFX	100Mbps	Fibra óptica	2000 m

1000BaseT	1000Mbps	4 pares trenzado (categoría 5UTP)	100 m
1000BaseSX	1000Mbps	Fibra óptica (multimodo)	550 m
1000BaseLX	1000Mbps	Fibra óptica (monomodo)	5000 m

Fig. 12 Implementaciones IEEE 802.3

2.3. INTERNET.

El inicio de Internet se remonta a los años 60´s, cuando en los E. U. se estaba buscando una forma de mantener las comunicaciones vitales del país en el posible caso de una Guerra Nuclear. Este hecho marcó profundamente su evolución, ya que aún ahora los rasgos fundamentales del proyecto se hallan presentes en lo que hoy conocemos como Internet (figura 13). [1]

[1] Douglas E. Comer. Redes globales de información con Internet y TCP/IP.

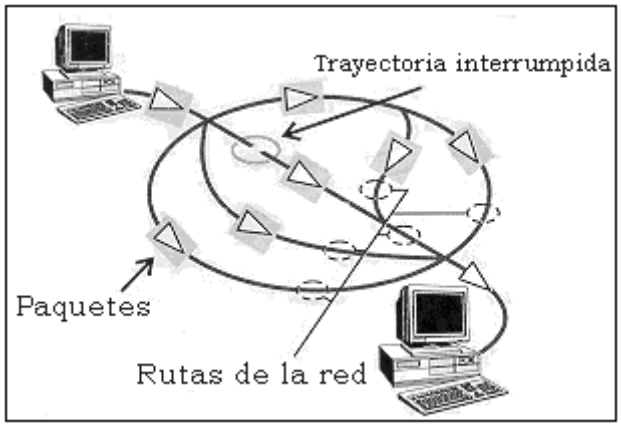


Fig. 13 Internet

En primer lugar, el proyecto contemplaba la eliminación de cualquier "autoridad central", ya que sería el primer blanco en caso de un ataque; en este sentido, se pensó en una red descentralizada y diseñada para operar en situaciones difíciles. Cada máquina conectada debería tener el mismo status y la misma capacidad para mandar y recibir información.

El envío de los datos debería descansar en un mecanismo que pudiera manejar la destrucción parcial de la Red. Se decidió entonces que los mensajes deberían de dividirse en pequeñas porciones de información o paquetes, los cuales contendrían la dirección de destino pero sin especificar una ruta específica para su arribo; por el contrario, cada paquete buscaría la manera de llegar al destinatario por las rutas disponibles y el destinatario reensamblaría los paquetes individuales para reconstruir el mensaje original. La ruta que siguieran los paquetes no era importante; lo importante era que llegaran a su destino.

Curiosamente fue en Inglaterra donde se experimentó primero con estos conceptos; y así en 1968, el Laboratorio Nacional de Física de la Gran Bretaña estableció la primera red experimental. Al año siguiente, el Pentágono de los E.U. decidió financiar su propio proyecto, y en 1969 se establece la primera red en la Universidad de California (UCLA) y poco después aparecen tres redes adicionales. Nacía así ARPANET (Advanced Research Projects Agency NETwork), antecedente de la actual Internet.

Gracias a ARPANET, científicos e investigadores pudieron compartir recursos informáticos en forma remota; este era una gran ayuda ya que hay que recordar que en los años 70's el tiempo de procesamiento por computadora era un recurso realmente escaso. ARPANET en sí misma también creció y ya para 1972 agrupaba a 37 redes.

El Protocolo utilizado en ese entonces por las máquinas conectadas a ARPANET se llamaba NCP (Network Control Protocol ó Protocolo de Control de Red), pero con el tiempo dio paso a un protocolo más sofisticado: TCP/IP, que de hecho está formado no por uno, sino por varios protocolos, siendo los más importantes el protocolo TCP (Transmission Control Protocol ó Protocolo de Control de Transmisión) y el Protocolo IP (Internet Protocol ó Protocolo de Internet). TCP convierte los mensajes en paquetes en la maquina emisora, y los reensambla en la máquina destino para obtener el mensaje original, mientras que IP es el encargado de encontrar la ruta al destino.

La naturaleza descentralizada de ARPANET y la disponibilidad sin costo de programas basados en TCP/IP permitió que ya en 1977, otro tipo de redes no necesariamente vinculadas al proyecto original, empezaran a conectarse. En 1983, el segmento militar de ARPANET decide separarse y formar su propia red que se conoció como MILNET.

ARPANET, y sus "redes asociadas" empezaron a ser conocidas como Internet.

Ese año, la Fundación Nacional para la Ciencia (National Science Foundation) inicia una nueva "red de redes" vinculando en una primera etapa a los centros de supercómputo en los E.U. (6 grandes centros de procesamiento de datos distribuidos en el territorio de los E.U.) a través de nuevas y más rápidas conexiones. Esta red se le conoció como NSFNET y adoptó también como protocolo de comunicación a TCP/IP.

Eventualmente, a NSFNET empezaron a conectarse no solamente centros de supercómputo, sino también instituciones educativas con redes más pequeñas. El crecimiento exponencial que experimentó NSFNET así como el incremento continuo de su capacidad de transmisión de datos, determinó que la mayoría de los miembros de ARPANET terminaran conectándose a esta nueva red y en 1989, ARPANET se declara disuelta.

2.4. INTRANET.

Red privada que permite a las corporaciones aprovechar los beneficios de la tecnología Internet utilizando sus mismas herramientas, protocolos y servicios: www, correo electrónico, videoconferencia, transferencia de archivos, etc.

Intranet es el término que se utiliza para referirse a las redes privadas integradas con tecnología Internet para la transmisión e intercambio de información corporativa (figura 14). De acuerdo con los requerimientos de la corporación, los servidores Intranet pueden estar conectados o desconectados de la red pública Internet.

Fig. 14 Intranet

Las intranet, al igual que Internet están basadas en protocolos abiertos. El más importante es TCP/ IP que es le protocolo de comunicación sobre el que está construido Internet.

Por tanto, necesitaremos que la red esté basada en él, que será lo normal si ya se cuenta con conexión a Internet. Esto permite utilizar

también protocolos como IPX, ya que pueden convivir sin mayor problema.

Por último y más importante, se requiere de una máquina que actúe como servidor y en donde se centralizarán todos o algunos de los servicios. Si la red está basada en servidor se podrá utilizar ese mismo servidor para instalar los programas oportunos, por ejemplo Microsoft cuenta con el IIS (Internet Information Server); pero si la red no está basada en servidor sino que es de tipo punto a punto, como una típica red con sólo estaciones de trabajo también será posible utilizar una de esas máquinas para que actúe como máquina servidora. Son muchos los programas shareware o incluso freeware que podemos encontrar para Windows y que nos permitirán tener plena funcionalidad sin necesidad de un servidor dedicado y por tanto con un costo de entrada muy bajo.

2.4.1. ¿Para qué sirve?.

Las redes locales permiten compartir recursos hardware y software de forma transparente entre los distintos integrantes de un mismo grupo de trabajo, así pues podemos compartir con ellos nuestras impresoras, archivos o la conexión a Internet, pero una intranet nos permite ir un paso más allá.

La popularidad de Internet ha conseguido que todos los servicios que están directamente relacionados con ella se estandaricen y se

conviertan en universales, pero estos servicios no solamente están disponibles para comunicarnos con el exterior, sino que son igualmente útiles en la gestión y administración de nuestra organización o departamento, o incluso en nuestro propio hogar.

El correo electrónico es sin dudad el más utilizado de estos servicios, y se convierte rápidamente en una herramienta imprescindible, pero hay otros que son igualmente interesantes como los servicios de Noticias, los famosos “chat”, la mensajería instantánea, la videoconferencia, etc. Todo esto junto con las páginas Web permite una interactividad con el resto de integrantes del grupo de trabajo que se verá rápidamente recompensada con mayor productividad y mejor coordinación.

2.4.2. Alcances operativos.

- Acceso distribuido a un amplio rango de información y servicios.
- Información corporativa compartida y suministrada en contexto.
- Auténtica colaboración de grupos de trabajo.
- Fácil e inmediata interacción con los expertos.

Dependiendo de la empresa que cree el intranet proporcionará a sus clientes todos los servicios necesarios para la implementación y optimización de la Intranet aprovechando la actual infraestructura. Desde el diseño de la estructura y organización del Web Site, la configuración de servidores y la implementación de mecanismos que

garanticen la seguridad e integridad de la información hasta la conexión a aplicaciones de procesamiento o bases de datos existentes.

2.4.3. Servicios para el usuario de Intranet.

- Intercambio de información.
- Administración centralizada.
- Comunicación y colaboración.
- Acceso a aplicaciones.
- Navegación.
- Servicios de red.
- Directorios.
- Seguimiento y gestión de toda la información.
- Seguridad.
- Administración.
- Interfaz común, basada en HTML.

2.4.4. Ventajas de Intranet.

- Se instala fácilmente una sola vez.
- Aprovecha infraestructura existente.
- Bajo costo de implementación.
- Interoperatividad a nivel de red.
- Administración centralizada.
- Conectividad con Internet.

- Intercambio de información**.**
  - A nivel grupo:

    Para aumentar la eficiencia y colaboración.
  - Entre grupos de trabajo:

    Para concretar proyectos comunes.
  - Entre puntos de venta y central:

    Para desarrollar estrategias.
  - Con clientes y proveedores:

    Para brindar información al instante.

2.5. ANCHO DE BANDA.

En redes, el ancho de banda es definido como la cantidad de información que puede pasar por un segmento de red en un momento determinado.

Existen ciertas características fundamentales del ancho de banda:

- El ancho de banda es finito, por lo que se tiene que moderar su uso de acuerdo a las necesidades más importantes en el momento y los servicios que se consideren como críticos. La principal limitación es el medio físico pues aunque las tecnologías han permitido grandes velocidades de transferencias, no se ha podido aprovechar al máximo el ancho de banda.

- El ancho de banda no es gratuito; generalmente se compra a un proveedor de servicios, lo cual lleva a los administradores de red a tomar decisiones sobre los equipos, servicios y políticas a establecer en la red, y traducir esto en términos de ahorro económico.

- La demanda de ancho de banda nunca deja de aumentar, a pesar de los nuevos dispositivos y tecnologías, el uso y competencia por el ancho de banda sigue en aumento debido a las aplicaciones que hacen uso de estas mayores capacidades de la red.

La tasa de transferencia es la medición real del ancho de banda en un momento dado y en un segmento determinado de la red. En realidad se trabaja con la tasa de transferencia y esta resulta ser menor al ancho de banda; esto se debe a diversas situaciones como la topología de la red, el número de usuarios en un momento determinado, el tipo de datos a transferir, las características y capacidades de los equipos terminales y servidores.

Es importante que un diseñador y administrador de redes considere los factores que pueden afectar la tasa de transferencia real. Al medir la tasa de transferencia regularmente, un administrador de red estará al tanto de los cambios en el rendimiento de la red y los cambios en las necesidades de los usuarios de la red. Así la red se podrá ajustar en consecuencia.

Se piensa que, entre más ancho de banda en una red, mayor va a ser su desempeño; esta proposición no es necesariamente cierta. La decisión de incrementar el ancho de banda disponible en una red recae sobre el administrador de la red cuando se determina que las capacidades de transferencia de la red comprometen la disponibilidad de los servicios de la red. Esta decisión se sustenta en estudios que consideran la topología de la red, las características de los equipos de red instalados, las necesidades de los usuarios y los servicios ofrecidos.

El incremento del ancho de banda disponible lleva a un gasto económico considerable; es por esto que el estudio de los factores mencionados, es un punto muy importante para tomar la decisión de incrementar el ancho de banda, pues esta acción puede que no sea la solución al incremento del flujo de información y la saturación del ancho de banda.

2.6. DEPENDENCIA FEDERAL COMISION NACIONAL DEL AGUA.

La Comisión Nacional del Agua es heredera de una gran tradición hidráulica y a lo largo de su historia ha estado integrada por destacados profesionales y especialistas de diversas disciplinas, reconocidos internacionalmente por su dedicación y capacidad técnica.

Dentro de las instituciones que le antecedieron destacan la Dirección de Aguas, Tierras y Colonización creada en 1917; la

Comisión Nacional de Irrigación, en 1926; la Secretaría de Recursos Hidráulicos en 1946 y la Secretaría de Agricultura y Recursos Hidráulicos en 1976.

La Comisión considera que la participación de la sociedad es indispensable para alcanzar las metas que se han trazado en cada cuenca del país, ya que entre otros aspectos, los habitantes pueden dar la continuidad que se requieres a las acciones planteadas.

Por otra parte, considera que el uso sustentable del agua se logra cuando se cumplen los aspectos siguientes:

1. El agua genera bienestar social: se refiere al suministro de los servicios de agua potable y alcantarillado a la población, así como al tratamiento de las aguas residuales.
2. El agua propicia el desarrollo económico: considera el agua como un insumo en la actividad económica.
3. El agua se preserva: es el elemento que cierra el concepto de sustentabilidad. La C.N.A. está convencida de que se debe preservar en cantidad y calidad adecuadas para las generaciones actuales y futuras y la flora y fauna de cada región.

Para cumplir con su propósito esencial, la Comisión se divide operativamente en tres grandes áreas:

1. Dirección General.
2. Dirección de Organismos de Cuenca.
3. Direcciones Locales.

La sede de la Dirección Local está en la ciudad de México y dentro de sus acciones principales se encuentran: apoyar a las Direcciones de Organismos de Cuenca y Direcciones Locales en la realización de las acciones necesarias para lograr el uso sustentable del agua en cada región del país, establecer la política y estrategias hidráulicas nacionales, integrar el presupuesto de la institución y vigilar su aplicación, establecer los programas para apoyar a los municipios en el suministro de los servicios de agua potable y saneamiento en las ciudades y comunidades rurales, promover el uso eficiente del agua en el riego e industria, entre otros.

Dirección General también establece la política de recaudación y fiscalización en materia de derechos de agua y permisos de descargas, coordina las modificaciones que se requieren a la Ley de Aguas Nacionales y apoya su aplicación en e país, opera el servicio meteorológico nacional, atiende a los medios de comunicación nacionales y se vincula con las dependencias federales para trabajar en forma conjunta en acciones que beneficien al Sector Hidráulico.

Las Direcciones de Organismos de Cuenca son las responsables de administrar y preservar las aguas nacionales en cada una de las trece regiones hidrológico-administrativas en que se ha dividido el país. Las regiones y sus sedes son:

- Península de Baja California (Mexicali, Baja California).
- Noroeste (Hermosillo, Sonora)
- .Pacífico Norte (Culiacán, Sinaloa).
- Balsas (Cuernavaca, Morelos).
- Pacífico Sur (Oaxaca, Oaxaca).
- Río Bravo (Monterrey, Nuevo León).
- Cuencas Centrales del Norte (Torreón, Coahuila).
- Lerma Santiago Pacífico (Guadalajara, Jalisco).
- Golfo Norte (Cd. Victoria, Tamaulipas).
- Golfo Centro (Jalapa, Veracruz).
- Frontera Sur (Tuxtla Gutiérrez, Chiapas).
- Península de Yucatán (Mérida, Yucatán).
- Aguas del Valle de México y Sistema Cutzamala (México, D. F.).

El desempeño de las Direcciones de Organismos de Cuenca es también muy importante, ya que tiene a su cargo aplicar la razón misma de ser de la institución en cada región del país. Dentro de las tareas que se realizan tenemos:

- Determinar la disponibilidad del agua.
- Lograr el uso sustentable del agua.
- Solucionar conflictos relacionados con el agua.
- Otorgar concesiones, asignaciones y permisos.
- Promover la cultura del buen uso y preservación del agua.

Además, las Direcciones de Organismos de Cuenca son el vínculo con los gobernadores de las entidades donde se ubican.

Por lo que se refiere a las Direcciones Locales, éstas tienen la importante labor de aplicar las políticas, estrategias, programas y acciones de la Comisión en las entidades federativas que les corresponde.

2.6.1. Misión.

Administrar y preservar las aguas nacionales, con la participación de la sociedad para lograr el uso sustentable del recurso (figura 15).

Fig. 15 Misión

Administrar y preservar las aguas nacionales…

Implica:

- Saber cuánta agua hay en nuestro país, clasificarla de acuerdo a su calidad y calcular su disponibilidad.
- Otorgar permisos para la explotación, uso o aprovechamiento de las aguas nacionales, a través de las concesiones, asignaciones y reservas para hacer un uso más justo y eficiente del agua.
- Asegurar el equilibrio hidrológico y una adecuada calidad del agua, mediante la construcción y operación de la infraestructura necesaria.
- Garantizar la seguridad de la población ante la presencia de fenómenos hidrológicos extremos.

2.6.2. Visión.

"Ser un órgano normativo y de autoridad con la calidad técnica y promotor de la participación de la sociedad y de los órdenes de gobierno en la administración del agua".

La visión establece el cambio de la CONAGUA hacia una organización cuya función predominante será el carácter normativo y de apoyo técnico en la administración y preservación del recurso, para lo cual la institución delegará la responsabilidad de construir, operar y mantener la infraestructura hidráulica urbana e hidroagrícola a las autoridades locales y usuarios, lo que implica el proceso de descentralización de la institución hacia estas estancias.

