PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE AMBATO

SERÉIS MIS TESTIGOS

DEPARTAMENTO DE INVESTIGACIÓN, POSTGRADOS Y AUTOEVALUACIÓN

TEMA:

"ANÁLISIS DE LA RED CORPORATIVA DE UNA EMPRESA AGROINDUSTRIAL, CON MIRAS A DEFINIR LA REESTRUCTURACIÓN DE LA MISMA PARA OBTENER UN MÁXIMO DE DISPONIBILIDAD."

Tesis de Grado previo a la Obtención del Título de Magister en Gerencia Informática con Mención en Desarrollo de Software y Redes

AUTOR:

XAVIER E. MIÑO RODRIGUEZ

DIRECTOR:

ING. MSC. JANIO JADAN

Ambato – Ecuador

Febrero 2010

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

Departamento de Investigación, Postgrados y Autoevaluación

HOJA DE APROBACIÓN

Tema:

"ANÁLISIS DE LA RED CORPORATIVA DE UNA EMPRESA AGROINDUSTRIAL, CON MIRAS A DEFINIR LA REESTRUCTURACIÓN DE LA MISMA PARA OBTENER UN MÁXIMO DE DISPONIBILIDAD."

Autor:

XAVIER E. MIÑO RODRIGUEZ

Janio Jadán, Ing. Msc.
DIRECTOR DE TESIS f. _____

Galo López, Ing. Msc.
CALIFICADOR f. _____

Marco Polo Silva, Ing. Msc.
CALIFICADOR f. _____

Telmo Viteri, Ing.
DIRECTOR UNIDAD ACADÉMICA f. _____

Pablo Poveda Mora, Ab.
SECRETARIO GENERAL PUCESA f. _____

SECRETARÍA GENERAL
PROCURADURÍA

DECLARACIÓN DE AUTENTICIDAD

Y RESPONSABILIDAD

Yo, Xavier Eugenio Miño Rodríguez portador de la cédula de ciudadanía No. 180264177-7 declaro que los resultados obtenidos en la investigación que presento como informe final, previo la obtención del título de MAGISTER EN GERENCIA INFORMÁTICA CON MENCIÓN EN DESARROLLO DE SOFTWARE Y REDES son absolutamente originales, auténticos y personales.

En tal virtud, declaro que el contenido, las conclusiones y los efectos legales y académicos que se desprenden del trabajo propuesto de investigación y luego de la redacción de este documento son y serán de mi sola y exclusiva responsabilidad legal y académica.

Xavier Eugenio Miño Rodríguez

CI. 180264177-7

Resumen

El presente trabajo, cubre el análisis de la red de datos de una empresa agroindustrial, la misma que requiere de acceso a Internet desde sus diferentes oficinas ubicadas en Quito y Santo Domingo de lo Tsachilas. En la actualidad la red de datos soporta gran parte de la gestión operativa de la empresa, tanto para procesos internos como externos, entregando servicios de Internet como son: Correo Electrónico e Internet, mediante los cuales se procesan los pedidos de los clientes. El presente trabajo permitirá que la empresa cuente con un análisis, el cual servirá de base para la reestructuración de la red de datos y contará con la mayor disponibilidad y eficiencia de los recursos disponibles. Se ha desarrollado un análisis detallado de la estructura actual de la empresa, y se ha determinado si ésta se ajusta a los niveles de disponibilidad y eficiencia requeridos para las operaciones normales de la empresa. De la misma forma se ha determinado el nivel de disponibilidad de la red de datos de la empresa y si la estructura de datos actual brinda las garantías necesarias para el transporte de la información de la Empresa.

Abstract

The following work covers the network information analysis of a farm-industrial company, which requires internet access from its offices located in Quito and Santo Domingo de los Tsachilas. Nowadays this information network supports itself a huge part of the operative management of the company, for internal processes as well as for external services delivering e-mail and internet which are used to make orders for clients. This work allows the company to have an analysis that will support a base to restructure the information network and will have more availability and efficiency of existing resources. A detailed analysis of the present structure of the company has been made and it has been determined if this adjusts to the availability and efficiency levels required by its regular operations. In the same way, the network information availability level of the company has been determined and if the present information structure gives the needed guarantee for the delivery of the information company.

TABLA DE CONTENIDOS

TABLA DE GRÁFICOS

Página

CAPITULO I

1. Proyecto de Investigación

1.1. Antecedentes

Las Organizaciones industriales y comerciales en la actualidad, dependen de Sistemas de Información y Comunicaciones, los cuales están integrados por redes y dispositivos de comunicaciones.

Tomando como referencia COBIT (*Control OBjectives for Information and related Technology - Objetivos de Control para tecnología de la información y relacionada*) y su definición de los criterios de información del negocio, que son: Efectividad, Eficiencia, Confidencialidad, Integridad, Disponibilidad, Cumplimiento y Confiabilidad, podemos indicar que las redes de computadores y los elementos que lo componen son indispensables para el cumplimiento de información especificado, como parte de la infraestructura.

La Empresa Objeto de nuestro análisis, cuenta con sus oficinas administrativas en la Ciudad de Quito, y su planta de producción en el área de influencia de Santo Domingo de los Sáchilas, cuenta con una red de datos que une los dos centros

geográficos, sobre la cual se integran todos los servicios de información como son aplicaciones, Internet, Voz y Correo Electrónico.

Nuestra empresa, maneja todas sus operaciones desde el contacto con el cliente hasta el despacho del producto terminado, utilizando herramientas de información que dependen de la red de la Disponibilidad de la Red de Datos.

La red de datos debe contar con una estructura que brinde alta disponibilidad para las aplicaciones y servicios que requiere la empresa.

Planteamiento del Problema

La empresa objeto de nuestro análisis ha implementado de manera progresiva aplicaciones que le permiten desarrollar sus actividades comerciales, todas estas aplicaciones para el normal funcionamiento de las operaciones deben estar todo el tiempo activas.

Debido al tipo de implementación establecido, no se ha dado una incorporación técnica de todos los servicios, sin contar con un adecuado análisis de las necesidades reales de la organización ni de la demanda de recursos establecida por cada uno de los servicios incorporados a la red de datos de la organización.

La principal problemática de la empresa es determinar si la estructura actual de la red de datos es eficiente y si le provee de la disponibilidad requerida para sus operaciones.

1.2. Problematización

El nivel de disponibilidad de la red de datos de la Empresa, no está de acuerdo a la demanda de la misma.

La Estructura de la red de datos actual no brinda las garantías necesarias para el transporte de la información de la Empresa.

La empresa requiere una propuesta de reestructuración adecuada a las necesidades de la empresa, en base a los recursos disponibles.

1.3. Delimitación

El presente proyecto se limitará única y exclusivamente a los elementos de comunicaciones que conforman la red de datos de la empresa.

El trabajo se enmarcará en el análisis de tráfico, especificaciones y configuraciones de los equipos de comunicaciones.

Definir la estructura actual de la red de datos y si es requerido, la definición de una nueva estructura y configuración de los equipos, para garantizar la máxima disponibilidad del servicio, tomando en cuenta protocolos de calidad de servicio.

1.4. Justificación

En la actualidad en la red de datos se soporta gran parte de la gestión operativa de la empresa, tanto para procesos internos como externos, los servidores que proveen los servicios de Internet como son Correo Electrónico e Internet, mediante los cuales se procesan los pedidos de los clientes así como los despachos del producto terminado, desde la coordinación de la logística hasta la entrega definitiva en manos del cliente.

Por lo antes expuesto, es imprescindible que la empresa cuente con el análisis propuesto en éste proyecto, el cual servirá de base para la reestructuración de la red de datos y contar con la mayor disponibilidad y eficiencia de los recursos con que se cuenta.

1.5. Objetivos

1.5.1. Objetivo General

Desarrollar un análisis detallado de la estructura actual de la empresa, y determinar si ésta se ajusta a los niveles de disponibilidad y eficiencia requeridos para las operaciones normales de la misma.

1.5.2. Objetivos Específicos

1. Determinar el nivel de disponibilidad de la red de datos de la Empresa.
2. Definir si la estructura de datos actual brinda las garantías necesarias para el transporte de la información de la Empresa.

3. Si la Red de Datos no cuenta con una estructura adecuada, hacer una propuesta de reestructuración adecuada a las necesidades de la empresa.

1.6. Hipótesis

Con un análisis de la cantidad y tipo de tráfico que transporta una red de datos, en cada uno de sus enlaces, se puede especificar la configuración óptima de los equipos para maximizar el uso de los recursos disponibles.

CAPITULO II

2. Conceptos Generales

Para iniciar nuestro análisis vamos a enmarcarnos en el escenario técnico que involucra una red de datos como la que nuestra empresa maneja, en este capítulo, daremos un vistazo a los conceptos generales que tenemos que tomar en cuenta, lo cuales servirán de base comparativa para definir los requerimientos que plantearemos en la red de datos.

Como punto de partida iniciaremos viendo el modelo OSI, el protocolo TCPIP, lo que representa la Administración de Redes desde el punto de vista de nuestro caso de estudio, el papel de la calidad de servicio y que debemos observar al realizar un análisis de tráfico en la red.

2.1. Administración de Redes

2.1.1. Historia

Las redes de comunicaciones se originan con el nacimiento de las telecomunicaciones, se inician cuando se creó la necesidad de interconectar dos o más puntos simultáneamente.

Desde sus orígenes las redes de computadoras han evolucionado considerablemente, desde la capacidad de las computadoras que se interconectan y los medios por medio de los cuales se realiza dicha interconexión como son: cables de cobre, fibra óptica o microondas.

Como habíamos indicado vamos a centrarnos en los tipos de redes que aplican en nuestro caso de estudio, estudiando específicamente TCP/IP ya que es un protocolo muy difundido en el manejo de redes locales y de área extensa, como por ejemplo en el Internet.

Una red es un conjunto de nodos, interconectados entre si y con la capacidad de comunicarse, compartiendo servicios, transmitiendo datos entre nodos servidores y nodos cliente, de acuerdo a la demanda de los mismos. Los nodos pueden ser: computadores, impresoras, servidores o cualquier equipo con la capacidad de enviar y/o recibir información. Un subconjunto de las redes de datos son los sitios, los cuales son grupos reducidos de nodos, una red puede estar integrada por varios sitios.

La capacidad de comunicación está dada por un protocolo de comunicaciones, que no es más que un lenguaje común que utilizan los nodos para enviar y recibir información, este lenguaje reúne las reglas y políticas que se toman en cuenta para llevar a cabo la comunicación.

2.1.2. Definición

Podemos definir en este punto que la Administración de Redes, como el conjunto de prácticas destinadas a mantener operativa la misma, considerando su seguridad y eficiencia, manteniendo un monitoreo y planificación adecuados.