La alta capacidad técnica está referida tanto a las características del personal y de la organización, como a las herramientas técnicas para el desempeño de las funciones y responsabilidades.

2.6.3. Estructura Orgánica.

La Comisión Nacional del Agua se estructura de la siguiente manera (figura 16):

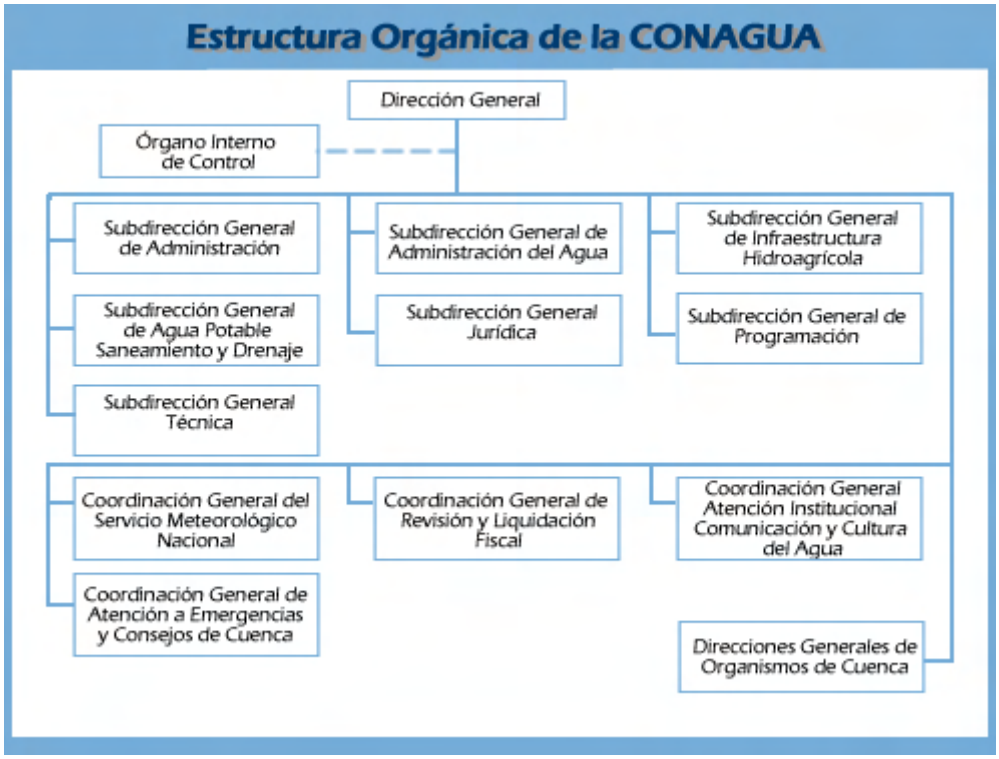


Fig. 16 Estructura orgánica

2.7. INFRAESTRUCTURA DE LA RED DE LA DIRECCIÓN LOCAL GUERRERO DE LA COMISIÓN NACIONAL DEL AGUA.

La red de la Dirección Local Guerrero tiene un enlace de 2048 kbps cuenta con un router Huawei 2811 con tecnología Fast Ethernet de 100 Mbps, una infraestructura de computo de 130 computadoras, con conexión a Internet controlado por 6 switches de la marca 3com, LinkPro, AlliedTelessyn (figura 17).

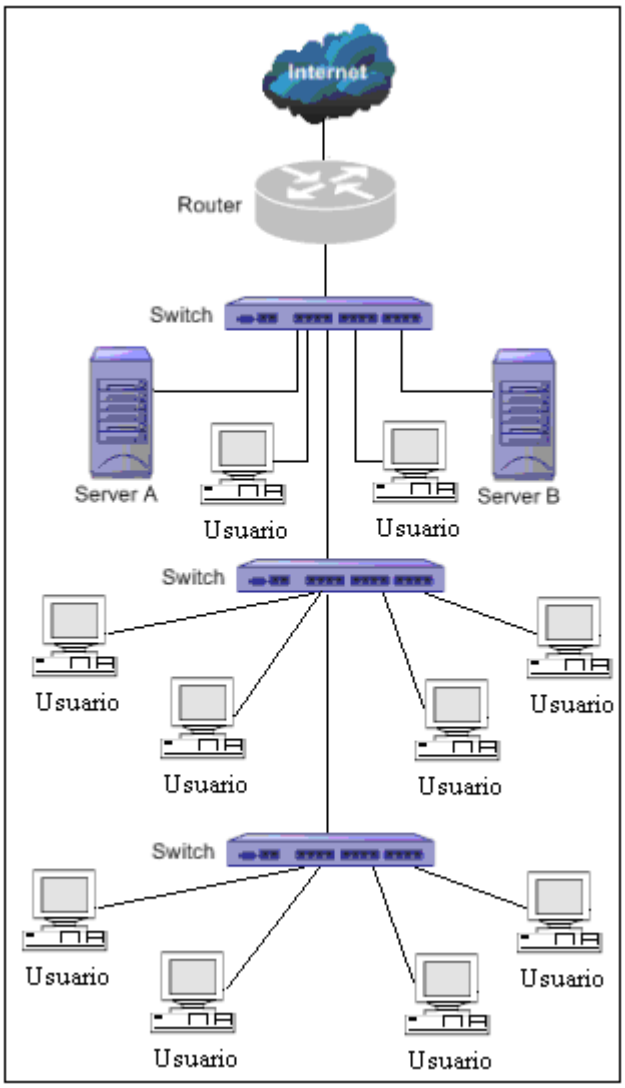


Fig. 17 Infraestructura de la red de la Dirección Local Guerrero

2.7.1. Servicios.

Estos son algunos de los recursos de tecnología de informática y telecomunicaciones que están disponibles en la institución.

- Acceso a Internet.
- Videoconferencia.
- Servicio de Mesa de Ayuda. Es una herramienta para administrar la tecnología de informática y telecomunicaciones en la C. N. A. ya que a través del mismo se reciben y atienden las solicitudes de soporte técnico a nivel central, trámites de garantías a nivel nacional, mantenimiento correctivo para equipo de telecomunicaciones a nivel nacional, y mantenimiento correctivo a nivel central para equipo de computo, dispositivos periféricos y equipos de respaldo de energía eléctrica.
- Correo electrónico
- Telefonía IP.
- Página de intranet. Herramienta para publicar información interna referente a la C. N. A., ya que a través de ella se puede consultar diferentes áreas y cuentan con los siguientes servicios:
    - Consultar cartelera de cine, teatro y parques familiares.
    - Participar en colaboraciones.
    - Anuncios oportunos.

- Servicios informáticos.
- Directorio de telefonía.
- Tablero de avisos.

2.7.2. Página de la intranet de la Comisión Nacional del Agua.

En la página de intranet se encuentra información referente a esta dependencia (figura 18).

Fig. 18 Página de intranet

Entre la información que proporciona la página podemos mencionar el plan estratégico (proceso de planeación estratégica, misión, visión, planeación y estrategia), directorio de Organismos de Cuenca y Direcciones Locales, publicaciones CONAGUA, documentos relacionados a la institución, capacitación en donde se ofrecen cursos a y talleres a los empleados, eventos, sitios de Organismos de Cuenca y Direcciones Locales, Soporte Técnico (drivers, mesa de ayuda, parches de seguridad, herramientas, manuales informáticos, etc.) y el link de "Sistemas", en el cual podemos encontrar las actividades que desarrollan las diferentes subdirecciones de la CONAGUA:

La ***Subdirección General de Administración*** para una mayor eficiencia en el desarrollo de las actividades maneja los siguientes programas:

- Gerencia de Recursos Financieros.

- Sistema Institucional de Viáticos (SIV).

- Gerencia de Personal.
  - Sistema de Captura de Evaluación y Perfiles (SICAPEP).
- Gerencia de Recursos Materiales.
  - Sistema de Administración de Compras en línea (SACEL).
  - Sistema para el manejo y Control de Almacenes (SiMCA).
  - Sistema para el Control Vehicular Web (SiCOVE).
- Gerencia de Informática y Telecomunicaciones.
  - Sistema de Mesa de Ayuda.
- *Gerencia de Innovación y Calidad.*
  - *Foro Virtual de Innovación y Calidad.*
  - *Sistema de Innovación CONAGUA.*

La **Subdirección General de Administración del Agua** maneja los siguientes programas:

- Registro Público de Derechos de Agua (REPDA).

- *Gerencia del Registro Público de Derechos del Agua.*
  - Sistema de Localización Geográfica del Registro Público de Derechos del Agua (LOCREPDA).

La ***Subdirección General de Agua Potable, Drenaje y Saneamiento*** maneja los siguientes programas:

- *Gerencia de Fortalecimiento de Organismos Operadores.*
    - Sistema de Programa de devolución de Derechos.

La ***Subdirección General de Infraestructura Hidráulica Urbana*** maneja los siguientes programas:

- Sistema de Registro de Contratistas de Obras (SISCON).
- Sistema de Información de Servicios Básicos del Agua (SISBA).
- Sistema de Información del Programa de Devolución de Derechos sobre usos del Agua (PRODDER).
- Sistema para la Subdirección General de Infraestructura Hidráulica Urbana (SSGIHU).

La ***Subdirección General de Programación*** maneja los siguientes programas:

- *Gerencia de Evaluación y Programación.*
    - Sistema de Información de Proyectos de Infraestructura Hidráulica (SIPROIH).
    - Sistema Integral de Información para el Seguimiento del Programa Anual de Obra Pública (SIPAO).
    - Sistema de Procedimiento Interno de Programación y Presupuestos (PROINPRO).
- Gerencia de Planeación Hidráulica.

- Sistema de Información Socioeconómica y Financiera del Agua (SISEFA).
- Sistema de Seguimiento y Evaluación de Programas Hidráulicos Regionales (SISEPH).
- Sistema de Prospectiva de Demanda y Oferta del Agua (PDYOA).

- *Subgerencia de Administración.*
  - Sistema de Planeación, Administración y control de Capacitación (SICAPA).
- *Subgerencia de Información Geográfica del Agua.*
  - Sistema de Información Geográfica del Agua (SIGA).
  - Sistema Nacional de Información Sobre Cantidad, Calidad, Usos y Conservación del Agua (SINA).

La ***Subdirección General de Técnica*** maneja los siguientes programas:

- *Gerencia de Aguas Subterráneas.*
  - Sistema de Información Geográfica para el Manejo del Agua Subterránea (SIGMAS).
  - Sistema de Localización Geográfica (SILOG).
- *Gerencia de Saneamiento y Calidad del Agua.*
  - Sistema de la Red Nacional de Monitoreo (SIRNM).
  - Sistema de Información Hidroclimatológica (SIH).

La ***Unidad de Comunicación Social*** maneja los siguientes programas:

- Sistema Integral de Administración y Control de Síntesis (SIACS).
- Sistema de Administración de Imágenes (SAI).

CAPITULO III. GESTION DE REDES.

3.1. GESTIÓN DE REDES.

3.1.1. ¿Qué es gestión de red? Necesidad de la gestión.

Se entiende por <<Gestión de redes y servicios de telecomunicación>> al conjunto de actividades destinadas a garantizar los servicios que prestan las redes.[1] El concepto de redes es muy amplio y aquí lo empleamos en sentido general. Un usuario final que utiliza servicios de comunicaciones no distingue si se le proporcionan mediante redes privadas o redes públicas.

Los recursos informáticos están interconectados mediante medios de transmisión y protocolos de comunicaciones organizados en las conocidas <<Arquitecturas de Ordenadores>> y que podemos denominar <<Sistemas de Comunicaciones>>.

Estos Sistemas de Comunicaciones están implementados mediante infraestructura de equipos de comunicaciones (módem, conmutadores, multiplexores, etc.) y facilidades de transmisión.

Estos son los que prestan los servicios finales, que los usuarios utilizan en la actividad diaria en las empresas y organizaciones.

[1] Frank Derflen. Descubre Redes LAN y WAN.

El tamaño y la complejidad de las redes han ido creciendo sin cesar debido en gran parte a la aparición de las redes públicas de datos y a la creciente oferta de servicios de comunicaciones de valor añadido.

Actualmente los Sistemas de Comunicaciones prestan servicios a los usuarios utilizando Redes Privadas y Redes Públicas. La interconexión entre las mismas proporciona mejores posibilidades en la provisión de servicios pero complica el control de las redes. Habiendo conseguido la transferencia de información a través de esta complejidad de redes, surge la necesidad de gestionarlas, es decir, de controlar los recursos que las componen en términos de rendimiento, capacidad, utilización, reconfiguración, diagnósticos, planificación, etc.

El término <<gestión>>, utilizado en muchos y diversos entornos de nuestra vida diaria, está relacionado con la planificación, el seguimiento, costos, control de recursos y actividades y en este sentido oímos hablar de buenos gestores y de gestores no tan buenos. Aplicando este término al entorno de redes, la gestión de red comprende la administración de los diferentes recursos que constituyen una red.

La gestión de red toma la forma de seguimiento, coordinación y control de los recursos informáticos y de comunicaciones.

Ejemplos de recursos pueden ser un módem, línea de comunicaciones, multiplexor, etc.

Las organizaciones dependen cada vez más del buen funcionamiento de los sistemas de comunicaciones, dado que un gran número de los empleados, utilizan recursos informáticos para la realización de su actividad diaria.

Cada vez es menos justificable la expresión <<la red no funciona bien>> de cara al interior de la empresa, o la expresión <<la línea está caída>> de cara al cliente.

Hoy, debido a la competencia de servicios, las organizaciones y empresas que no disponen de una buena gestión de sus redes y servicios de comunicaciones son cautivas de la tecnología y, en vez de emplear los recursos informáticos para hacer negocio, sus recursos informáticos pueden estar impidiendo el progreso de su negocio.

Los sistemas de comunicaciones (figura 19) pueden ser muy extensos y complejos en cuanto a que están constituidos por un gran número de equipos y a su vez estos ofrecen gran diversidad:

- Teléfonos
- Centralitas telefónicas
- Módem
- Multiplexores
- Concentradores
- Conmutadores de paquetes
- Terminales
- Ordenadores

Fig. 19 Sistemas de comunicaciones

Los fallos es los sistemas de comunicaciones son inevitables y el tiempo de no-funcionamiento de los mismos es muy caro para las organizaciones.

Algunos ejemplos de las consecuencias de los fallos de las redes, que como clientes sufrimos en la vida diaria son:

- Retrasos de los aviones que nos hacen pasar tiempo en los aeropuertos.
- Imposibilidad de obtener dinero de nuestra cuenta bancaria.
- Imposibilidad de realización de la matricula de la universidad.

3.2. SISTEMAS DE GESTIÓN. CLASIFICACIÓN.

Un sistema de Gestión (figura 20) es un sistema informático diseñado para la realización de actividades de gestión de redes y equipos de comunicaciones.

Fig. 20 Sistema de gestión

Existe una gran diversidad de gestión de redes, que refleja en gran medida la diversidad de equipos y servicios de telecomunicaciones existentes.

Podemos clasificar de forma muy general la gran diversidad de Sistemas de Gestión existentes en los cinco grandes grupos siguientes:

- Sistemas de Gestión de equipos de comunicaciones.
- Sistemas de Gestión de redes de comunicaciones.
- Sistemas de Gestión de Arquitecturas de ordenadores (Sistemas de Comunicaciones).- Sistemas de Gestión de redes de área loca,.
- Sistemas de Gestión normalizados.

Los fabricantes de equipos de comunicaciones han desarrollado también Sistemas de Gestión de sus propios equipos por la necesidad de los usuarios de controlar los servicios proporcionados por dichos equipos.

- Sistemas de Gestión de Sistemas de transmisión.
- Sistemas de Gestión de conmutadores de paquetes X.25.

Los fabricantes de ordenadores han desarrollado Sistemas de Gestión propios para controlar los recursos de comunicaciones propios de su arquitectura de comunicaciones.

A estos sistemas de gestión se les denomina Sistemas de Gestión de Fabricantes.

Existe gran variedad de los mismos, por ejemplo:

- Netview de IBM.
- UNMA (Unified Network Management Architecture) de ATT.
- ENMA (Enterprisewide Management Architecture) de DEC (Digital Equipment Corporation).

Dado el gran parque de redes de área de local instaladas, existen también diversos sistemas de gestión desarrollados para controlar las redes de área local, entre otros:

- LAN Manager.
- Netware.
- Vines.

Algunas corporaciones se han decidido por las soluciones particulares para la gestión, bien desarrollando Sistema de Gestión propios, o utilizando los Sistemas de Gestión de Fabricantes.

Sin embargo, la tendencia de la mayoría de las empresas y organizaciones es la utilización de Sistemas de Gestión normalizados a partir de normas aceptadas en los foros internacionales.

3.3. TIPOS DE GESTIÓN.

3.3.1. Gestión de la contabilidad.

Esta área funcional permite identificar los costos de la utilización de los recursos para en función de los mismos poder establecer los cargos por consumo de los mismos. Dependiendo del sistema gestionado, los cargos pueden convertirse en facturas. Por ejemplo, en los sistemas de comunicaciones que dan servicios comerciales.

Esta área funcional proporciona las herramientas necesarias para mantener informados a los usuarios de la red de la utilización realizada de los recursos.

Los procedimientos que permiten conseguir esta funcionalidad son:

- La identificación del uso de recursos y el intercambio de información entre diferentes sistemas de comunicaciones.
- La información sobre tarifas y límites para ciertos recursos y la posibilidad de establecer estos límites.
- La posibilidad de compartir costos cuando dos o más sistemas de comunicaciones cooperan en la prestación de un servicio.

En el caso de redes de una corporación, los usuarios de los recursos son internos y no se cobre ni se paga por utilización de los servicios.

Aún en este caso es necesaria la gestión de la contabilidad para conocer la rentabilidad de la inversión realizada en los recursos de comunicaciones.

En muchos casos se llegan a calcularse los cargos aunque no se pasan facturas.

Los procedimientos destinados a la medida de los recursos consumidos e el caso de redes que prestan servicios comerciales son de máxima importancia ya que:

- La facturación a los usuarios finales es el fin último de los mismos.
- La implementación del cargo o no, en una red depende de la organización de la corporación.
- La nota del cargo o factura en los sistemas comerciales no debería ser tan compleja que haga difícil su compresión y administración.
- Los usuarios necesitan estar bien informados de las políticas o metodologías seguidas para el cálculo de los cargos.
- Las estrategias para establecer los cargos pueden basarse en:

    - Localización geográfica.
    - Nivel de utilización:
        - No. de paquetes/ caracteres.

- Transacciones.
- Tiempo de conexión.

- Tamaño del Depto. o División.
- Combinación de los anteriores.

3.3.2. Gestión de la seguridad.

El propósito de de esta área funcional es el de servir de soporte a la aplicación de políticas de seguridad (figura 21).

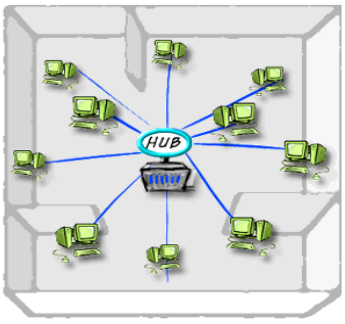


Fig. 21 Gestión de la seguridad

Los mecanismos que proporcionan son:

- La creación, eliminación y mantenimiento de servicios y mecanismos de seguridad de acuerdo con la política de seguridad establecida.
- La distribución de información de seguridad.
- La información acerca de las violaciones de la seguridad. También de los intentos fallidos.

El punto de partida de diseño de la seguridad de un sistema es la identificación de las vulnerabilidades del mismo. Las actuales comunicaciones son vulnerables porque corren el riesgo de ser escuchadas y modificadas de forma impune. En general una combinación es vulnerable si existe la posibilidad de que se produzca un efecto desautorizado de la misma.

Las comunicaciones están amenazadas por todos aquellos que puedan obtener algún beneficio de su conocimiento. Por ataque entendemos la acción encaminada a modificar o alterar el sistema para llevar a cabo dicha amenaza. Por tanto el diseño de las medidas de seguridad va orientado a evitar el efecto de los ataques.

La Política de se Seguridad establece en rasgos generales lo que está o no permitido, luego cualquier posibilidad de comportamiento no autorizado en una red es un riesgo para el sistema.

La finalidad de las medidas de protección para hacer a los sistemas seguros, no es contrarrestar todos los ataques posibles, sino hacer el costo de los mismos suficientemente alto como para reducir el riesgo a límites aceptables.

La introducción de medidas de seguridad excesivas en los sistemas de comunicaciones incrementa el costo de los mismos y puede afectar negativamente a sus prestaciones.

En función de la valoración de los riesgos se adopta una determinada política de seguridad que contempla principalmente, además de procedimientos, métodos, normas, etc., las medidas de protección específicas que denominamos <<servicios de seguridad>> para contrarrestar los efectos de las amenazas.

No todos los usuarios del sistema necesitan el mismo nivel de seguridad. La seguridad depende de sus aplicaciones en concreto. La solución adecuada es que los usuarios definan sus políticas de seguridad y para su realización se apoyen en facilidades de seguridad (sobre todo de gestión).

La política de seguridad de un sistema de comunicaciones debe establecer y definir lo que está o no autorizado. Indica la protección deseada incluyendo servicios de seguridad en la definición del sistema de comunicaciones con el fin de contemplar a nivel de especificación general del mismo las medidas de protección adecuadas para reducir a un nivel aceptable de riesgo.

Los riesgos que hay que tener en cuenta cuando se maneja información que se transmite por redes de telecomunicaciones se pueden clasificar en dos categorías:

- Referidos a la información. Los más importantes son: la ausencia de disponibilidad, la alteración y la destrucción de la misma y la revelación de las comunicaciones. Los sistemas de comunicaciones están sometidos a un gran número de

amenazas que no se habían previsto en el diseño de los mismos, como, falsificación de datos y programas, virus informáticos, caballos de Troya, bombas lógicas y gusanos.

- Referidos a los interlocutores. EL riesgo más importante es la falsificación de identidad. Las actuales técnicas de verificación de identidad basadas en contraseñas (password) pueden ser vulnerables.

En cuanto al análisis de riesgos, va estrechamente unido al servicio de comunicaciones específico que preste el sistema de comunicaciones considerado. En general se deben seguir los siguientes pasos:

a) Valorar el costo que supone para el intruso (posible atacante) la acción de llevar a cabo cada posible amenaza.
b) Valorar los beneficios que puede obtener el intruso en caso de llevar a cabo con éxito el ataque.
c) Valorar las pérdidas que para los usuarios ocasionaría la realización del ataque.
d) Valorar el costo de las medidas de protección que contrarrestan la amenaza. Desde ningún punto de vista será razonable la incorporación de medidas de seguridad que resulten más caras que los propios ataques a que se oponen.

Proporcionar seguridad completa en las redes abiertas de comunicaciones contra estos riesgos es un problema más complejo que proteger entornos informáticos centralizados.

En general, al especificar las medidas de seguridad necesarias para protección de la información en entornos de redes de comunicaciones, se deben considerar los siguientes aspectos: seguridad física, seguridad personal, seguridad administrativa, seguridad de los ordenadores y seguridad de las comunicaciones.

Dado que, por razones económicas, es inviable pensar en medidas de protección físicas extensibles a todo el ámbito de las redes, la técnica adecuada es el empleo de la criptografía.

Las técnicas criptográficas ofrecen las mejores soluciones para hacer frente a los riesgos comentados anteriormente. Pueden resolver los problemas de seguridad externa de las redes de comunicaciones y mejorar los aspectos de seguridad interna de las mismas.

La gestión de claves comprende los procedimientos necesarios para la generación, distribución, administración y mantenimiento de las claves.

3.4. HERRAMIENTAS DE GESTIÓN.

Un sistema de gestión que dispusiera de facilidades para la realización de todas las funciones de gestión, sería un sistema muy caro y muy complejo.

La solución es la especialización de los sistemas de gestión. La utilización de sistemas de gestión normalizados permite la gestión integrada aún utilizando distintos sistemas de gestión para controlar una red.

El estado del arte actualmente en gestión de redes es la existencia de un conjunto de equipos especializados en determinadas funciones de gestión que complementan a los sistemas de gestión de redes.

Actualmente, aunque se pueden diseñar sistemas de gestión que sean completos, en el sentido de incluir toda la funcionalidad necesaria para gestionar una red, no es la práctica habitual porque serían sistemas muy complejos y caros.

Se entiende por herramientas de gestión a las utilidades (hardware y software) que se emplean para ayudar a la realización de las actividades de gestión de red y que habitualmente no están incluidas en los sistemas de gestión.

Tradicionalmente el término <<Herramientas de gestión>> se ha aplicado a equipos específicos diseñados para la monitorización y localización de fallos en los sistemas de comunicaciones.

El sistema de gestión informa del funcionamiento de la red y a partir de la información recogida se detectan mal funcionamiento.

Con estos equipos específicos se trata de aislar e identificar el problema. Estos equipos se aplican a un trozo de red en concreto y en un momento determinado.

Luego hay una diferencia fundamental en cuanto a las prestaciones de estos equipos respecto a las mismas funciones incluidas en el sistema de gestión.

3.4.1. Tipos de herramientas.

En rasgos generales podemos clasificar a los equipos específicos de gestión de red en los siguientes grandes grupos:

- Equipos de pruebas de cableado.
- Monitores de red.
- Analizadores de red.
- Analizadores de protocolos.

3.4.2. Equipos de pruebas de cableado.

El osciloscopio, el reflectómetro y los exploradores de cables, son equipos de pruebas de cableado (figura 22). Son equipos de pruebas a nivel eléctrico, que permiten comprobar que la instalación física es correcta.

Permiten detectar si hay cruces entre cables, abertura de uno de los hilos, rotura total del cable, longitud excesiva del cable, conectores mal instalados, circuito abierto, cortocircuito.

Fig. 22 Equipos de pruebas de cableado

3.4.3. Monitoreo de red.

Fig. 23 Monitoreo de red

El monitoreo de red (figura 23) consiste en un ordenador y unos programas específicos que le permiten la captura de datos para poder realizar estadísticas de funcionamiento. Estos equipos incluyen también la facilidad de monitorización de señales en las interfaces. Normalmente decodifican los protocolos sencillos carácter a carácter, los protocolos de nivel de enlace y a veces también X. 25.

Lo más habitual es que sean equipos portátiles, que se pueden instalar en distintos puntos de la red para extraer de ella información de tipo estadístico, evolución de parámetros de funcionamiento, histogramas, tráfico por cada enlace, etc. Esta información es mostrada en forma de gráficos que hacen más fácil su interpretación.

Las funciones básicas que debe tener un monitor de red son:

- Poder extraer estadísticas globales de tráfico, número de errores, bytes transmitidos y recibidos, etc.
- Poder extraer estadísticas para cada terminal de la red y los errores que provoca.

- Proporcionar estadísticas en tiempo real y estadísticas históricas (carga máxima y medida por intervalos de tiempo).
- Determinar que ancho de banda se está utilizando en cada momento.

3.4.4. Analizador de red.

Los analizadores de red son también ordenadores que se pueden conectar a la red y que disponen de programas adecuados para poder decodificar protocolos de hasta nivel 4. Permiten capturar parte de la información que circula por la red, para después decodificarla e interpretarla para ayudar en la localización de problemas (figura 24). Estos equipos permiten simular tráfico con el formato del protocolo correspondiente.

Las funciones básicas que debe tener un analizador de red son:

- Poder capturar y decodificar tramas, llegando hasta el nivel 4 de OSI, interpretando la información de los cuatro niveles para los protocolos más comunes.
- Generar tráfico simulado, de la forma más real posible, para presentar situaciones de mayor carga en la red y así poder planificar y decidir futuras ampliaciones.

Son lo equipos más completos para comprobar el funcionamiento de los sistemas de comunicaciones. Tienen capacidad para decodificar e interpretar protocolos de hasta nivel 7 (aplicación). A veces estos equipos son configurables por módulos de tal forma que se elige su configuración en función de los protocolos que implemente la red en particular.

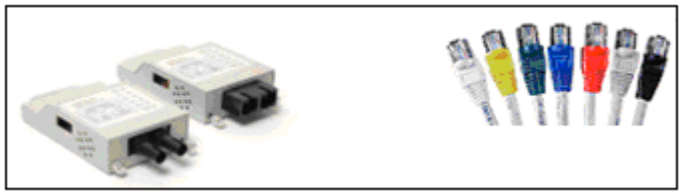


Fig. 24 Analizadores de red

3.4.5. Analizadores de protocolos.

El analizador de protocolos debe analizar la información y mostrarla de forma clara y completa al usuario en cada uno de los siete niveles del modelo OSI (figura 25).

Fig. 25 Analizadores de protocolos

Las funciones básicas que debe tener un analizador de protocolos son:

- Debe capturar las tramas de forma sofisticada mediante filtros definibles por el usuario, para obtener solamente aquellas que no pueden ser útiles para resolver el problema.
- La decodificación debe hacerla de forma clara, separando la información de cada uno de los niveles, interpretando el significado dentro de la comunicación, de cada una de las tramas del canal que ha intercambiado.
- Disponer de un amplio rango de protocolos para decodificar, por lo menos que tenga los generalmente más usados y la posibilidad de que el usuario defina otros nuevos protocolos.

El analizador de protocolos es una herramienta orientada a la comprobación del funcionamiento de los protocolos. Por medio del mismo se pueden detectar ineficiencias del protocolo en aplicaciones concretas.

El usuario del analizador de protocolos debe tener un conocimiento profundo del protocolo a analizar. El principal uso que se le da, es la captura de tráfico en situaciones conflictivas para que posteriormente sea analizado por personas expertas en el protocolo considerado (figura 26).

Fig. 26 Analizadores de protocolos II

CAPITULO IV. SOFTWARE DE MONITOREO.

4.1. PRUEBA Y EVALUACIÓN DE LAS HERRAMIENTAS DEL SOFTWARE DE MONITOREO DE LAS REDES DE COMPUTADORAS.

La diseminación y la utilización intensiva de los recursos de computadora e información distribuida electrónica, almacenados en equipos diferentes e instalados en lugares y organizaciones diferentes ha llegado a ser cada vez más grande en las sociedades humanas modernas. La tendencia actual es usar sistemas de información distribuida, inclusive aplicaciones, las bases de datos, el equipo de la computadora, los servidores, las computadoras personales y otro equipo conectado vía red, el acceso que proporciona a la información y servicios a través de una computadora en red. La tecnología de la red de computadoras ha llegado a ser la parte de sociedades modernas, configurando la infraestructura básica para la implementación del paradigma que dirige a la sociedad de la información. En esta nueva sociedad, los ciudadanos y las organizaciones estarán adoptando progresivamente en sus relaciones, alguna forma de recursos que son interconectados a otros recursos de la misma clase, proporcionando un nivel más grande de integración entre actividades humanas y procesos automatizados en varios segmentos de la sociedad.

El Internet es un ejemplo típico de esta integración que proporciona la conexión a una red global de información, interconectando miles de computadoras localizadas por todas partes del mundo. Los servicios disponibles por las redes de computadoras, son a un nivel (LAN) o nivel global (Internet), han llegado a ser más intensivamente usado por un número creciente de ciudadanos y hay un número constante, más grande y exigente de usuarios, que espera encontrar proveedores de servicio que reúnen los requisitos de la velocidad, la eficiencia y la confiabilidad. Llega a ser, por lo tanto, necesario asegurar que los sistemas de apoyo que proporcionan estos servicios en las redes, incluyendo personal, herramientas de software, equipos y comunicación, son capaces de reunir los requisitos de nivel de certeza y calidad de los usuarios. Acerca de la red física y la topología instalada, los servicios de apoyo deben asegurar también la estabilidad de la red en los problemas que proporciona la respuesta apropiada a resolverlos. En este nivel, los problemas comunes son: los desperfectos de hardware o software, información intensiva de tráfico y tráfico intensivo en la comunicación.

Para asegurar la funcionalidad de la red, es necesario emplear herramientas de software para la administración del sistema que permitirá el control de funciones básicas como control de usuarios, el inventario de programas, el control de acceso, así como también controlando la actividad de la red. Para proporcionar control de administración en todo funcionamiento de la red, es necesario tener en cuenta las características del ancho de banda de la red. El primer paso a seguir como objetivo es conocer la topología adoptada en el nivel

lógico y físico. Para llevarse a cabo esta actividad es necesario aplicar en la red, los conceptos de la separación y caracterización por capas, definido por la (ISO) organización Internacional de Estándares como Modelo de Referencia OSI, que permite la conexión entre sistemas diferentes, definiendo los estándares y protocolos que se deban adoptar para asegurar la comunicación entre hardware y los procesos relacionados.

Una de las funciones principales que se deben de realizar por una administración de redes es el controlar, tener en cuenta la visualización y el registro de los parámetros de las operaciones de la red. Un conjunto de criterios de selección se desarrolló y una aplicación práctica de herramientas escogidas de software en una red verdadera, implicar tres niveles de monitoreo, comprensión de: estado de red, actividad de la LAN y el uso de links de Internet. Las herramientas de monitoreo adoptadas proveen una manera estructurada para llevar el diagnóstico y soluciones para la mayor parte de los problemas.

4.1.1. Monitoreo de computadoras.

Las principales acciones en la administración de las redes son: monitoreo, el control de varios componentes y la intervención inmediata en la presencia de uno o de más desperfectos. Una red generalmente compuesta de equipos de varios suministradores, emplea una gran variedad de protocolos, los cuales giran en las tareas de administración gran complejidad magnífica.

Monitorear es un acto continuo para la observación del sistema y de la información almacenada. Un sistema de comunicación, debido a su importancia, se debe de monitorear para producir una visión actualizada de su comportamiento. Con los datos obtenidos de la observación continua, un modelo de comportamiento puede ser generado, ayudando a resolver problemas existentes y producir información que puede ser usada para pronosticar las necesidades para expansiones o inversiones futuras en telecomunicaciones.

El tráfico en una red puede ser representado básicamente por el número de clientes, el número de paquetes que fluye en la red y el número de colisiones. En redes basadas en Ethernet, como un resultado de un gran número de accesos de los clientes en la red, habrá un número creciente de paquetes y la probabilidad de choques.