Los objetivos fundamentales de la Administración de Redes son:

- Mantener la Continuidad de las Operaciones.
- Implementar métodos adecuados de monitoreo.
- Implementar políticas adecuadas de Resolución de Problemas.
- Mantener un adecuado suministro de recursos.
- Controlar el uso eficiente de los recursos de la red.
- Implementar políticas adecuadas de seguridad.
- Mantener el software y el hardware de la red actualizado.

Dependiendo de la topología, la infraestructura y la información que circula por la red, la administración se hace más necesaria y compleja entre los factores que inciden directamente en el tipo de administración a implementar tenemos:

- **Tipo de información que circula en la red:** En la actualidad por las redes de datos circulan diferentes tipos de información contenidas en Datos, Videos, Música, etc.
- **Tipo de Redes:** En las organizaciones se ha hecho común la interconexión de redes LAN y WAN, utilizando diferentes tecnologías, como pueden ser Cobre, Satélite, Microondas, etc.

- **Uso de Diversos Medios de Comunicación:** La diversidad de tecnologías implica el uso de una diversidad de medios de comunicación como son: Cobre, Fibra Óptica, Microondas, etc.
- **Protocolos de Comunicación:** Entre los protocolos de Comunicación tenemos: TCP/IP, NetBeui, IPS/SPX, etc.
- **Sistemas Operativos:** En el mercado se pueden integras en una red varios tipos de Sistemas Operativos como son: LINUX, UNIX, Windows, etc.
- **Arquitectura de Redes:** Se puede integrar varias arquitecturas, entre las que tenemos: Ethernet, Token Ring, FDDI, etc.

Como parte de las acciones que se llevan a cabo para la Administración de Redes podemos mencionar:

a) Como resultado del monitoreo debemos recolectar la información del estado de la red y componentes que la integran, entre los que tenemos: eventos, atributos y acciones a realizarse.
b) Reportes adecuados para la toma de decisiones y acciones a ejecutar.
c) Almacenamiento de la información relacionada con el monitoreo de la red.
d) Plan de contingencias que indique las acciones a seguir cuando se produzcan eventos que afecten la continuidad de operaciones.

Los elementos que componen una red como lo habíamos definido son los nodos, los mismos que son los elementos objeto de las políticas y procedimientos destinados a la administración de la red.

Los nodos, en un esquema administrativo de red son monitoreados continuamente para determinar su estado, para realizar dicho monitoreo, se utilizan herramientas de software que consultan periódicamente a los nodos sobre su estado, a estos programas se los denomina agentes, los cuales reportan a un consola de control información relacionada con: Problemas con el nodo, datos de diagnostico y estado, identificación y características del nodo.

Toda la información recolectada por el agente, es recopilada por parte del Administrador de la Red, que normalmente es un programa o conjunto de programas que permiten una administración centralizada de la información.

2.1.3. Funciones del Administrador de la Red

Para la Administración de los Servicios proporcionados por una red de datos, tomaremos como referencia lo determinado por OSI que enmarca en cinco factores que son:

a. Configuración.
b. Fallas.
c. Contabilidad.
d. Comportamiento.
e. Seguridad.

- **Configuración:** La configuración enmarca lo relacionado al monitoreo, operatividad y estado de la red. Se debe tener adicionalmente in inventario total de los elementos que componen la red de datos, su configuración y un registro

detallado de los cambios realizados. Esto implica el manejo documental de la planificación de configuraciones, programación de eventos e instalación de los nuevos nodos que formarán parte de la red.

- **Fallas:** Contempla la detección, aislamiento y corrección de las fallas que se presenten en la red de datos. Los errores que se presentan en la red y las condiciones en las que se presentan, requieren que se realicen los siguientes pasos:

  1) ***La detección de la falla.*** El diagnóstico del problema que incluye identificar las causas por las que se produjo el fallo.
  2) ***Corregir el problema y recuperar las operaciones***, que implica ejecutar las acciones correctivas necesarias para que el problema sea resuelto y poner nuevamente operativa la red de datos.
  3) ***Seguimiento,*** que represente definir el procedimiento adecuado para asegurarse que el problema no se presente nuevamente.

  Para la gestión de fallas se debe implementar políticas y procedimientos relacionados con la Gestión de Incidentes, se puede referenciar para esto a las recomendaciones y mejores prácticas dadas en ITIL en lo relacionado a este tema.

  Itil tiene como objetivos principales para la Gestión de Incidentes los siguientes:

a) Detectar las alteraciones que se den en los servicios de TI, en este caso en los servicios dados por la red de datos.
b) Registrar y clasificar estas alteraciones, mediante un debido monitoreo se pueden detectar los problemas que presente la red de datos.
c) Asignar al personal encargado de restaurar el servicio de comunicaciones o de transporte de datos, según se define en Acuerdo de Nivel de Servicio correspondiente.

Las actividades que se especifiquen deben tener un contacto directo con los usuarios, razón por la cual el Centro de Servicios, debe estar involucrado en todo momento.

El procedo de gestión de incidentes puede ser definido como se muestra en la siguiente Figura 2-1: Gestión de Incidentes.

Itil define a un incidente como: *"Cualquier evento que no forma parte de la operación estándar de un servicio y que causa, o puede causar, la interrupción o una reducción de calidad del mismo"*. Entendemos en este modo que cualquier solicitud al centro de servicios será un incidente, de esta manera se atenderán todas las peticiones sin importar el origen.

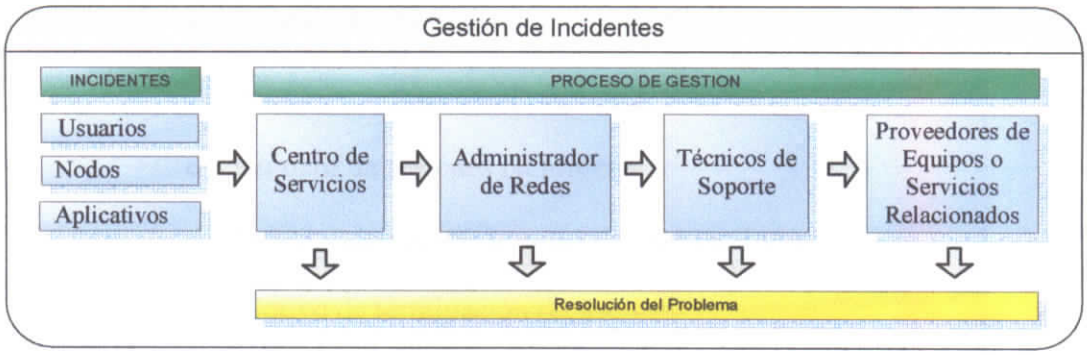


Figura 2.1. Gestión de Incidentes

Los beneficios que se desean alcanzar con una adecuada Gestión de Incidentes son entre otros:

a. Mejorar la Productividad de los Recursos,
b. Cumplir con los Acuerdos de Nivel de Servicio,
c. Control Adecuado de Procesos,
d. Monitoreo efectivo de los Servicios,
e. Optimización de los Recursos,
f. Mejores Niveles de Satisfacción,
g. Niveles Adecuados de Disponibilidad de los Servicios.

- **Contabilidad:** El control de la red determinado por el nivel de monitoreo que sea implementado debe incluir la recopilación de datos estadísticos de funcionamiento de la red para determinar la disponibilidad de la misma. Entre los datos recomendados que se deben capturar para llevar un control adecuado tenemos:

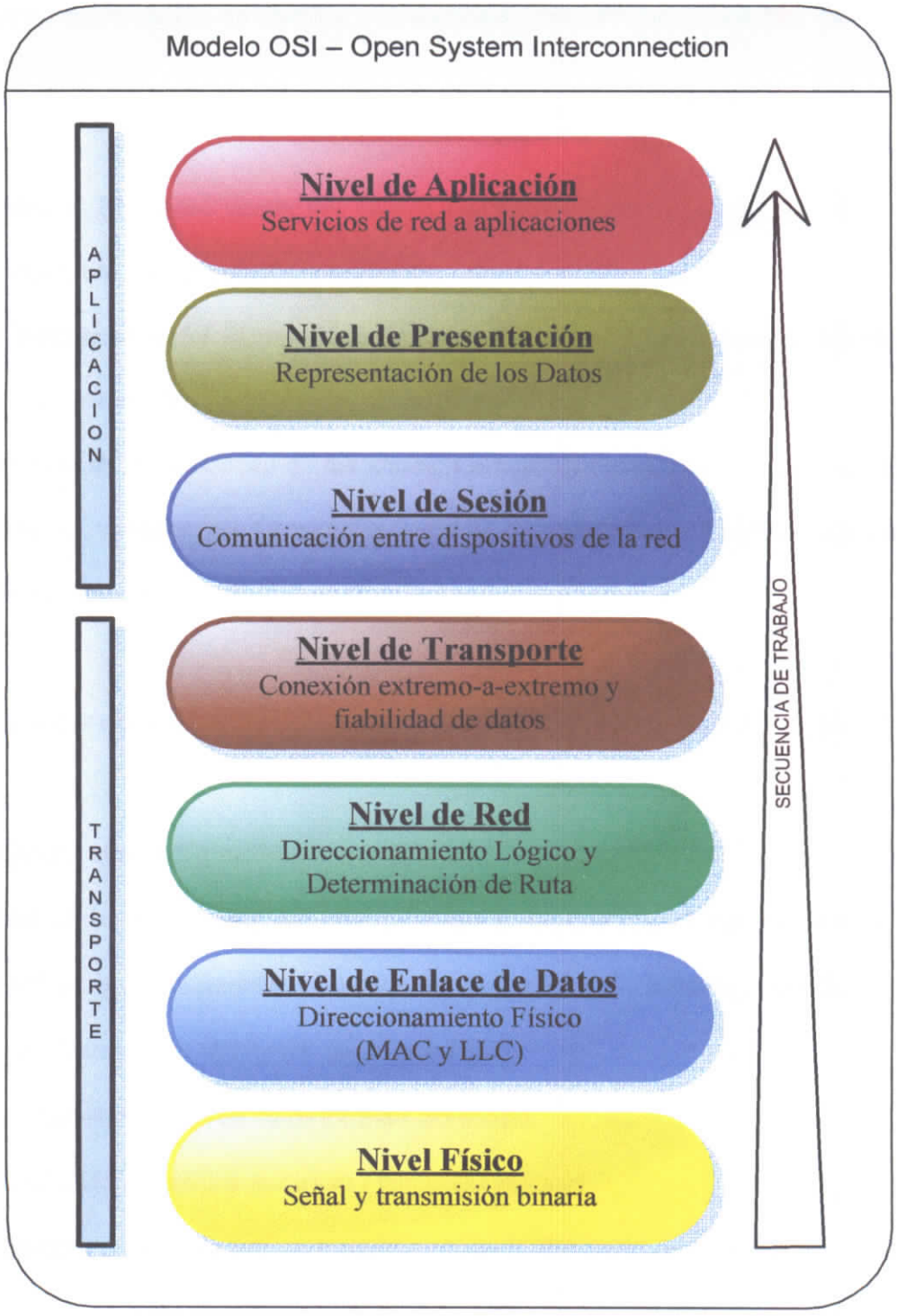


Figura 2.2. Modelo OSI – Open System Intercionnection

Se entiende por medio al aire, cobre, fibra, etc., que se utiliza para transmitir los datos.