Basado en estos parámetros y los conceptos de administración general, un agente de monitoreo y un agente administrador ha llegado a ser necesario. Estos agentes serán responsables por la interpretación de los datos recolectados cambiando la operación de los sistemas o estableciendo nuevas reglas para modificaciones que pueden introducirse en la red, para resolver los problemas y para mejorar el desempeño de la red, (figura 27) ilustra a estos agentes básicos.

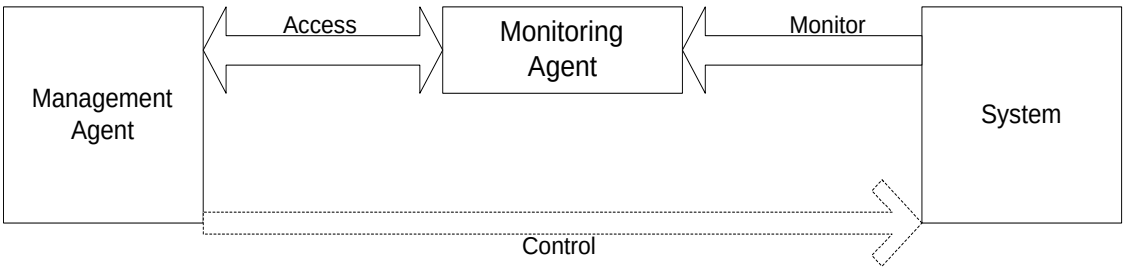


Fig. 27 Agentes de monitoreo

Hay una gran variedad de aplicaciones e implementaciones en los agentes de monitoreo en una red (figura 28), sin embargo, están las funciones comunes para casi todos los mecanismos como:

a) Leer: establece un contacto directo con el ambiente de comunicación e información que adquiere en los puertos de la red.
b) Filtrar: remover información y retener información seleccionada.
c) Recolectar: almacenar los datos filtrados, temporalmente o permanentemente.
d) Reportar: los datos suministrados son almacenados para una aplicación, cuando se soliciten.

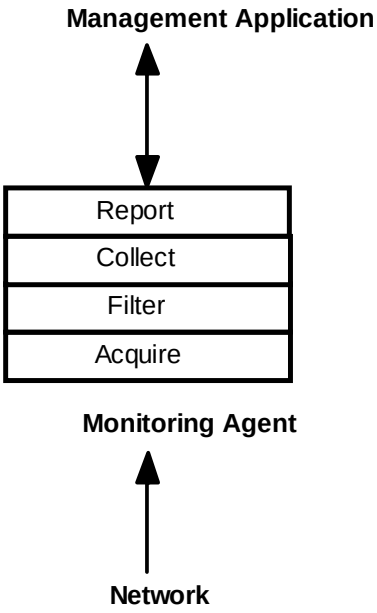


Fig. 28 Monitoreo de funciones

4.1.2. Monitoreo en capas.

Un factor de distinción entre los agentes de monitoreo son la capas en el modelo OSI que esta operando. Un agente de monitoreo es generalmente proyectado para operar solamente en una sola capa (o capas específicas). Las capas de la red, cuando están definidas por el modelo OSI, son clasificadas por sus funciones correspondientes e información para ser monitoreadas:

a) Red: reporta que circuitos están activos (up) o inactivos (down).
b) Transporte: mide el nivel de actividad en la red.

c) Sesión: caracterizan la suma de la carga neta en el nivel de usuarios y aplicación.
d) Aplicación: identifica los errores en las aplicaciones cliente/ servidor.

Monitorear una LAN propone medir la actividad interna de la red mostrando todas las características del tráfico en las capas de transporte y sesión. Finalmente, monitoreando los links de las WAN, muestra información cuantitativamente y cualitativamente en la capa de transporte, usada para la conexión de canales entre MAN o Intranet y canales Internet.

Uno de los asuntos principales puede ser dirigidos por la especificación de un sistema de monitoreo son los agentes. Dos enfoques posibles para agentes que puede ser empleado usando el concepto de dos tipos de monitores: integrado y externo.

4.1.3. Agentes integrados.

Algunos estados de la red pueden solamente ser obtenidos si los agentes de monitoreo integran los componentes de la red que están siendo monitoreados o si están insertados en este. Estos agentes son llamados agentes integrados y su ventaja principal se fía de la calidad de la información adquirida, que es verdaderamente, rápido y exacto. El principal problema de este enfoque es el uso del ancho de banda para

transmitir información de monitoreo, esto puede generar tráfico no deseable.

Cuando el equipo de res esta suministrado con capacidades de administración, esto es, las estaciones de trabajo, los servidores, lo switches, los routers, los gateways, las referencias relacionadas al hardware se pueden usar remotamente para propósitos de administración, tal como administran los estados de la red, configuran ya alteran las características del sistema. Esa implementación es posible usando protocolos diseñados para este propósito.

SNMP (Simple Network Management Protocol) es el protocolo para la administración recomendado para la administración de redes TCP/ IP (figura 29). Definido en el nivel de la aplicación. Las especificaciones de SNMP se contienen en RFC 1157.

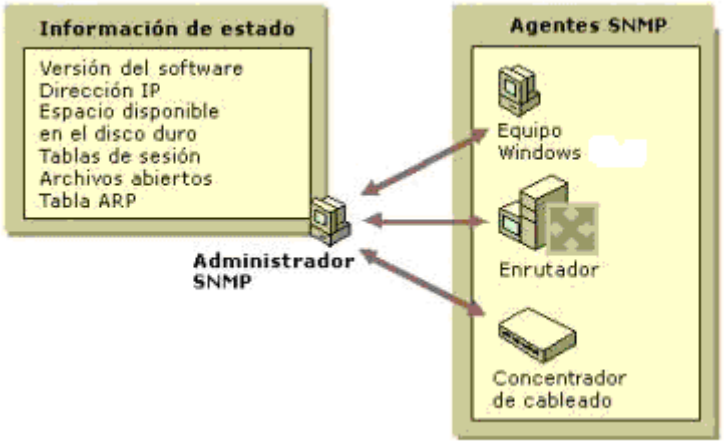


Fig. 29 SNMP

SNMP proporciona un método de administración de hosts de redes como concentradores, puentes, routers y equipos de servidor o estaciones de trabajo desde un equipo central que ejecuta un software de administración de redes. SNMP realiza servicios de administración mediante una arquitectura distribuida de sistemas de administración y agentes.

Sistema de Administración: Host activo en la red que ejecuta el software de administración de Protocolo Simple de Administración de Redes (SNMP). Este software solicita información a los agentes SNMP. El sistema de administración se llama también consola de administración.

Agentes: equipo que ejecuta software agente de SNMP. En la implementación de SNMP en Windows, la información de agente incluye comentarios acerca del usuario, la ubicación física del equipo y los tipos de servicio que se notifican dependiendo de la configuración del equipo.

SNMP puede usarse para:

- Configurar equipos remotos. La información de configuración puede enviarse a cada host conectado a la red desde el sistema de administración.
- Supervisar el rendimiento de la red. Puede hacer un seguimiento de la velocidad de procesamiento y el rendimiento de la red, y recopilar información acerca de la transmisión de datos.

- Detectar errores en la red o accesos inadecuados. Puede configurar las alarmas que se desencadenarán en los dispositivos de red cuando se produzcan ciertos sucesos. Cuando se dispara una alarma, el dispositivo envía un mensaje de suceso al sistema de administración. Entre las causas más frecuentes de alarma se puede mencionar cuando un dispositivo se cierra y se reinicia, un error de un vínculo detectado en un enrutador y un acceso inadecuado.
- Auditar el uso de la red. Puede supervisar el uso general de la red para identificar el acceso de un grupo o usuario, y los tipos de uso de servicios y dispositivos de la red.

Tanto los agentes como los sistemas de administración utilizan mensajes de SNMP para inspeccionar y comunicar información del host. Los mensajes de SNMP se envían mediante el Protocolo de Datagramas de Usuarios (UDP). El protocolo de Internet (IP) se utiliza para enlutar mensajes entre el sistema de administración y el host.

La información que pide el sistema de administración se encuentra en una base de datos de información de administración (MIB). La base de datos MIB contiene varios tipos de información acerca de un equipo conectado a la red, como la versión del software de red que se ejecuta en ese equipo y el espacio disponible en el disco duro.

4.1.4. Agentes externos.

En el monitoreo de LANs, es posible meter un solo mecanismo en un elemento principal que es capaz de controlar las comunicaciones entre un gran número de equipos. Este agente de monitoreo externo, permite también el monitoreo pasivo, sin intervenir en el flujo normal de comunicación por la red. Este enfoque, ampliamente empleado en redes locales, tiene varias limitaciones relacionadas con la habilidad de monitorear e interpretar mensajes protocolos de red que fluyen con un gran número de sistemas de comunicaciones en tiempo real.

El agente de monitoreo externo es implementado en algún componente externo para alcanzar el monitoreo por la colección de información que se transmite por la red. Desde que los agentes son pasivos y fácilmente adaptables, son usados ampliamente en redes locales.

Los agentes externos se encuentran comúnmente integrados en las aplicaciones de administración, formando herramientas de software, instalados en un host conectado a la red, tiene la habilidad de “escuchar” la transmisión y seleccionar información colectada usando filtros. Algunas ventajas de los agentes externos son:

- Se puede implementar en un hardware específico sin competir por recursos con la red o la aplicación.

- Un solo agente de monitoreo es capaz de suministrar información de una gran variedad de sistemas operativos y aplicaciones.
- Es un componente independiente, el agente de monitoreo puede ser modificado fácilmente y puede ser extendido.
- Los desperfectos eventuales de los agentes tienen un abaja probabilidad de causar los desperfectos en los servicios de la red.

Los inconvenientes principales son:

- Como observadores en la red “ellos detectan” todo lo que fluye a través y, es un dominio separado, ellos constituyen la fuente potencial de desperfectos con relación a la privacidad de información que fluye por la red.
- No hay garantía que la información completa es una representación necesaria de los estados de los componentes controlados, ellos representan sólo un enfoque.
- Debido a la gran cantidad de datos recolectados en los sistemas, ellos necesitan tener alto desempeño en el análisis de la función y en el almacenamiento de datos.

4.1.5. Parámetros de evaluación.

A continuación se presentarán los puntos más importantes que se tomaron en cuenta para seleccionar el software que cumple con los requerimientos esperados.

- Procedimiento de instalación. Analiza el procedimiento para la instalación del programa. Este parámetro considera el número de las variables para la configuración y el grado de la dificultad representado por el proceso de la instalación.
- Herramientas de análisis de datos. Identifica la existencia de las herramientas para el análisis de datos. Este parámetro de la evaluación es de gran importancia puesto que las herramientas disponibles pueden facilitar el análisis de los datos recolectados y generar los resultados más eficientemente.
- Interfaz de usuario. Analiza la calidad de la interfaz para el usuario, identificando el grado de sencillez para tener acceso a las características y a los recursos del programa.
- Número de alarmas. Identifica la disponibilidad de las alarmas para señalar al personal de la dirección de la red, la ocurrencia de los defectos y la emisión de alertas.
- Soporte para la interfaz de Point-to-Point: identifica la disponibilidad de la ayuda de la interfaz de Point-to-Point teniendo en cuenta el análisis de tráfico en este tipo de interfaz.

4.2. MONITORIZADORES DE RED.

4.2.1. Observer.

Observer es un analizador flexible. Un administrador de redes o un técnico del área de soporte, sabe que un analizador de red es una herramienta necesaria para cuando se presentan problemas en la red o cuando necesita saber que tan bien o tan ocupada está la red (figura 30). [1]

Características:

- Gran capacidad de interpretación y decodificación de protocolos.
- Útiles comentarios del sistema.
- Gran versatilidad y facilidad de manejo de ventanas para determinar problemas.
- Excelente utilidad y claridad de sus reportes.

Observer le permite introducirse al nivel de paquetes individuales hasta obtener vistas generales de la actividad de la red. Ofreciendo gran diversidad de niveles de revisión. Monitorea los nodos de la red, descubriendo su disponibilidad y rendimiento, produce estadísticas útiles de las actividades que se realizan en la red.

[1] www.integracion-de-sistemas.com/analisis-y-monitoreo-de-redes.html

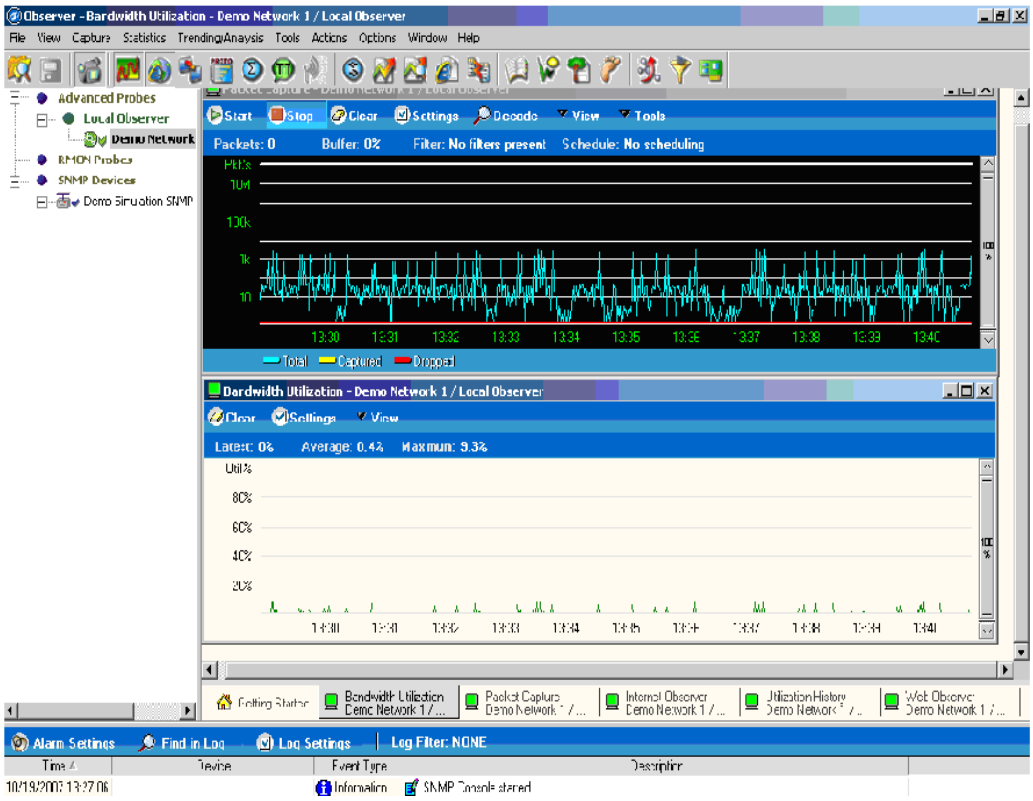


Fig. 30 Observer

Anteriormente se hicieron menciones de características importantes de este software, pero al momento de llevarlo a prueba como una versión trial, no mostró dichas características y los días que estuvo de prueba no mostró ninguna alerta.

4.2.2. Ethereal. [2]

Ethereal es un analizador de paquetes de red. Un analizador de red que captura paquetes de red y despliega la información del paquete tan detallada como sea posible (figura 31).

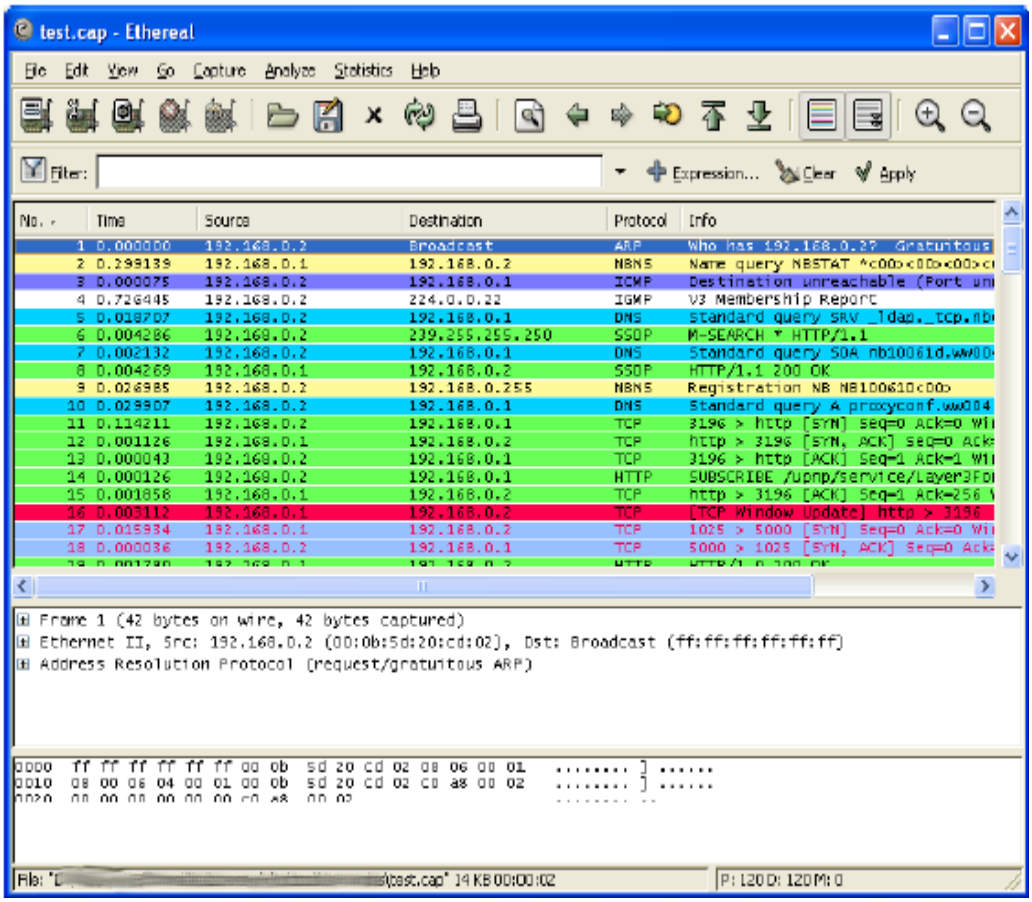


Fig. 31 Ethereal

[2] www.ethereal.com

Se puede pensar de un analizador de paquetes de red como un instrumento de medición que se usa para conocer que esta pasando dentro de un cable de red, como un voltímetro se usa por un electricista para examinar que esta pasando dentro de un cable eléctrico.