Para nuestro análisis, definiremos los medios que han sido utilizados en el establecimiento de la red de datos y la forma de conexión de los equipos que utilizan los mismos.

En esta capa intervienen además del medio, equipos como los repetidores y concentradores.

"Correlación con el objeto del estudio": En nuestro análisis se ha realizado un estudio detallado de la parte física de interconexión de todos los elementos y equipos que conforman la red de datos de la empresa, lo cual afecta directamente con la disponibilidad del servicio.

2.2.2. Capa 2: Nivel de Enlace de Datos

Al medio físico, que definimos en la Capa 1, debemos darle la capacidad de proporcionarnos una transmisión de datos sin errores, es decir que los datos transiten de manera fiable.

En el Nivel de Enlace de Datos, creamos y reconocemos los límites de los bloques de datos o tramas, así como su deterioro, pérdida o duplicidad que sufren durante la transmisión por causa del medio. Se incluye además mecanismos de regulación de tráfico que permita evitar la saturación de un receptor más lento que el emisor.

En ésta capa se define el direccionamiento físico, la topología de red, el acceso a la red, la notificación de errores, el ordenamiento de las tramas y su distribución así como el control de flujo.

Entran en escena además, las NIC (Network Interface Card), que son las que se encargan de que tengamos conexión y los Switchs, estos elementos poseen una dirección MAC (Control de Acceso al Medio) y una LLC (Control de Enlace Lógico).

En conclusión, se encarga de transformar la línea de transmisión común en una sin errores para la capa de red, esto se lleva a cabo dividiendo la entrada de datos en tramas denominadas de asentamiento, incluyendo un patrón de bits entre las tramas. Aquí se solucionan los problemas de reenvío, y duplicidad de mensajes cuando las tramas se destruyen. Controlando adicionalmente el tráfico.

Un problema grave que se controla es la transmisión bidireccional de datos.

Las tramas están compuestas por:

- Número de caracteres (Un campo del encabezamiento guarda dicho número. Sin embargo, si éste número es cambiado en una transmisión, la trama es difícil de recuperar).
- Caracteres de inicio y fin.

Normalmente se parte de un flujo de bits en marcos. Las características de la transmisión se describen a continuación:

a. ***Marcos:*** En nivel de enlace detecta y corrige los errores si es posible. Partiendo normalmente de un flujo de bits, parla lo que se calcula una comprobación de datos (Checksum) para cada uno.
b. ***Servicios para el nivel de red:*** se tienen dos tipos de servicios, el uno sin acuses de recibido, en el cual un equipo manda marcos al equipo de destino, el cual define que es apropiado si la frecuencia de errores es muy baja o si el tráfico es de tiempo real como por ejemplo la voz. El otro en cambio es un servicio con acuses de recibido, en el que simplemente el receptor envía un acuse de recibido al remitente por cada marco recibido.
c. ***Control de Flujo:***_Ésta característica es utilizada con protocolos que prohíben que el remitente pueda mandar marcos sin el permiso implícito o explicito del receptor.
d. ***Detección y corrección de errores:*** Para poder detectar errores, se incorporan un campo de CheckSum y un campo de control, que permiten la detección de posibles errores y el envío de mensajes de recepción correcta respectivamente.

2.2.3. Capa 3: Nivel de Red

Una vez que hemos garantizado la transmisión, el siguiente paso es asegurarnos que los datos lleguen de origen a destino, sin importar si los dos están o no conectados directamente. Esta es la función del Nivel de Red, para lo cual existen dispositivos

denominados encaminadores que son comúnmente llamados Routers por su nombre en inglés o enrutadores.

Debido a que esta capa es la encargada de garantizar que los datos lleguen a destino, aquí se implementa un control de la congestión de la red, los equipos son denominados nodos y la congestión se produce cuando un nodo se satura y afecta a toda la red. Aquí las unidades de datos son llamados paquetes.

En esta capa trabajan varios tipos de dispositivos como Routers y Firewalls, que principalmente trabajan con direcciones de máquinas ya que en este nivel se determina la ruta de los datos y su receptor final.

La función principal de este nivel es eliminar los cuellos de botella que se producen cuando existen demasiados paquetes enviados por lo que es necesario que cada paquete sea encaminado hacia su destinatario, para lo cual existe un registro de los paquetes que han sido enviados.

Aquí es en donde se solucionan todo tipo de problemas relacionados con la conexión a redes heterogenias, relacionados con tipos diferentes de protocolos o direccionamiento desigual.

2.2.4. Capa 4: Nivel de Transporte

Los datos estructurados por los niveles 5, 6 y 7, son divididos en partes, generalmente más pequeños para ser entregados a la capa 3, esta es la función

principal del Nivel de Transporte. De acuerdo a la especificación del modelo OSI, este nivel adicionalmente, asegura que los datos lleguen correctamente del emisor al receptor. Este nivel sirve de frontera entre los niveles superiores aislando cualquier tipo de implementación o desarrollo tecnológico realizado en los niveles inferiores, dándole una posición estratégica en la comunicación. Provee adicionalmente servicios de conexión para la capa de sesión los que serán utilizados por los usuarios de la red cuando envíen o reciban paquetes, asociando estos servicios al tipo de comunicación empleado, el cual difiere de acuerdo al requerimiento realizado por la capa de transporte.

Por ejemplo se puede establecer una comunicación manejada en relación a que los paquetes sean entregados en el orden exacto en el que fueron enviados, para asegurar un comunicación punto a punto exenta de errores, o simplemente se decide por no tomar en cuenta el orden de envío, cualquiera de las dos modalidades debe establecer antes de iniciar la comunicación para que la sesión envíe paquetes, siendo éste el tipo de servicio brindado por la capa de transporte durante la sesión hasta que esta finalice. Por lo antes expuesto definimos que la capa de transporte no está encadenada a las capas inferiores (1,2 y 3), más bien determina el tipo de servicio cada vez que se establece una sesión de comunicación, gestionando el servicio a través de las cabeceras que agrega al paquete a ser transmitido.

Complementando la definición de la capa como la encargada de transportar los datos del Origen al Destino, independiente del tipo de red física que se esté utilizando.

La PDU de esta capa se denomina Segmento, los protocolos utilizados en esta capa son TCP y UDP, orientado y no orientado a la conexión respectivamente.

En esta capa por ejemplo se ubica el protocolo TCP (Transfer Control Protocol) utilizado con IP (Internet Protocol).

2.2.5. Capa 5: Nivel de Sesión

A nivel superior, esta capa es la encargada de la implementación de los mecanismos para controlar el dialogo entre las aplicaciones de los sistemas finales del usuario, en la mayoría de los casos, los servicios que proporciona esta capa no son necesarios por lo que son prescindibles, sin embargo en algunas aplicaciones su implementación no se puede evitar.

Los principales servicios que proporciona esta capa son:

a. ***Control de Sesión:*** Llamado también control de diálogo, puede ser full-duplex o half-duplex, dependiendo del tipo se control que se quiera entre el emisor y el receptor.
b. ***Concurrencia:*** Permite que una misma operación crítica no se efectúe al mismo tiempo. Además permite marcar el flujo de datos para definir grupos.
c. ***Recuperación:*** Permite implementar un procedimiento de puntos de control para definir grupos de datos, de manera tal que si existe un fallo entre los puntos de control, se pueden retransmitir todos los datos entre los puntos de control en el cual se presento el fallo, y no todos los datos desde el principio.

Si bien es cierto, los servicios definidos pueden ser implementados e incorporados en las aplicaciones de capa 7, las herramientas de control de diálogo son aplicables ampliamente, se ha definido una capa específica como es la capa de sesión.

Esta capa al permitir que los usuario de diferentes máquinas establezcan sesiones entre ellos, permitiendo el transporte ordinario de datos, como lo hace la capa de transporte, proporcionando mejores servicios utilizados por algunas aplicaciones como por ejemplo sistemas remotos o transferencia de archivos, garantizando que una vez iniciada una sesión, se puedan realizar las operaciones programadas de principio a fin, pudiendo reiniciarlas en caso de interrupción.

Para concluir, podernos indicar que la capa de Sesión se encarga de mantener el enlace de datos entre los computadores que estén transmitiendo datos de cualquier tipo.

Normalmente los Firewalls utilizan esta capa para bloquear acceso a puertos por parte de un computador.

2.2.6. Capa 6: Nivel de Presentación

Hasta la capa cinco, el principal objetivo de las capas era garantizar la conexión y la entrega del paquete desde el emisor al receptor, la capa de presentación, se especializa en el contenido de la comunicación, gestionando lo referente a la semántica y sintaxis de los datos transmitidos, ya que entre el emisor y el receptor pueden diferir en la forma de manejarlas.

El manejo en cada uno de los equipos puede diferenciarse en la forma en que se representa la información en el equipo, esto se refiere al estándar de codificación de caracteres que se utilice como por ejemplo: ASCII, Unicode, EBCDIC. En el mismo sentido pueden diferenciarse en el formato en que se almacenan los datos de mas de un byte en un ordenador como por ejemplo el Big-Endian adoptado por Motorola, Little-Endian adoptado por INTEL. De igual manera se maneja todo tipo de información como puede ser sonido o imágenes, por lo que hay que garantizar que los datos lleguen de manera reconocible.

Resumiendo podemos decir que la Capa de Presentación es la encargada del manejo de las estructuras de datos abstractos realizando conversiones entre las diferentes interpretaciones del emisor y receptor, para su interpretación, como función complementaria se encarga de cifrar y comprimir datos, fungiendo como un traductor.

Adicionalmente, se ocupa de garantizar la fiabilidad del servicio, describiendo la calidad y naturaleza del envío de datos, definiendo el cómo y cuando se utiliza la retransmisión para asegurar la llegada de los mismos, dividiendo el mensaje entregado por la capa de sesión en varias partes o trozos (datagramas), que son numerados correlativamente y los entrega a la capa de red para ser enviados. Si en la recepción se utiliza el protocolo IP, la capa de transporte reordena los paquetes recibidos. Se puede utilizar en el sentido inverso multiplexando la conexión de transporte entre varias conexiones de datos, permitiendo que diversas aplicaciones utilicen el mismo flujo de datos hacia la capa de red.

Esta capa también permite cifrar los datos y comprimirlos. En pocas palabras es un traductor.

Por todo ello, podemos resumir la definición de esta capa como aquella encargada de manejar la estructura de datos abstracta y realizar las conversiones de representación de los datos necesarios para la correcta interpretación de los mismos.