Ethereal es utilizado para:

- Los administradores de redes lo utilizan para localizar problemas de la red.
- Los ingenieros de la seguridad de redes lo utilizan para examinar la seguridad de la red.
- Los desarrolladores lo utilizan para eliminar errores en las implementaciones de protocolo.
- Las personas lo utilizan para aprender protocolos internos de la red.

Para comenzar la captura se debe seleccionar la interfaz (tarjeta de red) desde que se realizará la captura (figura 32). Para esto se debe ir a “Capture--Options--Interface” y seleccionar la tarjeta de red adecuada. Luego haciendo clic en “Start” se puede dar comienza a la captura y aparece un diálogo con la cuenta de los paquetes capturados y algunos datos estadísticos.

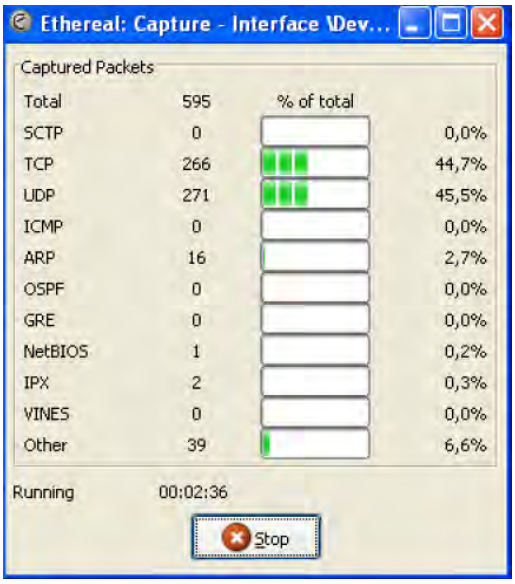


Fig. 32 Captura de paquetes

Cuando se desee dar por terminada la captura (haciendo clic en “Stop” en el diálogo antes mencionado). A continuación se mostrará una nueva pantalla con la información capturada en tres secciones que se muestran a continuación (figura 33):

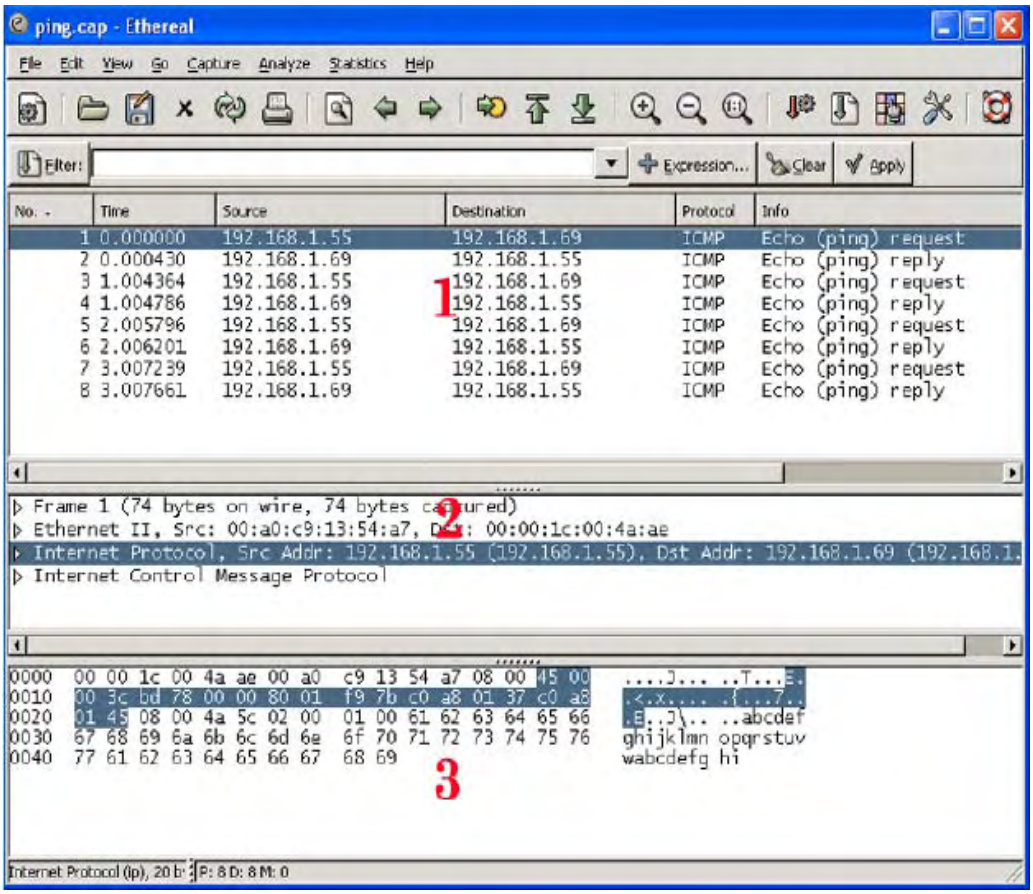


Fig. 33 Información capturada

Se pueden observar tres secciones principales. A continuación se explica cada una de las secciones:

1. Contiene la lista de paquetes individuales con su información más relevante. En “Origen” (“Source”) y “Destino” (“Destination”) se muestra la dirección IP correspondiente. Si algún paquete no contiene direcciones de capa 3, entonces mostraría direcciones de capa 2, es decir, direcciones MAC. En “Protocolo” (“Protocol”) muestra información relativa al protocolo.

2. En esta sección se puede observar los detalles del protocolo seleccionado en la sección 1. Se observa el contenido de cada uno de los encabezados de cada capa. Se puede observar información relativa a capa 1 en la línea que comienza con “frame 1”. La línea que comienza con “Ethernet II” contiene información relativa a este protocolo y así sucesivamente.
3. En la última sección se observan los paquetes en bruto, es decir, tal y como fueron capturados en la tarjeta de red. En realidad es la misma información que se presenta en las dos secciones anteriores, pero sin acomodar la información de forma legible al ojo humano.

Usando los filtros de display, se puede elegir qué paquetes deberían o no exhibirse en pantalla. Esto es útil para mostrar sólo los paquetes que se deseen ver.

También cuenta con filtros de captura que nos permiten indicar en qué tipos de paquetes estamos interesados. Por medio de estos filtros, el sistema operativo entregará a Ethereal solo los paquetes que cumplen con los requisitos indicados.

4.2.3. Capsa.

Capsa es un programa que monitoriza y analiza todo el tráfico que circula por una red capturando sus paquetes TCP/IP en tiempo real. El programa monitorea el tráfico de la red de trabajo transmitido por un local en una red de área local (figura 34); de esta manera se puede determinar y solucionar problemas de red. Capsa tiene la capacidad de capturar paquetes y realizar acertados análisis de datos.

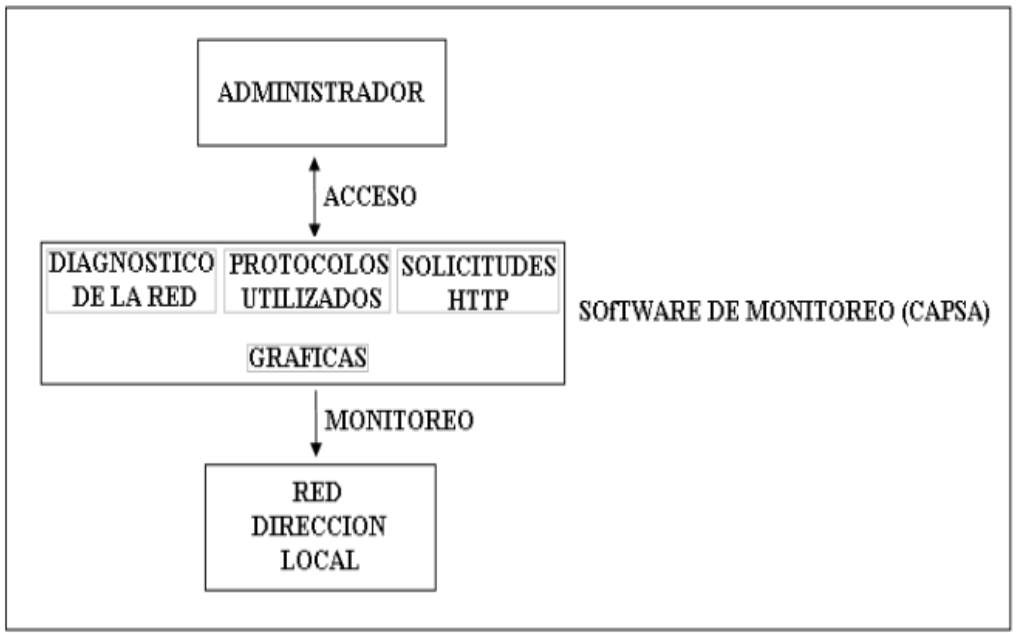


Fig. 34. Monitoreo de tráfico de una red de trabajo.

Con la ayuda de Capsa, se pueden lograr fácilmente las siguientes tareas:

- Análisis del tráfico de la red.
- Monitoreo de la comunicación de la red.
- Diagnostico de los problemas de la red.
- Análisis de la seguridad de red.
- Detección del desempeño de la red.

Características:

- Análisis de redes.
- Captura de paquetes.
- Muestra de estadísticas detalladas de conexiones IP.
- Análisis de tráfico de red.
- Análisis de paquetes.
- Permite ver protocolos de distribución, distribución de tamaño de los paquetes, con tablas y gráficos. Genera reportes estadísticos.

Diagnosticar. La opción de de diagnósticos, nos dará información acerca del estado de la red. Por medio de eventos se sabrán los problemas que existen en la red, conocer el origen y destino del evento (figura 35).

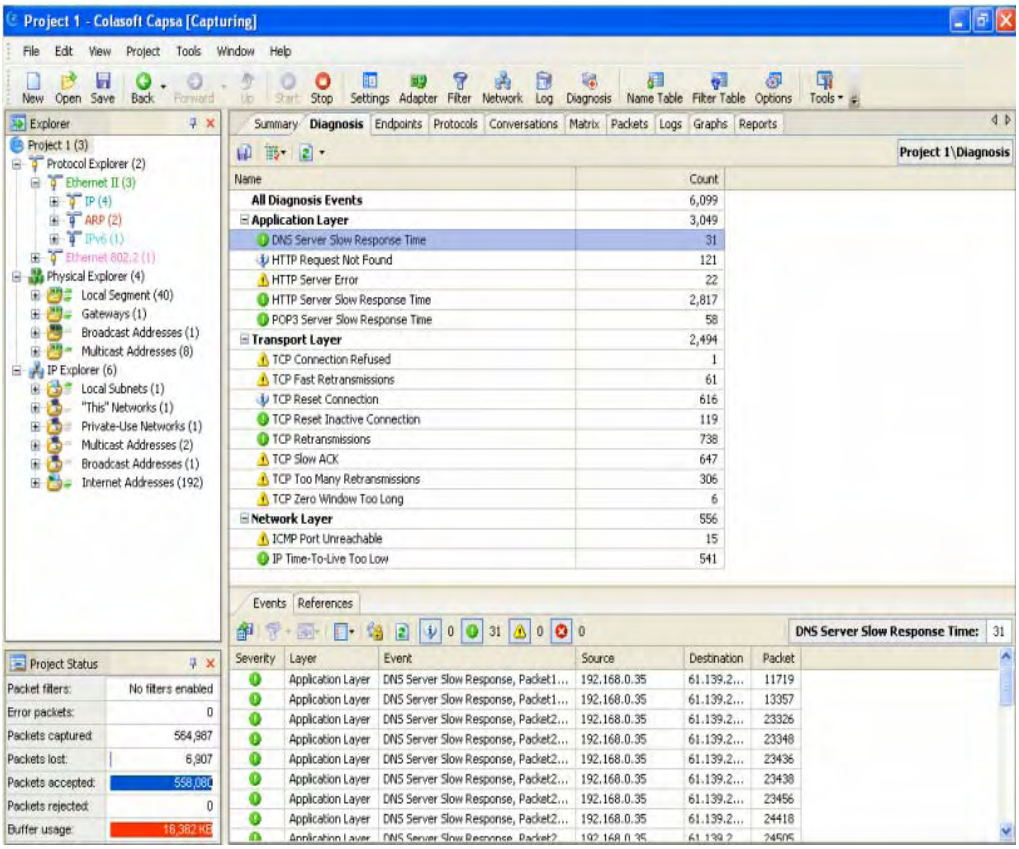


Fig. 35. Diagnosticar.

Estadísticas de protocolos. Provee estadísticas de los protocolos utilizados por las redes de comunicaciones (figura 36).

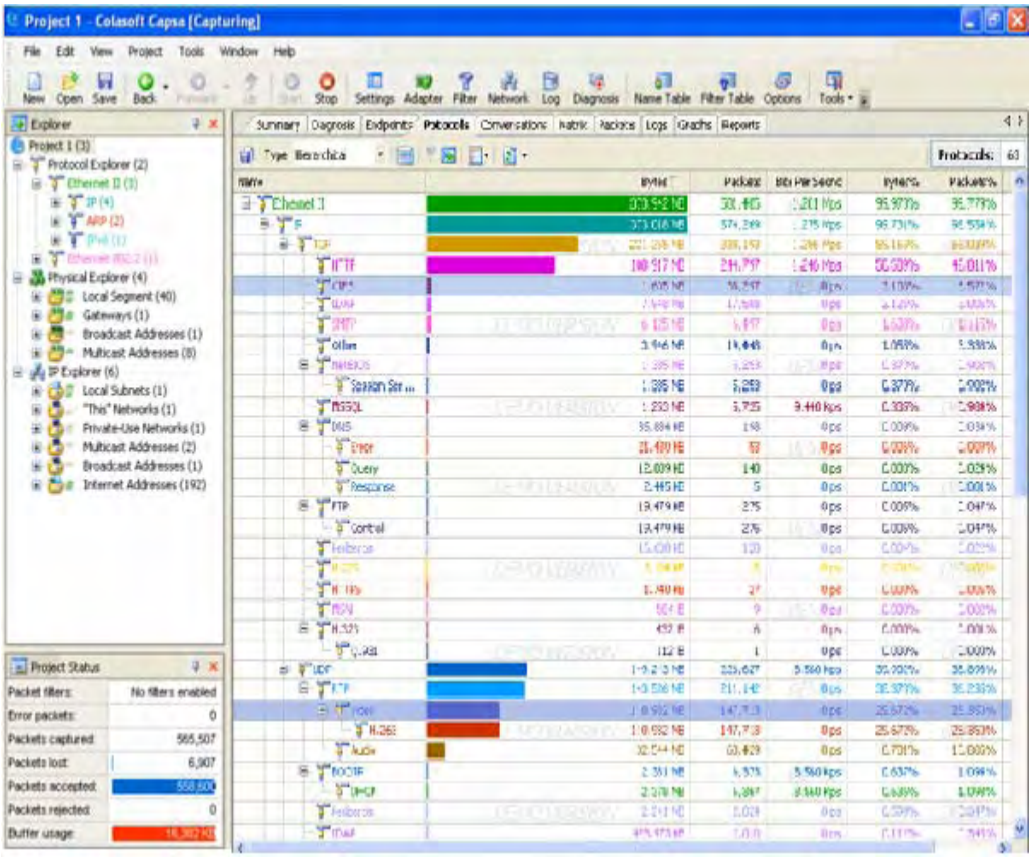


Fig. 36. Estadísticas de Protocolos.

La figura nos muestra los protocolos que esta utilizando la red, total de bytes usados de cada protocolo, paquetes, etc.

Logs. En esta opción (figura 37) se muestran direcciones que están siendo accesadas por los usuarios, así como la hora en la que accesan.