2.2.7. Capa 7: Nivel de Aplicación

Esta capa permite a las aplicaciones, sean o no de usuario, la capacidad de acceder a los servicios de las capas inferiores, las mismas que se utilizan para el intercambio de datos de varios tipos como pueden ser: correo electrónico, bases de datos, servidores de archivos, etc. Actualmente debido a la diversidad de aplicaciones existentes, se han desarrollado igual número de protocolos. Debido a que el usuario normalmente no trabaja con el nivel de aplicación, trabaja con aplicaciones que tienen acceso a este ocultando la complejidad de este trabajo. Por ejemplo el usuario no envía directamente código html/xml para conseguir una página web, esto lo hace la aplicación.

Entre los protocolos más utilizados, no necesariamente relacionados con la capa de Aplicación del modelo tenemos:

- HTTP (HyperText Transfer Protocol = Protocolo de Transferencia de Hipertexto)
- FTP (File Transfer Protocol = Protocolo de Transferencia de Archivos)
- SMTP (Simple Mail Transfer Protocol = Protocolo Simple de Correo)
- POP (Post Office Protocol = Protocolo de Oficina de Correo)

- IMAP: reparto de correo al usuario final.
- SSH (Secure Shell = Capa Segura) utilizado para conexiones remotas.
- Telnet Terminal Remoto

Entre los protocolos más utilizados en la capa de aplicación tenemos:

- SNMP (Simple Network Management Protocol)
- DNS (Domain Name Service).

En esta capa se especializa en definir como los programas de aplicación deben trabajar para realizar una conexión o transferencia de datos. En esta capa se implementas las operaciones con ficheros del sistema.

Como sirve de límite entre la aplicación del usuario y la capa de presentación interactúa entre las dos entregando y recibiendo los comandos que facilitan la comunicación.

2.2.8. Bloque de Datos

El modelo OSI, permite al final del ciclo definido de la comunicación integrar un bloque de datos que permiten garantizar que los datos lleguen del origen al destino de manera completa. El Bloque de Datos se esquematiza en la Figura 2.3: Formato del Bloque de Datos.

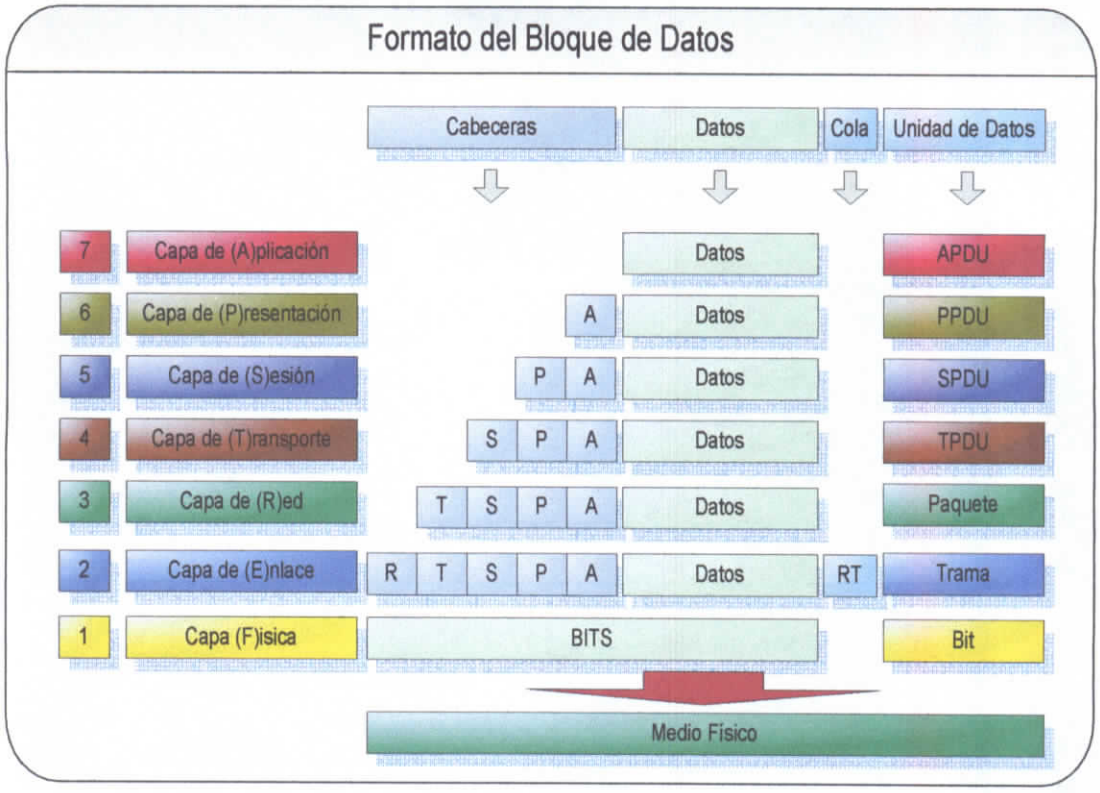


Figura 2.3. Formato del Bloque de Datos

2.2.9. Flujo de la Comunicación

La comunicación en el modelo OSI se desarrolla de arriba hacia abajo en el origen y de abajo hacia arriba en el destino, los datos se originan en la capa de aplicación, conforme baja por las diferentes capas se van incorporando las cabeceras de las diferentes capas, hasta llegar a la transmisión por el medio físico, cuando llega al destino, conforme va subiendo por las diferentes capas las cabeceras se van eliminando hasta entregar los datos en la Aplicación que está integrada con la Capa de Aplicación. En la Figura 2.3.: Flujo de la Comunicación, podemos observar la integración del flujo de la comunicación.

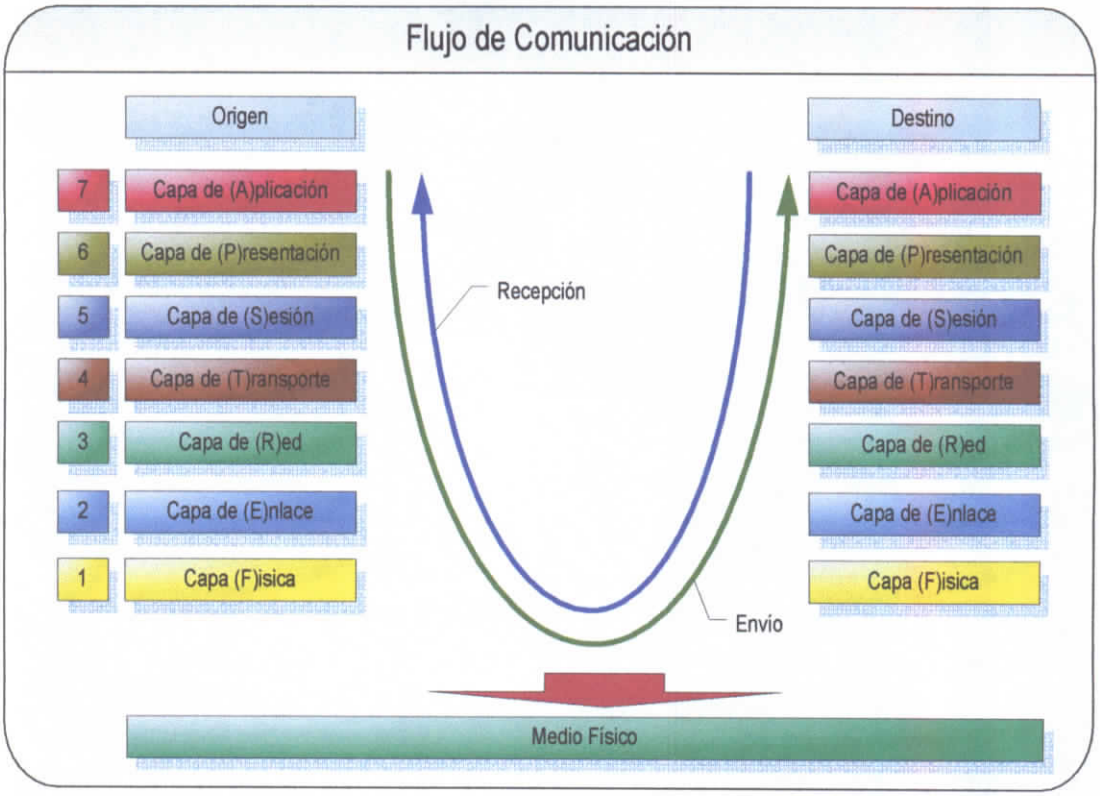


Figura 2.4. Flujo de la Comunicación

2.3. TCP/IP

Una vez que hemos definido y revisado el modelo OSI, estamos listos para ver su aplicación. TCP/IP es el protocolo de comunicaciones o mejor dicho conjunto de protocolos, el cual es usado ampliamente en la actualidad en redes de datos, principalmente por su amplia difusión en el Internet. La correspondencia entre el modelo OSI y TCP/IP, lo podemos apreciar en la Figura 2.4.: Correspondencia entre el Modelo OSI y el Modelo TCP/IP.

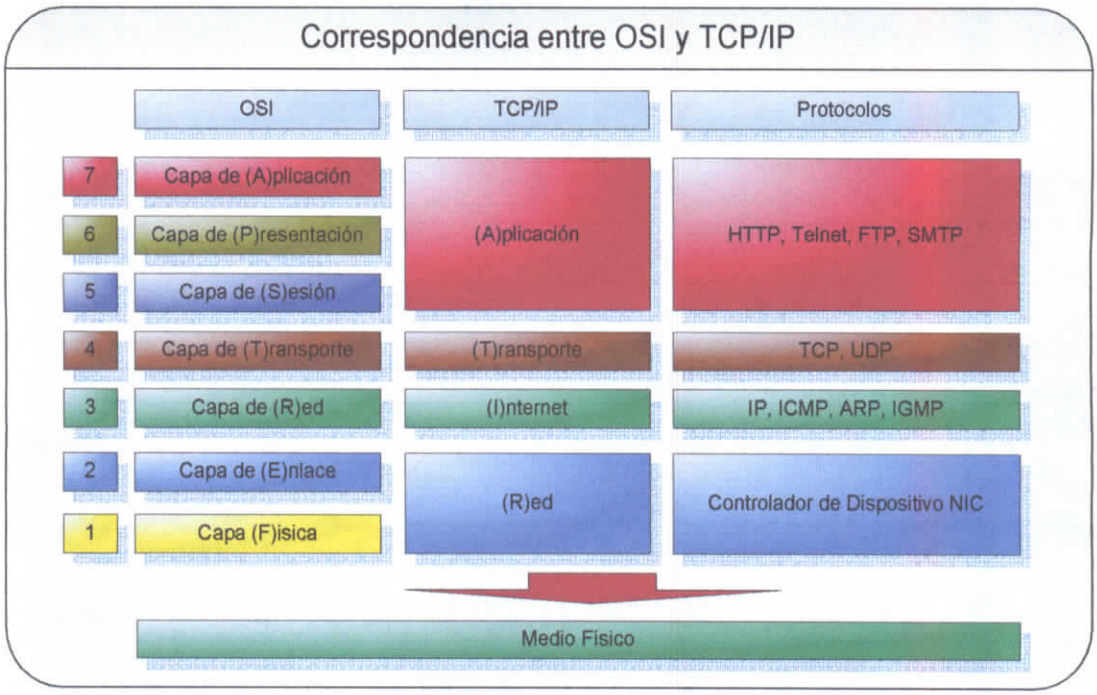


Figura 2.5. Correspondencia entre el Modelo OSI y el Modelo TCP/IP

El conjunto de protocolos TCP/IP está compuesto por dos protocolos:

1. ***El protocolo TCP (Transmission Control Protocol)*** o Protocolo de Control de Transmisión, que trabaja a nivel de Transporte del modelo OSI, garantizando un transporte fiable de los datos, permitiendo que dos anfitriones (host) establezcan una conexión e intercambiar datos, garantizando la entrega de datos, evitando que los datos se pierdan durante la transmisión, garantizando además que los paquetes sean entregados en el mismo orden en el que fueron enviados.
2. ***El protocolo IP (Internet Protocol)*** o Protocolo de Internet, que trabaja a nivel de Red del modelo OSI, encaminando los datos hacia otras máquinas, utilizando direcciones formados por series de cuatro números (byte = octeto), con un formato de punto decimal, por ejemplo: 192.168.35.1.