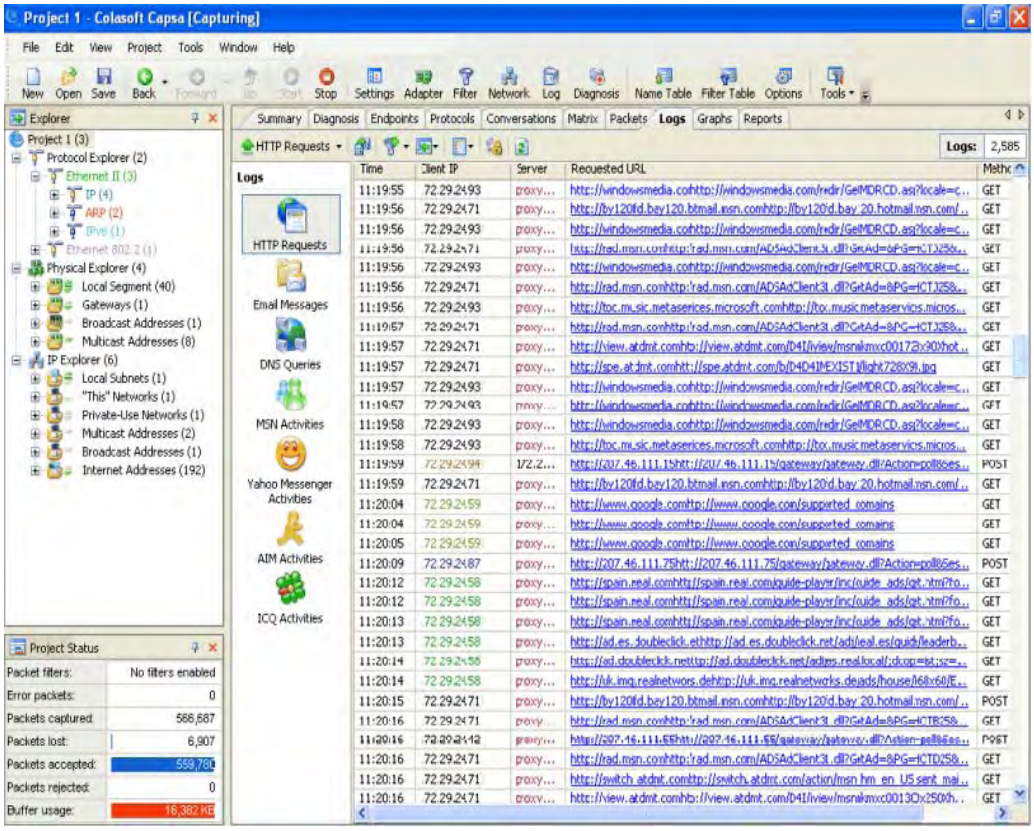


Fig. 37. Accesos.

Gráficas. Despliegue gráfico de información estadística de toda la red o de nodos específicos, provee múltiples gráficos y opciones de visualización (figura 38 y 39).

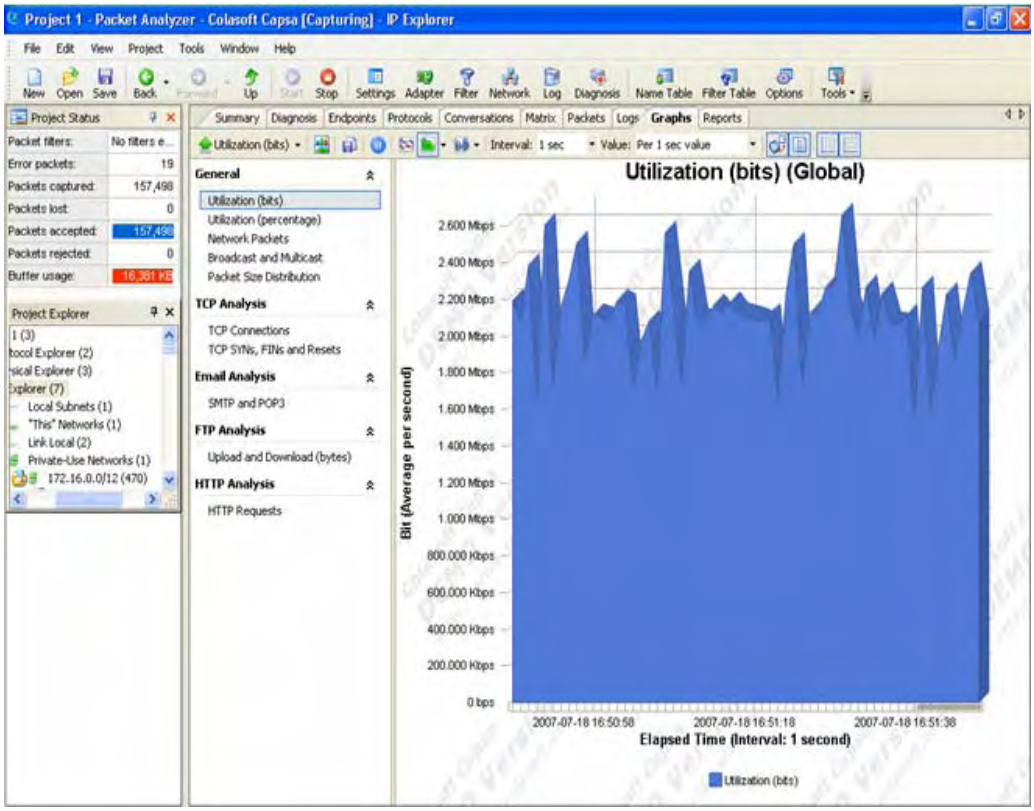


Fig. 38. Gráficas.

Permite ver gráficas de la utilización de la red o solo de algún nodo específico en bits o en porcentaje, también muestra gráficas de los paquetes cantidad de paquetes utilizados, distribución del tamaño de los paquetes.

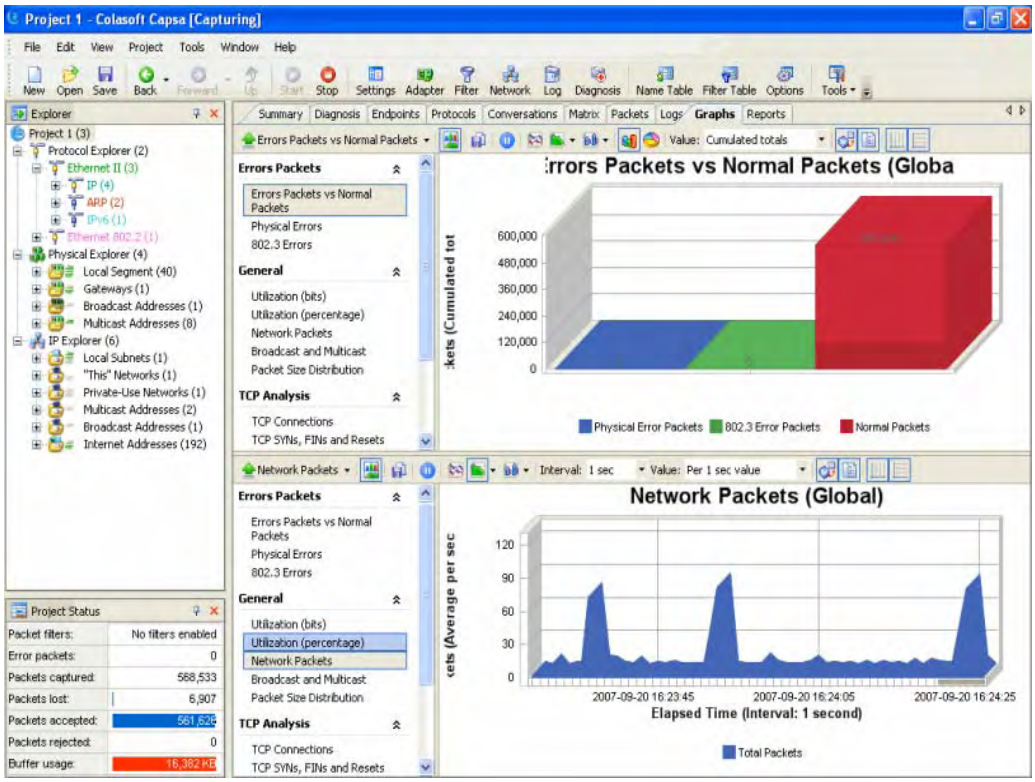


Fig. 39. Gráficas II.

4.3. SOFTWARE DE MONITOREO SELECCIONADO.

Tas la investigación de diferentes software solo se escogieron tres para investigarlos con más profundidad ya que fueron los mejores para este propósito. No obstante el mejor a mi criterio y a las investigaciones realizadas Capsa es el mejor porque cumple con las características deseadas. Todo eso es en base a que estos software no dan lo mejor de si, por ser versiones Triales o Demos.

CAPITULO V. MONITOREO EN LA RED DE LA DIRECCION LOCAL GUERRERO DE LA C. N. A.

5.1. MONITOREO EN LA RED DE LA DIRECCION LOCAL GUERRERO DE LA CONAGUA.

El monitoreo de la red de la Comisión Nacional del Agua se realizo de lunes a viernes de 9:00 A.M. a 6:00 P.M., durante el mes de Agosto de 2007.

Los resultados obtenidos del análisis se muestran a continuación.

5.2. PÁGINAS MÁS VISITADAS.

PROTOCOLO	URL	CONTENIDO
http	www.veautos.com.mx	Sitio de venta, compra autos nuevos, usados
http	www.kala.com.mx	Horóscopos
http	www.zango.com	Sitio de juegos
http	www.jarochos.net	Portal de entretenimiento
http	www.tvazteca.com.mx	Portal de entretenimiento
http	www.foxsports.com	Sitio de deportes
http	www.esmas.com	Portal de entretenimiento
http	www.videojuegos.com	Sitio de juegos
http	www.radiocentro.com.mx	Radio por Internet
http	www.diariodeguerrero.com.mx	Periódico en línea
http	www.juegos.com	Sitio de juegos
http	www.laz.com.mx	Radio por Internet
http	www.vefutbol.com.mx	Sitio de fútbol
http	www.conference.com.mx	Sitio de capacitación empresarial y gubernamental
http	www.lfai.org.mx	Sitio del Instituto

		Federal de Acceso a la Información Pública
http	www.mercadolibre.com.mx	Portal de ventas, compras de gran variedad de artículos
http	www.blogger.com	Sitio de blogs
http	www.elrellano.com	Sitio de videos
http	www.extudiantes.com	Portal de estudiantes y sociedad chilpancingueña
http	www.youtube.com	Sitio de videos
http	www.bancomer.com.mx	Sitio bancario
http	www.surdeacapulco.com.mx	Periódico en línea
http	www.latinchat.com	Chat
http	www.univision.com	Portal de entretenimiento
	www.google.com.mx	Buscador Web
http	www.forolatino.com	Venta de discos de música
http	www.disneylatino.com	Sitio para niños
http	www.paypal.com./es	Sitio de comercio
http	www.hotmail.com.mx	Correo electrónico
http	www.gamenext.es	Sitio de Juegos
http	www.pronosticos.gob.mx	Sitio de consulta de sorteos

http	www.windows media.com	Sitio de música
http	www.hitsfm.com	Sitio de música
http	www.universal.com	Portal de entretenimiento
http	www.tubreveespacio.com	Sitio de pensamientos y reflexiones
http	www.cartoonnetwork.com.mx	Sitio para niños
http	www.latino.msn.com	Portal de entretenimiento
http	www.lyricsplugin.com	Sitio de música

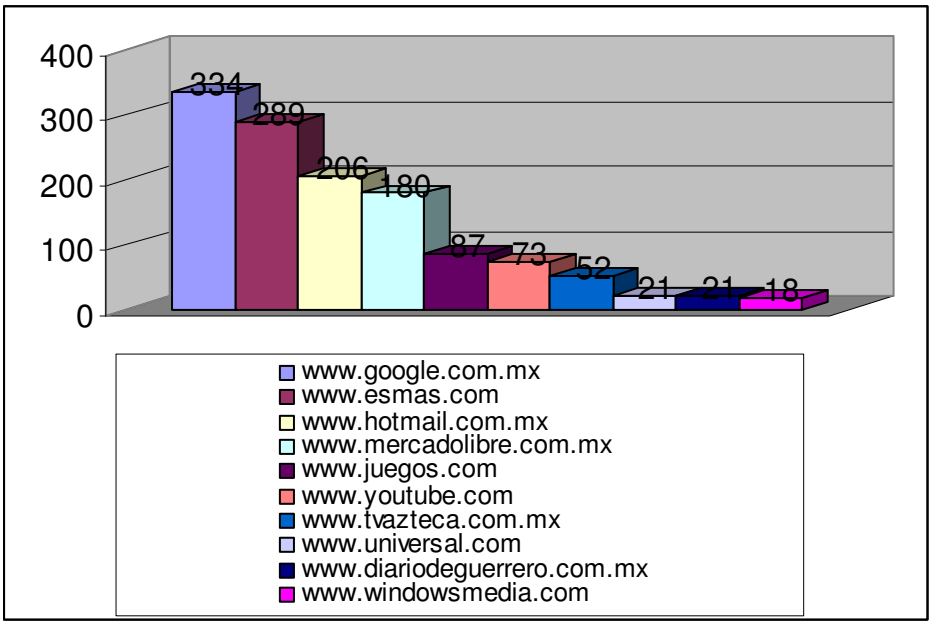
Tabla 1. Páginas más accesadas

En la tabla 1, están las páginas que más fueron accesadas en la Dirección Local en el mes de agosto de 2007.

5.2.1. Las 10 páginas más vistas.

URL	NO. VISITAS
www.google.com.mx	334
www.esmas.com	289
www.hotmail.com.mx	206
www.mercadolibre.com.mx	180
www.juegos.com	87
www.youtube.com	73
www.tvazteca.com.mx	52
www.universal.com	21
www.diariodeguerrero.com.mx	21
www.windowsmedia.com	18

Tabla 2. 10 páginas más vistas.



Gráfica 1. 10 Páginas más vistas.

La gráfica 1 muestra las 1º páginas más vistas en la Dirección Local.

5.3. PAGINAS VISITADAS CON CONTENIDOS PARA ADULTOS.

URL	DIRECCION IP	AREA
www.sexywebcam.com	172.29.24.16	Subdirección de Administración
www.pajilleros.com	172.29.24.16	Subdirección de Administración
www.elreyano.com	172.29.24.16	Subdirección de Administración
www.assallworld.com	172.29.24.20	Subdirección de Administración
www.quantcast,com/onlyfreepornvideos.com	172.29.24.20	Subdirección de Administración
www.zazoum.com	179.29.24.20	Subdirección de Administración
www.ballhoneys.com	179.29.24.20	Subdirección de

		Administración
www.sexojovencitas.es	172.29.24.61	Subdirección de Administración del Agua
www.colegialas-indecentes.com	172.29.24.61	Subdirección de Administración del Agua
www.bamodels.com	172.29.24.61	Subdirección de Administración del Agua
www.zazoum.com	172.29.24.85	Subdirección de Técnica
www.fling.com	172.29.24.97	Subdirección Jurídica
www.deuvosguard.com	172.29.24.98	Subdirección Jurídica
www.sexo-patas.com	172.29.24.98	Subdirección Jurídica
www.centerfoldgalleries.com	172.29.24.105	Consejos de Cuenca
www.desnudasmodelos.com	172.29.24.105	Consejos de Cuenca
www.danni.com	172.29.24.105	Consejos de Cuenca

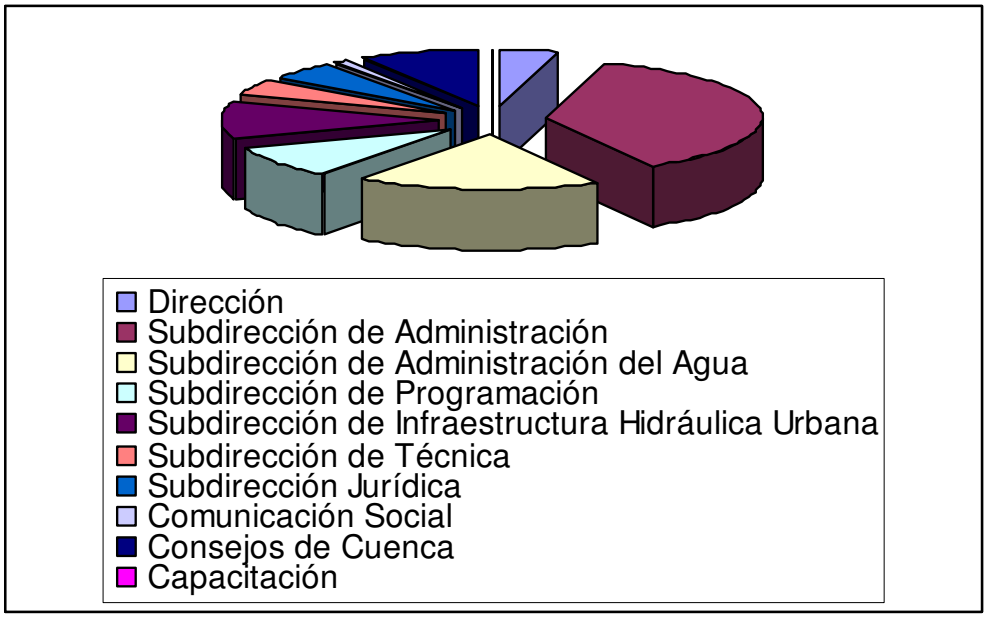
www.nastydirectory.com/m/macandbumble	179.29.24.105	Consejos de Cuenca
www.euforia.com	172.29.24.116	Consejos de Cuenca
www.adultfriender.com	172.29.25.116	Consejos de Cuenca
www.swingersmexico.com.mx	172.29.24.116	Consejos de Cuenca

Tabla 3. Páginas visitadas con contenido para adultos.