El conjunto de Protocolos TCP/IP, se ha convertido en el estándar que contiene todas las reglas de Internet. Se basa en el principio de asignar una dirección IP a cada equipo en la red para poder direccionar los paquetes de datos en la red. Gracias a su orientación original de uso militar, cumple con algunos criterios de seguridad que garantizan la transmisión de datos como son:

- Segmentación de paquetes.
- Uso de direcciones para cada equipo.
- Enrutamiento de Datos en la Red
- Control de errores en la transmisión de datos

2.3.1. COMANDOS TCP/IP

TCP integra dos grupos de comandos para implementar los servicios de red que son los siguientes:

- ***Comandos Remotos.*** Denominados también BERKELEY debido a que fueron desarrollados por la Universidad de Berkeley (California), están diseñados para comunicaciones entre sistemas operativos UNIX, como copia de archivos, conexiones, ejecución de Shell entre otros, todo vía remota, permitiendo utilizar los recursos de diversas redes como si fueran una sola. Entre los comandos más comunes tenemos:

RCP	Realiza una copia de archivos al mismo o a otro servidor
RLOGINGL-RLOGINVT	Se utiliza para hacer una conexión al mismo o a otro servidor
REXEC-RSH	Permite ejecutar comandos del sistema operativo en el mismo o en otro servidor.

- ***Comandos DARPA.*** Están diseñados para implementar emulación de terminales, transferencia de archivos, correo electrónico y manejo de información sobre usuarios. Se pueden utilizar para comunicación con computadores que manejen diferentes sistemas operativos. Entre los más comunes tenemos:

Kernel PC/TCP y **herramientas** asociadas: Se utilizan para cargar el núcleo TCP/IP en la memoria del computador.	
BOOTP	Asigna la dirección IP de la estación de trabajo
INET	Descarga el núcleo PC/TCP de la memoria y/o realiza estadísticas de red
KERNEL	Carga el núcleo TCP/IP en la memoria y lo deja residente

Configuración de la red: Permiten configurar TCP/IP con determinados parámetros.	
IFCONFIG	Configura el hardware para TCP/IP

IPCONFIG	Configura el software TCP/IP y la direcci6n IP

Transferencia de archivos: Se utilizan para transferir archivos entre distintos computadores.	
DDAT'ES	Muestra las fechas y horas guardadas en un archivo creado con el comando TAR
FTP	Transfiere archivos entre una estación de trabajo y un servidor
FRPSRV	Convierte una estación de trabajo en un servidor FTP
PASSWD	Se utiliza para poner contraseñas en las estaciones de trabajo a los usuarios para poder utilizar él comando FTPSRV
RMT	Permite realizar copia de archivos en una unidad de cinta
TAR	Realiza una copia de archivos creando un único archivo de BACKUP
TFTP	Transfiere archivos entre una estación de trabajo un servidor o a otra estación de trabajo sin necesidad de validar al usuario

Impresión: Permiten el control de la impresión en las impresoras conectadas al servidor.	
DOPREDIR	Imprime un trabajo de impresión que aún no ha sido impreso

IPRINT	Envía un texto o un archivo a un servidor de impresoras de imagen
LPQ	Indica el estado de la cola de impresión indicada
LPR	Envía un texto o un archivo a una impresora local o de red.
LPRM	Elimina trabajos pendientes de la cola de impresión
ONPREDIR	Realiza tareas de configuración para el comando PREDIR
PREDIR	Carga o descarga el programa que permite la impresión remota y lo deja residente.
PRINIT	Se usa con los comandos PREDIR y ONPREDIR
PRSTART	Indica a la estación de trabajo remota que imprima un archivo usando la configuración por defecto

Conexión a servidores: Permiten la conexión de los computadores a servidores de nuestra red.	
SUPDUP	Permite conectarse a otro servidor de la red
TELNET - TN	Es el método normal de conectarse a un servidor de la red

Información sobre los usuarios: Muestran información sobre los usuarios conectados a la red.	
FINGER	Muestra información sobre un usuario conectado a otra estación de trabajo

NICNAME	Muestra información sobre un usuario o sobre un servidor solicitada al centro de informaci6n de redes
WHOIS	Muestra información sobre un usuario registrado que esté conectado a otra estación de trabajo

Envío y recepción de correo: Estos comandos permiten el envío y/o recepción de correo entre los usuarios de la red.	
MAIL	Permite enviar y recibir correo en la red
PCMAIL	Permite leer correo. Se ha de usar con el comando VMAIL
POP2 - POP3	Se utiliza para leer correo. Se han de usar con VMAIL Y SMTP
SMTP	Se utiliza para enviar correo en la red
SMTPSRV	Permite leer el correo recibido
VMAIL	Es un comando que muestra una pantalla preparada para leer el correo recibido. Se utiliza en conjunción con los comandos PCMAIL, POP2 0 POP3

Chequeo de la red: Permiten chequear la red cuando aparecen problemas de comunicaciones.	
HOST	Indica el nombre y la dirección IP de una estación de trabajo determinada
PING	Envía una Llamada a una estación de trabajo e informa si se puede establecer conexión o no con ella

SETCLOCK	Muestra la fecha y la hora que tiene la red

2.3.2. ¿TCP/IP COMO FUNCIONA?

El funcionamiento de TCP/Ip se basa en el ensamblaje de bloques de datos en paquetes, cada paquete contiene una cabecera con información de control, en la que se incluye la dirección de destino y los datos, de esta manera el envío de información en la red se la realiza mediante una serie de paquetes.

En la capa de red se implementa el protocolo IP (Internet Protocol), el cual está concebido para permitir que las aplicaciones se ejecuten transparentemente sobre redes interconectadas, siendo independiente del hardware.

Paralelamente en la capa de transporte se implementa el protocolo TCP (Transfer Control Protocol), el cual asegura que los paquetes sean entregados, garantizando que lo que se envió sea lo que se recibe, este protocolo en al caso de que detecte que no es posible una transmisión fiable terminará la conexión.

2.4. Calidad de Servicio

La calidad de servicios comúnmente llamada Qos (Quality of Service), en el mundo de las redes de datos o redes de información, a nivel de telecomunicaciones, generalmente es interpretada de dos maneras:

- A la capacidad de definir por parte de los equipos que conforman la red y que prestan los servicios para permitir la fijación de las condiciones en que se desarrollaran las comunicaciones es decir la asignación de recursos, prioridades de transmisión, etc.
- A las cualidades del servicio que prestan las redes de comunicaciones en parámetros medibles y cuantificables, como es el tiempo de transferencia, tiempo de enlace, etc.

Ethernet es su concepción opera mediante conmutación de paquetes, la calidad de servicio en este tipo de redes se basa en la capacidad de controlar las distorsiones de la comunicación que se pueden presentar como son:

1. ***Pérdida de Paquetes:*** Los paquetes se pueden perder al no poder ser entregados al receptor, el principal problema que se produce por este concepto es la indisponibilidad del receptor debido a la saturación del buffer de entrada, lo que obliga a que los paquetes perdidos sean retransmitidos.
2. ***Retardo de Paquetes:*** Los paquetes se pueden retardar por dos factores: el primero por el camino o ruta que siguió el paquete debido al camino que tomo que no necesariamente es el más directo por evitar congestiones, dando la posibilidad que sea el más largo y el segundo por espera en la cola de entrada en el host de destino.
3. ***Jitter:*** Se denomina a la llegada de un grupo de paquetes con una prioridad distinta a la cola de entrada los cuales son procesados primero, lo que genera que los paquetes tengan retardos dispares, lo que afecta a las comunicaciones que

requieren que la llegada de los paquetes sean ordenados como es el caso del audio y el video en tiempo real.

4. ***Tiempo de Llegada de Paquetes:*** El tiempo de llegada de los diferentes paquetes debido al camino que tomaron los paquetes o al tiempo que pasaron en las diferentes colas antes de llegar al destino, provoca que los mismos lleguen en desorden, problema que es resuelto por determinados protocolos exclusivamente.
5. ***Errores en Paquetes:*** Fallas en el medio de comunicación utilizado para que los paquetes sean transportados, provoca la corrupción de datos o el reamado erróneo de los mismos.

El concepto básico de la calidad de servicio es indicarle a los diferentes equipos o nodos que intervienen en la comunicación y envío de paquetes, que priorice el envío de los paquetes y el procesamiento de los mismos obedeciendo una jerarquía como la siguiente:

0 *Tareas de Fondo*

1 *Estandar*

2 *Video*

3 *Audio*

4 *Best Effort*

5 *Paquetes de Aplicaciones del Negocio*

La satisfacción del cliente, normalmente estructurada en un SLA, define el referente de medida en lo relacionado a la calidad de servicio, que normalmente se cuantifica

en base a la percepción de éste en relación al servicio que recibe. De manera referencial se siguen cuatro factores de referencia:

a. ***Punto de Vista del Operador:*** Relacionada con la calidad que es capaz de entregar y que calidad fue a que entrego realmente.
b. ***Punto de Vista del Cliente:*** Relacionada con la calidad que realmente recibió y la calidad que el percibió que le entregaron.
c. ***Punto de Vista de la Tecnología:*** Los equipos utilizados para realizar la transmisión de paquetes y la gestión de los mismos proveen de contadores que permiten medir la calidad proporcionada mediante factores como son: La disponibilidad de las redes, los tiempos que se retardo en la comunicación, la velocidad de transferencia, la taza de errores.
d. ***Punto de Vista de la Demanda:*** Este punto de vista de difícil y complicado de definir y medir, debido a que por lo general se utilizan equipos de medida en cada punto del cliente, lo que dificulta la medición porque se requiere un numero significativo de equipos para que la muestra sea aceptable.