5.4. ACCESOS A INTERNET POR ÁREA.

AREA	NO. ACCESOS
Dirección	71
Subdirección de Administración	579
Subdirección de Administración del Agua	283
Subdirección de Programación	147
Subdirección de Infraestructura Hidráulica Urbana	168
Subdirección de Técnica	75
Subdirección Jurídica	75
Comunicación Social	19
Consejos de Cuenca	138
Capacitación	0

Tabla 4. Accesos a Internet por área.



Gráfica 2. Accesos a Internet por área.

La gráfica 2 muestra todos los accesos a Internet por área.

5.5. ACCESOS A INTRANET POR AREA.

AREA	NO. ACCESOS
Dirección	53
Subdirección de Administración	194
Subdirección de Administración del Agua	41
Subdirección de Programación	11
Subdirección de Infraestructura Hidráulica Urbana	48
Subdirección de Técnica	25
Subdirección Jurídica	30
Comunicación Social	27
Consejos de Cuenca	39
Capacitación	0

Tabla 5. Accesos a intranet por área.

Gráfica 3. Accesos a intranet por área

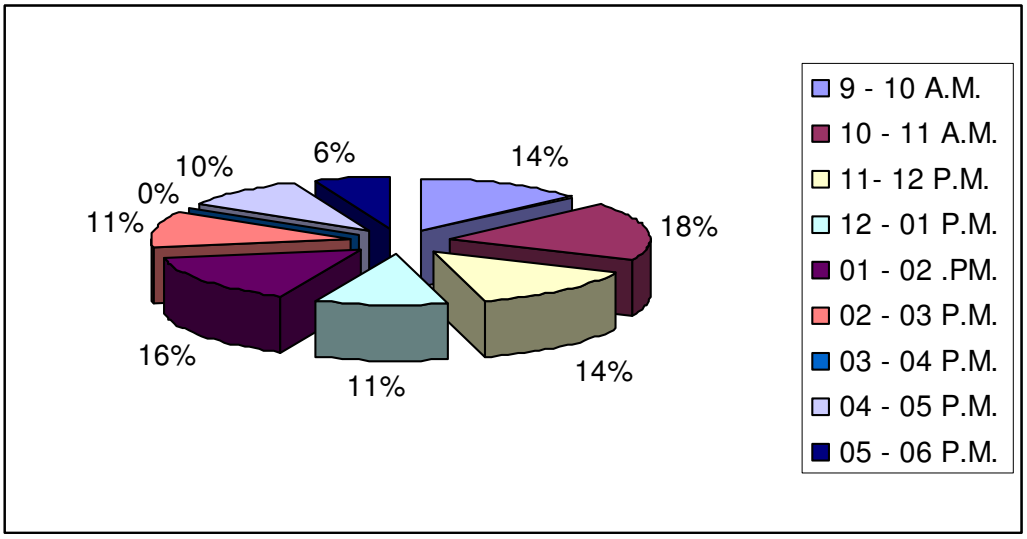
La gráfica 3 muestra todos los accesos a intranet por área.

5.6. PÁGINAS ACCESADAS POR DÍA.

La siguiente tabla muestra los accesos que se realizaron diariamente por hora, durante el mes de Agosto de 2007.

HORA	LUNES	MARTES	MIERCOLES	JUEVES	VIERNES	TOTAL
9 - 10 A.M.	43	68	55	58	54	278
10 - 11 A.M.	57	92	76	62	77	364
11- 12 P.M.	58	69	47	56	55	285
12 - 01 P.M.	44	50	23	48	54	219
01 - 02 .PM.	58	79	75	46	63	321
02 - 03 P.M.	48	41	56	40	47	232
03 - 04 P.M.	----	----	----	----	----	----
04 - 05 P.M.	31	34	76	24	37	202
05 - 06 P.M.	27	35	24	14	22	122

Tabla 6. Páginas accesadas por día.



Gráfica 4. Páginas accesadas diariamente por hora.

CAPITULO VI. POSIBLES SOLUCIONES.

6.1. POSIBLES SOLUCIONES.

Es importante de antemano, saber cuales son las opciones para solucionar el problema de utilización del ancho de banda, ya que en muchas de las ocasiones, a pesar de que se les dan las políticas para mejorar el ancho de banda al personal, no hacen nada para mejorarlo. Es por eso que es necesario tener equipos y software necesarios para ayudar a mantener una red eficiente y provechosa.

A continuación se darán a conocer algunos equipos y software que ayudarán de manera eficiente a controlar y mejorar el ancho de banda de la red de manera sustancial.

6.1.1. PacketShaper y Sitara.

Muchas aplicaciones corporativas utilizan de manera intensiva los enlaces WAN o conexiones a Internet con delegaciones remotas, proveedores o clientes. De manera que el tráfico de aplicaciones críticas se ve compartiendo recursos con otras aplicaciones menos críticas para los objetivos de la compañía. Los equipos de Sitara y Packeteer permiten la gestión del ancho de banda, transmitiendo los datos esenciales a una velocidad constante, con un ancho de banda reservado mientras que los datos menos urgentes siguen siendo

transmitidos pero utilizando menos recursos, de manera que ningún tipo de tráfico monopoliza el enlace.

6.2. PACKETSHAPER. [1]

Otra de las posibles soluciones podría ser utilizar un dispositivo que detecte y clasifique aplicaciones de red, realice un análisis, haga reparto de ancho de banda y además que realice reportes del comportamiento de la red. Este podría ser el PacketShaper de la empresa Packeteer, el dispositivo que a continuación se menciona cumple con las características antes mencionadas (figura 40).

Fig. 40. PacketShaper.

La serie PacketShaper es la solución diseñada para gestionar el funcionamiento de las aplicaciones.

[1] www.packeteer.com

PacketShaper pone a la disposición un proceso de cuatro pasos para gestionar el funcionamiento de las aplicaciones.

6.2.1. Detecta y clasifica las aplicaciones de red.

Clasifica de forma automática el tráfico de red en categorías basadas en la aplicación, protocolos, subred, URL o cualquier otro criterio, produciendo miles de categorías potenciales. Clasifica la información en base al nivel 7 del modelo OSI (figura 41).

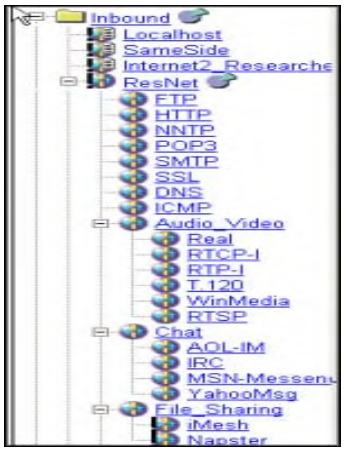


Fig. 41. Clasificación de información.

6.2.2. Analiza la conducta de la red.

Proporciona análisis detallado del funcionamiento de la aplicación y de la eficiencia de la red. Describe el uso del ancho de

banda en los momentos de mayor tráfico y de tráfico medio (figura 42). Analiza los tiempos de respuesta según sean producidos por retenciones de la red o por retenciones de los servidores. Clasifica los usuarios, las Web´s y las aplicaciones más frecuentes.

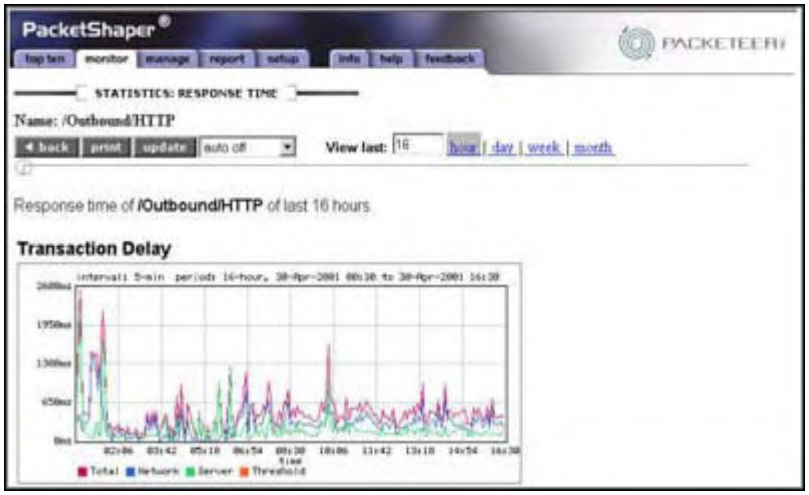


Fig. 42. Análisis de la red.

6.2.3. Refuerza el reparto del ancho de banda basado en políticas.

Con el reparto del ancho de banda en políticas y la distribución del tráfico, PacketShaper protege las aplicaciones críticas, reteniendo aquellas que son menos urgentes y optimizando el funcionamiento del enlace. Se especifican los mínimos y máximos de ancho de banda por sesión o por aplicación (figura 43). La tecnología TCP Rate Control de PacketShaper previene proactivamente la congestión de los flujos tanto

entrantes como salientes, eliminando los paquetes rechazados y las retransmisiones innecesarias.

Fig. 43. Reparto de ancho de banda

6.2.4. Realiza informes de funcionamiento de las aplicaciones.

La capacidad de realizar informes (tablas, gráficos, estadísticas, etc.) permite planificar actividades y disminuir el impacto de los cambios en las configuraciones (figura 44). Con acuerdos de nivel de servicio se pueden definir los funcionamientos de los estándares, comparar los rendimientos actuales con los objetivos y generar los informes acordados. Los sistemas de PacketShaper proporcionan monitoreo controlando las características que se proporciona a los administradores de la red con la inteligencia para controlar el

desempeño de la aplicación y llevar al máximo los recursos existentes de la red.

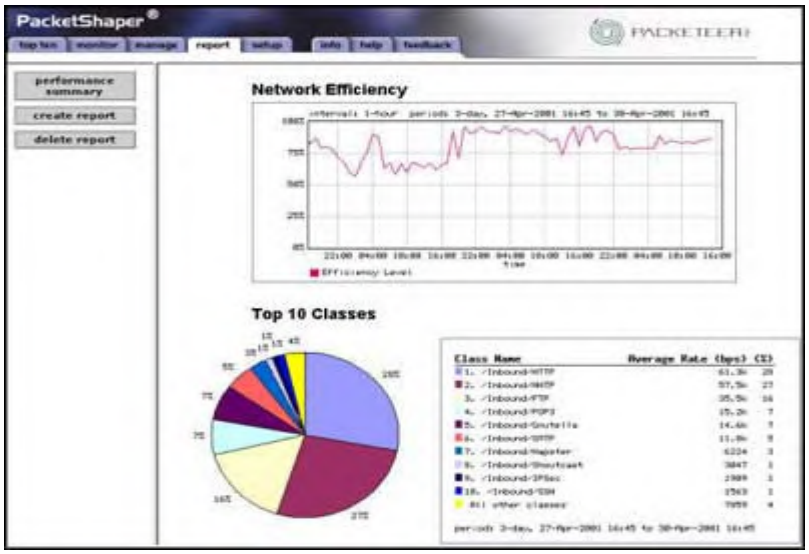


Fig. 44. Informes de funcionamiento de aplicaciones.

PacketShaper es instalado al lado de un router conectado a WAN, además este identifica el tráfico de la red y los tiempos de respuesta (figura 45).

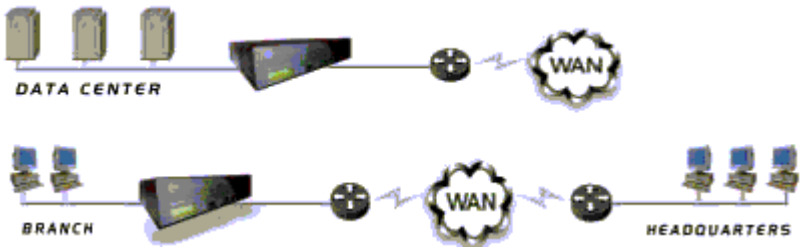


Fig. 45. PacketShaper.

6.3. SITARA. [2]

6.3.1. QoSWorks.

QoSWorks es la primera plataforma que integra todas las utilidades QoS que los administradores de red necesitan para priorizar y manejar el tráfico de red. Las compañías y proveedores de servicios QoSworks utilizan el ancho de banda más eficientemente, mejoran el servicio prestado a los usuarios y proporcionan un rendimiento medible para todas las aplicaciones. QoSWorks permite a la red proporcionar todos los recursos cuando éstos son necesarios.

Hoy en día, las redes IP transportan una importante mezcla de tráfico, el cual recibe, independientemente de su importancia para la empresa, la misma prioridad de entrega.

[2] www.sitaranetworks.com

El problema de priorizar y proteger tráfico crítico para le negocio es especialmente difícil en el extremo de la red, donde el ancho de banda es más limitado. En este sentido, incrementar la capacidad de la línea nonos garantizará el ancho de banda necesario para dar prioridad a las aplicaciones. La solución consiste en implementar. QoSWorks es una plataforma escalable diseñada específicamente para las necesidades de los proveedores de servicios. Incorpora todas las utilidades QoS que un administrador de red necesita para establecer políticas eficaces, incluyendo un clasificador de tráfico integrado, un administrador de políticas, el administrador de tráfico Sitara Accurate(que combina y coordina múltiples mecanismos de administración de tráfico QoS), una inteligente política de Web caching y monitorización, así como la obtención de informes en tiempo real.

Al incorporar múltiples utilidades QoS en una sola plataforma, se garantiza a los administradores de red que no sufrirán nunca más los problemas derivados de instalar y sincronizar múltiples productos QoS en red. Asimismo, QoSWorks es completamente transparente para las operaciones de redes existentes y no requiere software adicional ni cambios en el hardware de red, ni en los dispositivos informáticos. De hecho, QoSWorks optimiza el rendimiento de los routers existentes descargándolos de los procesos QoS.

6.3.2. Características de QoSWorks.

QoSWorks es el primer dispositivo de red QoS que integra todos los mecanismos QoS necesarios para manejar el amplio rano de tráfico con la mayor eficacia a cualquier velocidad incluyendo:

- Administrador de Tráfico Sitara Achúrate (combina y coordina múltiples mecanismos de gestión de tráfico QoS).
- Política inteligente de Web caching.
- Clasificación Wire speed.
- Administración intuitiva y flexible de políticas.
- Monitorización y obtención de informes en tiempo real.

6.3.3. Política inteligente de Web caching.

Además de integrar y coordinar múltiples mecanismos de administración de red con Achúrate, QoSWorks incorpora su propia caché, crítico para controlar y administrar tráfico HTTP Web que demandan gran ancho de banda que podrían comprometer aplicaciones críticas o sensibles a los tiempos de recuperación de datos. La caché QoSWorks almacena las páginas Web que se acceden más frecuentemente en una caché local, evitando así el tener usuarios navegando por la WAN para obtener las mismas páginas una y otra vez. El uso de caché no solo reduce el tráfico sobre la WAN, sino que también mejora los tiempos de respuesta para los usuarios finales.

A diferencia de una caché independiente y un administrador de tráfico, donde cada dispositivo tiene su propio clasificador y un administrador de tráfico, donde cada dispositivo tiene su propio clasificador y requiere que cada paquete sea procesado dos veces, la caché Web integrada de Sitara no requiere la reconfiguración de routers, navegadores o la instalación de un switch para redirigir peticiones a la caché.

La caché integrada de QoSWorks utiliza “Política inteligente”. Esto permite al administrador:

- Habilitar o deshabilitar el uso de la caché en base a una política determinada.
- Crear políticas que controlen la renovación de peticiones o prebúsquedas de tal modo que estas funciones no puedan poner en peligro el rendimiento de aplicaciones críticas.

6.3.4. Administrador de tráfico Sitara AccuRate.

A continuación se muestran los mecanismos de control de tráfico que están integrados y automáticamente coordinados con el Administrador de tráfico Sitara AccuRate.

Mecanismos QoS	**Que hace**	**Tipos de tráfico**
Encolamiento basado en clases.	Proporciona una fina modularidad en la repartición de ancho de banda y control de prioridades de tráfico.	Trabaja a través de todos los protocolos TCP o no TCP. Incluyendo UDP, Voz sobre IP, IPX.
Ratio de configuración TCP	Mejora la eficiencia de la conexión WAN reduciendo las retransmisiones; proporciona controles de flujo end-to-end; minimiza el retraso de encolamiento.	TCP
Asignación de ancho de banda por conexión.	Garantiza una política en la cual todas las sesiones tengan el mismo ancho de banda. Importante para redes con un gran número de sesiones de	TCP

	usuarios de aplicaciones.	
Optimización del tamaño de los paquetes.	Reducción del tamaño de los paquetes en la fuente de origen a un tamaño específico desde un máximo de 1, 500 bytes y hasta un mínimo de 64 bytes. Crítico cuando se mezclan videoconferencia o voz sobre IP con tráfico caracterizado por grandes paquetes.	TCP
Control de la utilización del ancho de banda.	Permite a las distintas categorías de tráfico tomar prestado ancho de banda no utilizado proveniente de otras clases específicas, de este modo se maximiza la utilización del ancho de banda mientras se garantiza que las aplicaciones sólo utilizan los recursos asignados.	Funciona con todas las clases de tráfico.