2.5. Análisis de Tráfico

Para analizar el tráfico de una red Ethernet típica de bus compartido, nos basamos en la utilización de sondas conectadas directamente al bus. Las sondas están provistas de su propia interfaz Ethernet, la cual funciona en modo promiscuo para capturar el trafico que será analizado constituyéndose así en la plataforma en que se ejecutaran de forma continua, aplicaciones propietarias o de dominio público, con las cuales se

determina el tipo de información que circula por la red y el impacto que pudiera llegar a tener sobre el rendimiento de la misma.

De esta forma se puede llegar a determinar la existencia de virus, el uso excesivo de aplicaciones de comunicaciones punto a punto, que son las que frecuentemente degradan el rendimiento de la red, principalmente si son utilizados los enlaces principales de acceso a Internet.

En la configuración de las redes actuales que utilizan conmutadores (switches), la sonda se conecta directamente a cada conmutador.

A dichas sondas se las conoce comúnmente como Sniffer, que refiriéndonos a la configuración de la red por su topología el medio de transmisión como puede ser Cable UTP, Fibra Óptica, etc. sea compartido por todos los elementos que se integran en la red, esta característica permite que un computador capture las tramas de información que circulen en el medio, sin necesidad que estos sean dirigidos hacia él. El Sniffer, logra capturar las tramas al poner su tarjeta de red en modo promiscuo de manera tal que en la capa de enlace de datos, las tramas no destinadas al equipo no son descartadas, y así se puede capturar todo el tráfico que viaja por la red.

Para complementar la idea, el modo promiscuo basa su utilidad en que todos los paquetes que pasan por una red tienen la información completa del protocolo al que pertenece y las opciones para ser ensamblado, se encuentren o no cifrados, por lo tanto puedo saber el contenido del paquete. Entre la información que contiene el paquete se encuentra: la dirección física (o dirección MAC) de quien lo envía y quien

lo tiene que recibir, de esta manera, cuando transmitimos un fichero, este se divide en varios paquetes de tamaño predeterminado.

La eficiencia de la captura de datos de los equipos utilizando sniffers, varía de acuerdo a la topología y el hardware que se utilice para comunicarse entre las redes. El modo promiscuo es muy utilizado para ver que paquetes atraviesan la red, para detectar ataques, errores, pérdida de paquetes, sobrecargas, etc. Al analizar los datos que pasan por la red se puede determinar preferencias de uso, necesidades de ancho de banda, accesos no permitidos a protocolos y a equipos.

Existen varias alternativas para detectar equipos o nodos que se encuentren en modo promiscuo, se basan en el uso de herramientas que envían paquetes que nadie respondería a excepción de equipos en modo promiscuo, entre las alternativas tenemos:

- ***Latencia en paquetes ICMP:*** Se lanzan muchas peticiones TCP erróneas, debido a que ningún equipo las tendrá en consideración a excepción de la que se encuentre en modo promiscuo, se envía paralelamente un ping a todos los equipos de la red, conocedores que el equipo que se demore en responder será el que se encuentre en modo promiscuo ya que éste se encontrará procesando los paquetes TCP erróneos. De ser el caso de tener un ataque, el atacante evitaría ser detectado al bloquear la entrada de peticiones ICMP en el cortafuegos de su equipo.
- ***Uso de Paquetes PING ICMP:*** Se envía un ping a todos los equipos de la red con la MAC del paquete errónea, el único equipo que responda será el que está

en modo promiscuo ya que no haría comprobación de la MAC. Sin embargo igual que el método anterior de ser el caso de un atacante se puede proceder de la misma forma para evitar ser detectado.

- ***Uso de Paquetes ARP:*** Al igual que en el método anterior, se lanza una petición ARP, con una dirección MAC con errores, el único equipo que responda será el que se encuentre en modo promiscuo. La forma de evitar ser detectado es disponer de una distribución de LINUX modificada de manera tal que no responda consultas ARP erróneas.
- ***Detección en base a resoluciones DNS:*** Varios de los programas de captura de paquetes, que funcionan en equipos configurados en modo promiscuo sueles activar una función de resolver las IP de los equipos remitentes y destinatarios. El método consiste en enviar paquetes modificando la dirección IP por una que no esté activa en la red, para detectar el momento en que se realicen las resoluciones DNS. La forma de evitar este método es desactivar esta función.

2.6. Analizador de Protocolos

Para analizar el tráfico es necesaria la utilización de herramientas como son los analizadores de protocolos que es una herramienta que permite el desarrollo y depuración de protocolos y aplicaciones de red. Permite al ordenador capturar los paquetes que viajan por la red para ser analizadas, sea en tiempo real o después de capturarlas.

Por análisis vamos a entender que el programa puede capturar la trama y reconocer a que protocolo pertenece como puede ser TCP, ICMP, etc., desplegando al usuario la

información decodificada. Así se puede ver todo lo que está circulando por la red en el período de tiempo en el que se está desarrollando el análisis.

Esto es importante cuando se están desarrollando protocolos o programas de transmisión de datos en una red, ya que permite comprobar lo que realmente hace el programa en la red.

Entre los usos que se da a los analizadores de protocolos tenemos:

- Soportar el desarrollo y demanda de nuevas aplicaciones.
- Analizar la eficiencia de una red de datos, mediante el análisis del tráfico, lo cual permite detectar problemas concretos.
- Análisis remoto de tráfico de redes.
- Monitorear varias redes simultáneamente.

Los analizadores de protocolos que se distribuyen comercialmente son de diversos tipos, desafortunadamente sus costos son muy elevados, dependiendo el numero de protocolos que pueden reconocer y decodificar, de la tecnología de red, si es software, o algún hardware especializado.

CAPITULO III

3. Herramientas de Análisis de Tráfico

Como se había definido una Sonda o Sniffer, es un programa que nos permite monitorizar el tráfico en una red computadoras, adicionalmente podernos con esta información analizar el tráfico, con el propósito de detectar los cuellos de botella y problemas que existan en la misma.

En nuestro caso de estudio, existen una gama de aplicaciones y soluciones destinadas las que incluyen hardware y software, desde aplicaciones propietarias de diferentes marcas hasta soluciones de código abierto, las cuales se implementan generalmente bajo Linux o UNIX.

Para efectos de nuestro estudio hemos seleccionado tres aplicaciones que nos permitirán recopilar la información necesaria para nuestro análisis.

3.1. Ethereal / WireShark

Ethereal es un potente analizador de protocolos, bautizado recientemente como WireShark, funciona bajo Unix, Mac OS y Windows.

Permite capturar los paquetes de viajan a través de una red, permitiendo además una captura en disco teniendo la capacidad de leer más de 20 tipos distintos de formatos. Soporta más de 300 protocolos debido a su desarrollo de código abierto.

Por su versatilidad es comúnmente utilizado como analizador de protocolos destinado a realizar análisis de los problemas y solucionarlos en redes de comunicaciones, así como también para el desarrollo de software y protocolos, es popular a nivel didáctico en centros educativos.

Cuenta con todas las ventajas de tcpdump, pero fortalecido con una interfaz gráfica incluyendo opciones de filtrado de información y organización. Permite ver de forma gráfica lo que pasa a través de la red, aunque es frecuentemente utilizado en redes Ethernet, es compatible con otro tipo de redes, estableciéndose en modo promiscuo. Aunque no muy popular cuenta además con una versión basada en texto denominada tshark.

Como se había indicado, WireShark permite examinar los datos que están pasando en vivo por la red o se puede almacenarlos en un archivo de captura en el Disco Duro del equipo para un análisis posterior, por medio de los detalles almacenados de cada paquete, con esta información utilizando la gama completa de protocolos que contiene, podemos incluso reconstruir el flujo completo de una sesión TCP.

Se distribuye como Software Libre y existen versiones funcionales para la mayoría de sistemas operativos entre los que se cuenta: Linux, Solaris, FreeBSD, NetBSD, OpenBSD, Mac OS X, Microsoft Windows, etc.

Las características más sobresalientes de Wireshark son:

- Mantenido bajo la licencia GPL.
- Trabaja tanto en modo promiscuo como en modo no promiscuo.
- Puede capturar datos de la red o leer datos almacenados en un archivo (de una captura previa).
- Basado en la librería pcap.
- Tiene una interfaz muy flexible.
- Gran capacidad de filtrado.
- Admite el formato estándar de archivos tcpdump.
- Reconstrucción de sesiones TCP
- Se ejecuta en más de 20 plataformas.
- Es compatible con más de 480 protocolos.
- Puede leer archivos de captura de más de 20 productos.

Debido al amplio espectro de posibilidades y a la capacidad de captura de WireShark, es necesario que se asignen permisos especiales al equipo en el que está instalado, por esta razón siempre debe ser ejecutado con un perfil Superusuario, principalmente porque hay que tomar en cuenta la cantidad de analizadores de protocolo que tiene implementados, los que se ejecutan cuando un paquete llega a la interfaz.

Siempre existe el riesgo de un error en el código del los analizadores, lo que potencialmente podría vulnerar la seguridad del sistema permitiendo entre otras cosas permitir la ejecución de código externo, por esta razón los desarroladores de Ethereal lo quitaron antes de ser lanzada la versión 3.6.

Si no se tiene confianza en el analizador, una alternativa viable es utilizar las herramientas tcpdump o dumpcap, los cuales permiten capturar los paquetes directamente desde la interfaz de usuario con privilegios de superusuario, y almacenarlos en el disco, para analizarlos posteriormente con WireShark con privilegios más reducidos.

A continuación revisaremos de manera general la herramienta tcpdump y pcap, con el objetivo de profundizar en la potencialidad de la misma, debido a que WireShark está implementado sobre las bases y principios de estas herramientas, el analizarlas y estudiarlas nos darán el conocimiento necesario para entender rápidamente el aplicativo que utilizaremos.

3.1.1. TCPDUMP

Tcpdump, es una herramienta que trabaja en línea de comandos que fue desarrollada principalmente para analizar el tráfico que se transporte por una red de datos, permitiendo al usuario captura y visualizar en tiempo real los paquetes que están siendo transmitidos en la red en la que está conectado el computador sobre el que se ejecuta. Funciona en todas las plataformas UNIX entre las que podemos resaltar:

Linux, Solaris, BSD, Mac OS X, HP-UX y AIX. Trabaja utilizando la biblioteca libpcap que permite capturar los paquetes que circulan en la red.
Para Windows se desarrollo una herramienta similar llamada WinDump, soportada por la biblioteca Winpcap.

Es necesario contar con privilegios de superusuario para utilizar estas herramientas.

Como parte de su funcionalidad, tiene la capacidad de implementar filtros para depurar la información obtenida. Los filtros se constituyen como expresiones que van después de las opciones, permitiéndonos así seleccionar la información que nos interesa. Si no se especificaran los filtros, la herramienta simplemente entrega todo el tráfico que el adaptador de red seleccionado vea.

Tcpdump es utilizado principalmente para:

- Depurar aplicaciones de comunicaciones utilizadas en la red.
- Corregir problemas de la red.
- Capturar datos enviados por otros usuarios. Esto es muy utilizado por usuarios poco éticos para capturar contraseñas e información, debido a que se aprovecha de protocolos como telnet y http, los cuales no cifran los datos que envían en la red.

Formato de Uso:

tcpdump	[-aAdDeflLnNOpqRStuUvxX] [-c count] [-C file_size] [-E algo:secret] [-F file] [-i interface] [-M secret] [-r file] [-s snaplen] [-T type] [-w file] [-W filecount] [-y datalinktype] [-Z user] [expression]
-A	Imprime cada paquete en código ASCII
-D	Imprime la lista de interfaces disponibles
-n	No convierte las direcciones de salida
-p	No utiliza el interfaz especificado en modo promiscuo
-t	No imprime la hora de captura de cada trama
-x	Imprime cada paquete en hexadecimal
-X	Imprime cada paquete en hexadecimal y código ASCII
-c count	Cierra el programa tras recibir 'count' paquetes
-C file_size	
-E	algo:secret
-F file	
-i interface:	
-M secret	Escucha en el interfaz especificado
-r file	
-s snaplen	
-T type	
-w file	Guarda la salida en el archivo 'file'
-W filecount	

-y datalinktype

-Z user

Filtros	
type [host|net|port]:	Máquina en particular [host], red completa [net] o puerto concreto [port].
dir [src|dst|src or dst|src and dst]:	Especifica desde [src] o hacia dónde [dst] se dirige la información.
proto [tcp|udp|ip|ether]:	Protocolo que queremos capturar.

3.1.2. Ejemplos de aplicación

Capturar tráfico cuya dirección IP de origen sea 192.168.3.1 — *tcpdump src host 192.168.3.1*

Capturar tráfico cuya dirección origen o destino sea 192.168.3.2 — *tcpdump host 192.168.3.2*

Capturar tráfico con destino a la dirección MAC 50:43:A5:AE:69:55 — *tcpdump ether dst 50:43:A5:AE:69:55*

Capturar tráfico con red destino 192.168.3.0 — *tcpdump dst net 192.168.3.0*

Capturar tráfico con red origen 192.168.3.0/28	*tcpdump src net 192.168.3.0 mask 255.255.255.240* *tcpdump src net 192.168.3.0/28*
Capturar tráfico con destino el puerto 23	*tcpdump dst port 23*
Capturar tráfico con origen o destino el puerto 110	*tcpdump port 110*
Capturar los paquetes de tipo ICMP	*tcpdump ip proto \\icmp*
Capturar los paquetes de tipo UDP	*tcpdump ip proto \\udp* *tcpdump udp*
Capturar el tráfico Web	*tcpdump tcp and port 80*
Capturar las peticiones de DNS	*tcpdump udp and dst port 53*
Capturar el tráfico al puerto telnet o SSH	*tcpdump tcp and \(port 22 or port 23\)*
Capturar todo el tráfico excepto el web	*tcpdump tcp and not port 80* *tcpdump tcp and ! port 80*
Capturar todo el tráfico a host	*tcpdump -vvv -n -s 65535 -A -p -w*

10.168.1.100 puerto 80, en full verbose mode, full snap length, sin ponerla en modo promiscuo, sin convertir las direcciones de salida, imprimir en ASCII y volcar todo el dump en un file.	*/tmp/tcpdump host 10.168.1.100 and port 80*

Nota: *Toda la información relacionada con TCPDUMP y los ejemplos han sido tomados de Wikipedia, por motivos didácticos se ha cambiado el formato de presentación y en algunos casos la forma de expresarlos.*

3.1.3. Como funciona?

Vamos a ver a continuación un ejemplo detallado de cómo funciona la captura de información utilizando la herramienta windump.

Como punto de partida, nos debe interesar conocer la información de nuestras interfaces de red y como están configuradas en para darnos acceso a nuestra red, para lo cual ejecutamos en la consola de comandos *ipconfig /all* y obtendremos la siguiente información:

C:\>ipconfig /all

Configuración IP de Windows

Nombre del host . . . . . : imit01

Sufijo DNS principal . . . . . : xxxxxxxxxx.int

Tipo de nodo. . . . . : híbrido

Enrutamiento habilitado. . . . . : No

Proxy WINS habilitado. . . . : No

Lista de búsqueda de sufijo DNS: xxxxxxxxxx.int

xxxxxxxxxx.int

Adaptador Ethernet Conexiones de red inalámbricas :

Sufijo de conexión específica DNS : xxxxxxxxxx.int

Descripción. . . . . : Intel(R) PRO/Wireless 3945ABG

Network Connection

Dirección física. . . . . : 00-1B-77-91-23-37

DHCP habilitado. . . . . : No

Autoconfiguración habilitada. . . : Sí

Dirección IP. . . . . : 192.168.35.202

Máscara de subred . . . . . : 255.255.255.0

Puerta de enlace predeterminada : 192.168.35.2

Servidor DHCP . . . . . : 192.168.35.45

Servidores DNS . . . . . : 192.168.35.10

Servidor WINS principal . . . . . : 192.168.35.10

Concesión obtenida . . . . . : jueves, 04 de febrero de 2010 13:26:08

Concesión expira . . . . . : lunes, 08 de febrero de 2010 0:46:08

Adaptador Ethernet Conexión de área local :

Sufijo de conexión específica DNS :

Descripción. . . . . : Intel(R) PRO/100 VE Network Connection

Dirección física. . . . . : 00-1B-24-6C-5B-40

DHCP habilitado. . . . . : No

Dirección IP. . . . . : 192.168.35.31

Máscara de subred . . . . . : 255.255.255.0

Puerta de enlace predeterminada : 192.168.35.2

Servidores DNS . . . . . : 192.168.35.10

C:\>

Con WinDump podemos solicitar la misma información pero desafortunadamente no es tan detallada como la que obtenemos con ipconfig, sin embargo debemos referenciarnos a la nomenclatura devuelta por WinDump, en nuestro ejemplo el resultado es:

C:\>windump –D

1.\Device\NPF_GenericDialupAdapter

(Adapter for generic dialup and VPN capture)

2.\Device\NPF_{C4AA022D-69A2-414B-9DD4-6E1E4C31BF35}

(Intel(R) PRO/Wireless 3945 ABG Network Connection (Microsoft's Packet Scheduler))

3.\Device\NPF_{B68F11BE-FA4A-4595-905E-3FB117C5898E}

(Intel(R) PRO/100 VE Network Connection (Microsoft's Packet Scheduler))

C:\>

En este caso si se desea capturar el tráfico de la interfaz *Intel(R) PRO/100 VE Network Connection (Microsoft's Packet Scheduler)* tenemos que utilizar WinDump con la opción *i* seguida del nombre de la interface con lo cual obtendremos el siguiente resultado:

Nota: Se ha dado formato a la salida para mejor comprensión del lector.

C:\> windump -i \Device\NPF_{B68F11BE-FA4A-4595-905E-3FB117C5898E}

windump: listening on
\Device\NPF_{B68F11BE-FA4A-4595-905E-3FB117C5898E}

16:34:50.576610 (NOV-ETHII)
IPX 00000000.00:00:74:82:da:0e.4100 >
00000000.ff:ff:ff:ff:ff:ff.0452: ipx-sap-nearest-req FileServer

16:34:50.618603 arp who-has 192.168.35.100 tell COMEX2

16:34:50.806430 802.1d config ffff.00:a0:d1:e7:25:d8.8002 root ffff.00:a0:d1:e7:25:d8 pathcost 0 age 0 max 6 hello 1 fdelay 4

16:34:50.888800 arp who-has 192.168.35.144 tell SECREUIO

16:34:50.889868 IP SECREUIO.137 > 192.168.35.255.137: UDP, length 50

16:34:51.573925 IP imit01.xxxxxxxxxx.int.19529 > SRVDAT01.53: 42116+ PTR? 100.35.168.192.in-addr.arpa. (45)

16:34:51.576920 IPX 00000000.00:00:74:82:da:0e.4100 > 00000000.ff:ff:ff:ff:ff:ff.0452: ipx-sap-nearest-req FileServer

16:34:51.634277 IP SECREUIO.137 > 192.168.35.255.137: UDP, length 50

16:34:51.806428 802.1d config ffff.00:a0:d1:e7:25:d8.8002 root ffff.00:a0:d1:e7:25:d8 pathcost 0 age 0 max 6 hello 1 fdelay 4

16:34:52.384276 IP SECREUIO.137 > 192.168.35.255.137: UDP, length 50

16:34:52.442901 IP SRVDAT01.53 > imit01.xxxxxxxxxx.int.19529: 42116 NXDomain 0/1/0 (122)

16:34:52.453219 arp who-has 192.168.35.100 tell imit01.xxxxxxxxxx.int

16:34:52.453465 arp reply 192.168.35.100 is-at 00:d0:b7:b6:24:b0

(oui Unknown)

16:34:52.453476 IP imit01.xxxxxxxxxx.int.137 >

192.168.35.100.137: UDP, length 50

16:34:52.453879 IP 192.168.35.100 > imit01.xxxxxxxxx.int:

ICMP 192.168.35.100 udp port 137 unreachable, length 86

16:34:52.806432 802.1d config ffff.00:a0:d1:e7:25:d8.8002 root

ffff.00:a0:d1:e7:25:d8 pathcost 0 age 0 max 6 hello 1 fdelay 4

16:34:53.806409 802.1d config ffff.00:a0:d1:e7:25:d8.8002 root

ffff.00:a0:d1:e7:25:d8 pathcost 0 age 0 max 6 hello 1 fdelay 4

16:34:53.939594 IP imit01.xxxxxxxxx.int.1674 >

SRVDAT01.445: P 3407829249:3407829387(138) ack

3380057047 win 17364

16:34:53.941910 IP imit01.xxxxxxxxxx.int.137 >

192.168.35.100.137: UDP, length 50

16:34:53.942026 IP imit01.xxxxxxxxxx.int.137 >

192.168.35.100.137: UDP, length 50

16:34:53.942403 IP 192.168.35.100 > imit01.xxxxxxxxxx.int: ICMP 192.168.35.100 udp port 137 unreachable, length 86

16:34:53.942803 arp who-has imit01.xxxxxxxxxx.int tell 192.168.35.100

16:34:53.943108 IP imit01.xxxxxxxxxx.int.1674 > SRVDAT01.445: P 138:266(128) ack 40 win 17325

16:34:53.945495 IP imit01.xxxxxxxxxx.int.1674 > SRVDAT01.445: P 266:376(110) ack 79 win 17286