Tabla 7. Mecanismos de control de tráfico.

6.3.5. La solución QoSWorks.

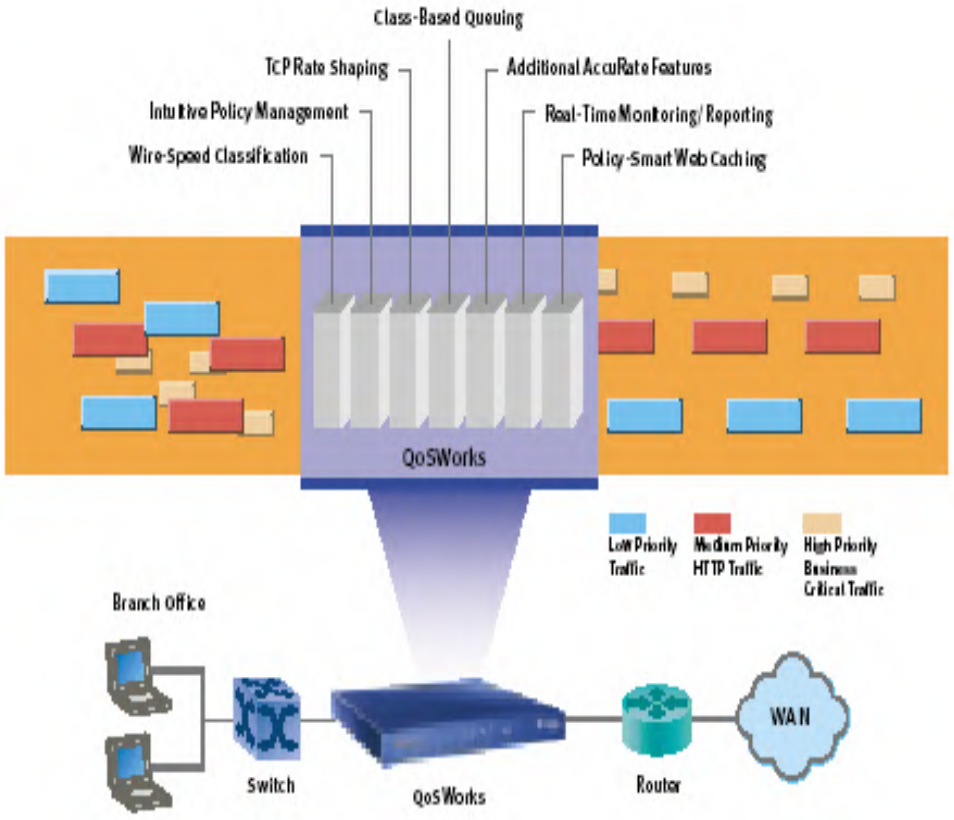


Fig. 46. Solución QoSWorks.

Concepto	Concepto traducido
Wire Speed Classification	Clasificación Wire Speed
Intuitive Policy Management	Administración de Políticas Intuitivas
TCP Rate Shaping	Ratio de Configuración TCP
Class-Based Queuing	Encolamiento Basado en Clases
Additional AccuRate Features	Características Adicionales de

	AccuRate
Real-Time Monitoring/ Reporting	Monitorización/ Informes en Tiempo Real
Policy-Smart Web Caching	Política Inteligente de Web Caching

Tabla 8. Conceptos traducidos.

QoSWorks es el primer dispositivo de red altamente escalable que integra todos los mecanismos QoS necesarios para manejar el amplio rango de tráfico con la mayor eficiencia a cualquier velocidad.

6.3.6. Clasificación Wire-Speed.

Cuando QoSWorks es instalado sobre la red, inmediatamente comienza a monitorizar los flujos de tráfico activo y desarrolla rápidamente una clasificación de tráfico. Este proceso de auto-descubrimiento funciona "escuchando" las conversaciones existentes (flujos de tráfico) sobre la red e identificando los diferentes tipos de tráfico, como el tráfico Web (HTTP y FTP), e-mail. Las aplicaciones y usuarios están clasificados por varios parámetros incluyendo:

- Direcciones IP fuente y de destino.
- Protocolo de red.
- Puerto de red.
- Subred.

6.3.7. Política de Administración flexible e Intuitiva.

QoSWorks simplifica dramáticamente la configuración de políticas con su interfaz intuitiva y un conjunto de filtros predefinidos que permiten a los administradores de red establecer políticas sofisticadas, sin embargo, efectivas en menos de 15 minutos. QoSWorks también proporciona una alta modularidad en la administración de políticas de afinamiento que se correspondan con las necesidades del negocio. Utiliza un sistema jerárquico basado en grupos que permite a los administradores de red dividir un enlace físico en un número anidado de enlaces virtuales lógicos que acotan el diseño lógico de la red. Para cada aplicación y/o usuario/grupo de usuarios los siguientes parámetros están especificados en el enlace virtual:

- Ancho de banda mínimo garantizado (Kbps).
- Ancho de banda máximo (kbps).
- Prioridad (5 configuraciones).
- Ancho de banda de la sesión (kbps, utilizado para el control de admisión).
- Control de Admisión (disminución, caída, negación).
- Caché (habilitada/deshabilitada).

Cualquier ancho de banda asignado y no utilizado puede ser compartido dentro del grupo basándose en las prioridades.

6.3.8. Monitorización y obtención de informes en tiempo real.

Uno de los desafíos más difíciles para los administradores de red al establecer políticas es obtener información precisa sobre quién está utilizando la red, con qué frecuencia y para qué propósito. Utilizando la clasificación Wire-Speed, QoSWorks proporciona una ventana en tiempo real sobre el tráfico de la red. Gráficos e informes de sencillo manejo facilitan visualizar cuanto ancho de banda está consumiendo cada usuario o aplicación, y permiten comprobar el grado de eficacia de los servicios de red sobre peticiones de dichos usuarios o aplicaciones.

La eficacia de las políticas en vigor puede ser monitorizada en tiempo real en la ventana de estado de QoSWorks. Por ejemplo, si una aplicación parece requerir más ancho de banda del previsto originalmente, el administrador puede ajustar la política en segundos y evaluar los resultados.

6.4. Equipo seleccionado.

El equipo que se selecciono para ser utilizado como solución a este problema es el PacketShaper, ya que cumple con las características necesarias para controlar y mejorar el ancho de banda de la red de la Dirección Local Guerrero, además se podrá contar con una red eficiente, el ancho de banda que se utilizará se usará de manera correcta, ya que existirán algunas limitaciones, pero todo esto será en beneficio de todos, el ancho de banda será utilizado como se debe.

CAPÍTULO VII. CONCLUSIONES Y RECOMENDACIONES

7.1. CONCLUSIONES.

El objetivo propuesto se ha cumplido satisfactoriamente, ya que por medio del software de monitoreo se logró hacer un análisis de estudio de la red de la Dirección Local Guerrero de la Comisión Nacional del Agua.

El análisis de la red permitió conocer:

- La utilidad que el personal da a Internet.
- La utilidad de intranet para el personal.
- Conocer la frecuencia de accesos a la red.
- Los tiempos en los que se produce tráfico de red.

Todos estos acontecimientos son de gran importancia para el administrador de la red, puesto que a pesar de que la red tiene diez años funcionando, nunca se había realizado un análisis de la red. Al cuestionar al administrador el porqué no se había realizado un análisis de la red con anterioridad; comentó que la razón es que un monitoreo necesita dedicación, el cual, el administrador carece por las actividades que realiza dentro de la dependencia.

Con este estudio, el administrador tendrá una perspectiva más amplia acerca del estado de la red, ya que los sistemas de monitoreo existentes, dan reportes de uso diario y en cualquier momento, por lo que el administrador podrá definir los anchos de banda, para repartirlo de manera adecuada según la utilidad del mismo.

También es importante que al analizar el administrador pueda detectar el incremento de uso de ancho de banda en labores propias de la empresa, para que, en un futuro si es necesario, se realice alguna modificación o actualización de la red; y se tome la mejor decisión según las necesidades de la red.

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

- Monitorear una red es una actividad que no puede considerarse secundaria; porque permite saber con anticipación sobre posibles caídas del sistema, fluctuación en la velocidad de transmisión de datos y un sin fin de elementos que resultan oro molido para el administrador de la red.

7.2. RECOMENDACIONES.

La red de la Dirección Local Guerrero cuenta con medidas de seguridad para controlar la información que circula hacia dentro y fuera de la red. Para ello, se utilizan firewalls, que protegen una red de otra; controlando todas las comunicaciones que pasan entre ellas. Y en función de la información que contenga la comunicación, permite o deniega su paso.

El análisis realizado por medio del software de monitoreo, mostró que el firewall de la dependencia no está realizando su trabajo eficientemente; la razón de esto, es que no cumple con las políticas de seguridad especificadas en el software; pues se están accesando a contenidos que el software debería de denegar, por ejemplo: páginas de pornografía, juegos, música, entre otros.

Por tal motivo, el administrador de la red debería de optar por realizar monitoreos de la red continuamente, ya que, los usuarios de la red han encontrado la manera de evadir dicho firewall.

Las diferentes opciones que se presentan en el manejo de la protección de la red, hace necesario implementar un sistema de monitoreo y protección eficiente, para evitar el mal uso de estas, al acceder a páginas que no están contempladas en las labores especificas de cada área; por lo tanto, se debe de supervisar y corregir la instalación de software de protección, como los antivirus y firewall,

con una configuración general y otras particulares, dependiendo del acceso que debe tener cada usuario a la red.

Además se debe de concientizar el personal a dar buen uso a la red; empezando con el cierre de todas aquellas aplicaciones que no se tengan en uso, ya que el simple hecho de que permanezcan abiertas; por ejemplo, una página de Internet, sin prestarle atención genera un consumo del ancho de banda disponible para la dependencia.

ANEXOS.

GLOSARIO.

Bomba lógica: programa informático que se instala en un ordenador y permanece oculto hasta cumplirse una o más condiciones preprogramadas para entonces ejecutar una acción.

Bridge: (puente), es un dispositivo de interconexión de redes que opera en la capa 2 del modelo OSI. Este interconecta dos segmentos de red (o divide una red en segmentos) haciendo el pasaje de datos de una red para otra.

Broadcast: sistema de entrega que proporciona la copia de un paquete dado a todos los anfitriones conectados para la difusión del paquete.

Caché: es una clase de memoria RAM estática; se presenta de forma temporal y automática para el usuario, que proporciona acceso rápido a los datos de uso más frecuente.

Chat: es un sistema mediante el cual dos o más personas pueden comunicarse a través de Internet en forma simultánea, es decir en tiempo real, por medio de texto, audio y hasta video, sin importar si se encuentra en diferentes ciudades o países.

CONAGUA: Comisión Nacional del Agua.

Criptografía: es el arte o ciencia de cifrar y descifrar información utilizando técnicas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.

CSMA/CD: (Carrier Sense Multiple Access with Collision Detection), Aceeso Múltiple con Escucha de Portadora y Detección de Colisiones. Es una técnica usada en redes Ethernet para mejorar sus prestaciones.

C.N.A.: Comisión Nacional del Agua.

Driver: es un programa informático que permite al sistema operativo interactuar con un periférico haciendo una abstracción del hardware y proporcionando una interfaz, posiblemente estandarizada para usarlo.

Freeware: es un software de computadora que se distribuye sin costo, y por tiempo ilimitado.

FTP: File Transfer Protocol. Protocolo de transferencia de Archivos.

Gateway: puerta de enlace, pasarela. Nodo en una red informática que sirve de punto de acceso a otra red.

Gusano: es un virus informático que tiene la propiedad de duplicarse a si mismo.

Host: (anfitrión) es una máquina conectada a una red de ordenadores y que tiene un nombre de equipo. Es un nombre único que se le da a un dispositivo conectado a una red.

Html: (HyperText Markup Languaje), se traduce como Lenguaje de Marcas Hipertextuales. Es un lenguaje de marcación diseñado para estructurar textos y presentarlos en forma de hipertexto, que es el formato estándar de las páginas Web.

Hub: o concentrador es un equipo de redes que permite conectar entre sí otros equipos y retransmite los paquetes que recibe desde cualquiera de ellos a todos los demás.

IEEE: Institute of Electrical and Electronic Engineers. Instituto de Ingenieros Electricistas y Electrónicos. Está involucrada en el establecimiento de estándares de informática y comunicaciones.

IPX: Internet Packet Exchange. Intercambio de paquetes interred. Familia de protocolos definida por Novell Corporation.

ISO: (Internacional Standard Organization). Organización Internacional de Estándares. La organización de normalización mejor conocida por haber propuesto el modelo de referencia de 7 capas de la historia temprana de la conectividad de datos.

LAN: (Local Área Network) Red de Área Local. Red que usa tecnología diseñada para abarcar un área geográfica pequeña.

Mainframe: es una computadora grande, potente y costosa usada principalmente por una gran compañía para el procesamiento de una gran cantidad de datos.

MAN: (Metropolitan Area Network), es una red que da cobertura en un área geográfica extensa. Representa una evolución de una LAN a un ámbito más amplio, cubriendo áreas mayores que en algunos casos no se limitan a un entorno metropolitano sino que pueden llegar a una cobertura regional e incluso nacional mediante la interconexión de diferentes redes de área metropolitana.

Mbps: Mega bits por segundo. Transferencia de millones de bits por segundo.

Multiplexor: dispositivo que puede recibir varias entradas y transmitirlas por un medio de transmisión compartido.

OSI: Open System Interconection. Interconexión de Sistemas Abiertos. Se trata de los protocolos, específicamente estándares de ISO, para la interconexión de sistemas de computadoras cooperativos.

Periféricos: se denominan periféricos tanto a las unidades o dispositivos a través de los cuales la computadora se comunica con el mundo exterior, como a los sistemas que almacenan o archivan la información, sirviendo de memoria auxiliar de la memoria principal.

Protocolo: conjunto de reglas que establecen cómo debe llevarse a cabo la comunicación a todos los niveles.

QoS: (Quality of Service) Calidad de Servicio, son las tecnologías que garantizan la transmisión de cierta cantidad de datos en un tiempo dado.

Reflectometro: es un instrumento electrónico usado para caracterizar y localizar los defectos en cables metálicos.
Router: se emplean para conectar LAN´s separadas permitiendo crear una "Inter.-red" de LAN´s. Opera en la capa de red de una LAN e inteligentemente acepta bits de datos de un lado y los dirige a la red correcta.

Shareware: es un software de computadora que se distribuye sin costo, pero generalmente por un tiempo especificado.

Switch: (conmutador), es un dispositivo de interconexión de redes que opera en la capa 2 del modelo OSI. Un conmutador interconecta dos o más segmentos de red, funcionando de manera similar a los puentes, pasando datos de un segmento a otro.

Token Ring: se refiere a un tipo de tecnología de red que controla al acceso de medios pasando un paquete distintivo llamado token (ficha= de máquina en máquina. Una máquina puede transmitir un paquete sólo cuando tiene la ficha (token)).

Troyano: son programas que ejecutan acciones destructivas, bajo ciertas condiciones, borrando la información de los discos duros, colgando sistemas, etc. Estos requieren que su víctima abra o ejecute un archivo anexado a un mensaje de correo electrónico para que de este modo el virus instale una copia de sí mismo y a partir de ello, empiece su proceso de infección.

UDP: (User Datagram Protocol), es un protocolo del nivel de transporte del modelo OSI, basado en el intercambio de datagramas.

URL: Uniform Resource Locutor, es decir, localizador uniforme de recurso. Es una secuencia de caracteres, de acuerdo a un formato estándar, que se usa para nombrar recursos, como documentos e imágenes en Internet, para su localización.

WAN: (Wide Área Network) Red de Área Amplia. Cualquier tecnología de red que abarca distancias geográficas extensas. También llamadas Redes de gran alcance.

WWW: (World Wide Web), es un sistema de documentos de hipertexto y/o hipermedios enlazados y accesibles a través de Internet.

X.25: es un estándar popular para las redes de conmutación de conjunto de bits. Fue aprobado en 1976.

BIBLIOGRAFIA.

- Descubre Redes LAN y WAN. Frank Derflen. Editorial Prentice Hall. 1999.
- Redes de computadoras. Andrew S. Tanenbaum. Editorial Pearson Education. 1997.
- Redes globales de información con Internet y TCP/IP. Douglas E. Comer. Editorial Pearson Education. 1996.
- www.desi.iteso.mx/redes/redes1.htm
- www.ethereal.com
- www.integracion-de-sistemas.com/analisis-y-monitoreo-de-redes.html
- www.colasoft.com
- www.packeteer.com/support
- www.sitaranetworks.com
- www.geocities.com/SiliconValley/8195/redes.html

- http://docente.ucol.mx/970310/public_html
- www.opalsoft.net/qos/Spanish-QOS.htm
- www.epson.cl/productos/suministros/conectividad.htm
- www.sei.cmu.edu/activities/str/descriptions/dce_body.html
- www.cna.gob.mx/conagua/Default.aspx