16:34:53.948619 IP imit01.xxxxxxxxxx.int.1674 > SRVDAT01.445: P 376:514(138) ack 118 win 17247

16:34:53.950369 IP imit01.xxxxxxxxxx.int.1674 > SRVDAT01.445: P 514:648(134) ack 157 win 17208

16:34:53.951732 IP imit01.xxxxxxxxxx.int.1674 > SRVDAT01.445: P 648:772(124) ack 196 win 17169

16:34:53.952843 IP imit01.xxxxxxxxxx.int.1674 > SRVDAT01.445: P 772:882(110) ack 235 win 17130

16:34:53.954184 IP imit01.xxxxxxxxxx.int.1674 > SRVDAT01.445: P 882:1016(134) ack 274 win 17091

16:34:53.955881 IP imit01.xxxxxxxxxx.int.1674 >

SRVDAT01.445: P 1016:1152(136) ack 313 win 17052

16:34:53.957158 IP imit01.xxxxxxxxxx.int.1674 >

SRVDAT01.445: P 1152:1278(126) ack 352 win 17013

16:34:53.958131 IP imit01.xxxxxxxxxx.int.1674 >

SRVDAT01.445: P 1278:1388(110) ack 391 win 16974

16:34:53.959457 IP imit01.xxxxxxxxxx.int.1674 >

SRVDAT01.445: P 1388:1524(136) ack 430 win 16935

16:34:54.160652 IP imit01.xxxxxxxxxx.int.1674 >

SRVDAT01.445: . ack 469 win 16896

16:34:54.705904 IP 200-100-0-2.dsl.telesp.net.br.5678 >

255.255.255.255.5678: UDP, length 65

16:34:54.705939 CDPv1, ttl: 120s, Device-ID 'Atacazo', length 60

16:34:54.806398 802.1d config ffff.00:a0:d1:e7:25:d8.8002 root

ffff.00:a0:d1:e7:25:d8 pathcost 0 age 0 max 6 hello 1 fdelay 4

16:34:55.441965 IP imit01.xxxxxxxxxx.int.137 >

192.168.35.100.137: UDP, length 50

16:34:55.442118 IP imit01.xxxxxxxxxx.int.137 >

192.168.35.100.137: UDP, length 50

16:34:55.442502 IP 192.168.35.100 > imit01.xxxxxxxxxx.int: ICMP

192.168.35.100 udp port 137 unreachable, length 86

16:34:55.635902 arp who-has 192.168.35.144 tell SECREUIO

16:34:55.806395 802.1d config ffff.00:a0:d1:e7:25:d8.8002 root

ffff.00:a0:d1:e7:25:d8 pathcost 0 age 0 max 6 hello 1 fdelay 4

16:34:56.806328 802.1d config ffff.00:a0:d1:e7:25:d8.8002 root

ffff.00:a0:d1:e7:25:d8 pathcost 0 age 0 max 6 hello 1 fdelay 4

16:34:56.948652 IP imit01.xxxxxxxxxx.int.24043 >

SRVDAT01.53: 21013+ PTR?

143.35.168.192.in-addr.arpa. (45)

16:34:57.454299 arp who-has imit01.xxxxxxxxxx.int tell 192.168.35.100

16:34:57.454318 arp reply imit01.xxxxxxxxxx.int is-at 00:1b:24:6c:5b:40

(oui Unknown)

16:34:57.806320 802.1d config ffff.00:a0:d1:e7:25:d8.8002 root

ffff.00:a0:d1:e7:25:d8 pathcost 0 age 0 max 6 hello 1 fdelay 4

16:34:57.806644 IP SRVDAT01.53 > imit01.xxxxxxxxxx.int.24043: 21013 NXDomain 0/1/0 (122)

16:34:57.807273 arp who-has COMEX2 tell imit01.xxxxxxxxxx.int

16:34:57.807550 arp reply COMEX2 is-at 00:19:d1:27:bc:6f (oui Unknown)

16:34:57.807561 IP imit01.xxxxxxxxxx.int.137 > COMEX2.137: UDP, length 50

16:34:57.808103 IP COMEX2.137 > imit01.xxxxxxxxxx.int.137: UDP, length 193

16:34:57.939241 IP imit01.xxxxxxxxxx.int.1674 > SRVDAT01.445: P 1524:1664(140) ack 469 win 16896

16:34:58.207556 IP imit01.xxxxxxxxxx.int.1674 > SRVDAT01.445: P 1524:1664(140) ack 469 win 16896

16:34:58.268489 IP imit01.xxxxxxxxxx.int.1674 > SRVDAT01.445: P 1664:1804(140) ack 508 win 16857

16:34:58.413538 IP imit01.xxxxxxxxxx.int.1674 > SRVDAT01.445: P 1804:1950(146) ack 547 win 16818

16:34:58.415763 IP imit01.xxxxxxxxxx.int.1674 >

SRVDAT01.445: P 1950:2096(146) ack 586 win 16779

16:34:58.535682 IP imit01.xxxxxxxxxx.int.1674 >

SRVDAT01.445: . ack 625 win 16740

16:34:58.696340 arp who-has 192.168.35.144 tell SECREUIO

16:34:58.806340 802.1d config ffff.00:a0:d1:e7:25:d8.8002 root

ffff.00:a0:d1:e7:25:d8 pathcost 0 age 0 max 6 hello 1 fdelay 4

16:34:59.301412 IP imit01.xxxxxxxxxx.int.137 >

COMEX2.137: UDP, length 50

16:34:59.302038 IP COMEX2.137 >

imit01.xxxxxxxxxx.int.137: UDP, length 193

16:34:59.359773 IP imit01.xxxxxxxxxx.int.13637 >

SRVDAT01.53: 40375+ PTR?

144.35.168.192.in-addr.arpa. (45)

16:34:59.806358 802.1d config ffff.00:a0:d1:e7:25:d8.8002 root

ffff.00:a0:d1:e7:25:d8 pathcost 0 age 0 max 6 hello 1 fdelay 4

16:35:00.318556 IP SRVDAT01.53 >

imit01.xxxxxxxxxx.int.13637: 40375 NXDomain 0/1/0 (122)

16:35:00.319149 arp who-has 192.168.35.144 tell imit01.xxxxxxxxxx.int

16:35:00.634543 arp who-has 192.168.35.144 tell SECREUIO

16:35:00.806351 802.1d config ffff.00:a0:d1:e7:25:d8.8002 root

ffff.00:a0:d1:e7:25:d8 pathcost 0 age 0 max 6 hello 1 fdelay 4

16:35:01.806299 802.1d config ffff.00:a0:d1:e7:25:d8.8002 root

ffff.00:a0:d1:e7:25:d8 pathcost 0 age 0 max 6 hello 1 fdelay 4

16:35:01.817013 arp who-has 192.168.35.144 tell imit01.xxxxxxxxxx.int

16:35:01.910248 arp who-has 192.168.35.100 tell PSARANGO

16:35:02.806297 802.1d config ffff.00:a0:d1:e7:25:d8.8002 root

ffff.00:a0:d1:e7:25:d8 pathcost 0 age 0 max 6 hello 1 fdelay 4

16:35:03.317001 arp who-has 192.168.35.144 tell imit01.xxxxxxxxxx.int

16:35:03.806283 802.1d config ffff.00:a0:d1:e7:25:d8.8002 root

ffff.00:a0:d1:e7:25:d8 pathcost 0 age 0 max 6 hello 1 fdelay 4

16:35:04.420208 IP SECREUIO.137 >

192.168.35.255.137: UDP, length 50

16:35:04.711838 arp who-has 192.168.35.144 tell SECREUIO

16:35:04.806313 802.1d config ffff.00:a0:d1:e7:25:d8.8002 root

ffff.00:a0:d1:e7:25:d8 pathcost 0 age 0 max 6 hello 1 fdelay 4

16:35:04.822453 IP imit01.xxxxxxxxxx.int.28340 >

SRVDAT01.53: 27043+ PTR?

148.35.168.192.in-addr.arpa. (45)

16:35:05.165329 IP SECREUIO.137 > 192.168.35.255.137: UDP, length 50

16:35:05.677921 arp who-has GERENTE2

80 packets captured

162 packets received by filter

0 packets dropped by kernel

C:\>

Como se puede observar, el volumen de información que captura WinDump es muy extenso lo cual puede hacer que analizar la información sea muy difícil, por lo que se

pueden aprovechar las opciones de las que dispone para mejorar la calidad de la información capturada.

Por ejemplo, si requerimos que no resuelva las direcciones IP para que estas sean convertidas, simplemente utilizamos la opción *n*, puede ser que necesitemos que la información sea menos extensa o al contrario más completa podemos definir que la longitud de la información sea la que nosotros requerimos, por principio, la herramienta entrega los primeros 68 bytes, que es el tamaño de las cabeceras IP, TCP y UDP, para lo cual utilizamos la opción *s tamaño en bytes* , como podemos observar a continuación:

Utilizando la opción –n:

C:\> windump -i \Device\NPF_{B68F11BE-FA4A-4595-905E-3FB117C5898E} -n

windump: listening on

\Device\NPF_{B68F11BE-FA4A-4595-905E-3FB117C5898E}

17:29:56.088252 802.1d config ffff.00:a0:d1:e7:25:d8.8002 root ffff.00:a0:d1:e7:25:d8 pathcost 0 age 0 max 6 hello 1 fdelay 4

17:29:56.104416 IPX 00000000.00:00:74:82:da:0e.4100 > 00000000.ff:ff:ff:ff:ff:ff.0452: ipx-sap-nearest-req 0004

17:29:57.088251 02.1d config ffff.00:a0:d1:e7:25:d8.8002 root ffff.00:a0:d1:e7:25:d8 pathcost 0 age 0 max 6 hello 1 fdelay 4

17:29:57.105196 IPX 00000000.00:00:74:82:da:0e.4100 >

00000000.ff:ff:ff:ff:ff:ff.0452: ipx-sap-nearest-req 0004

17:29:58.088265 802.1d config ffff.00:a0:d1:e7:25:d8.8002 root

fff.00:a0:d1:e7:25:d8 pathcost 0 age 0 max 6 hello 1 fdelay 4

17:29:58.104313 (NOV-ETHII) IPX 00000000.00:00:74:82:da:0e.4100 >

00000000.ff:ff:ff:ff:ff:ff.0452: ipx-sap-nearest-req 0004

17:29:59.088301 802.1d config ffff.00:a0:d1:e7:25:d8.8002 root

ffff.00:a0:d1:e7:25:d8 pathcost 0 age 0 max 6 hello 1 fdelay 4

17:29:59.105503 (NOV-ETHII) IPX 00000000.00:00:74:82:da:0e.4100 >

00000000.ff:ff:ff:ff:ff:ff.0452: ipx-sap-nearest-req 0004

8 packets captured

11 packets received by filter

0 packets dropped by kernel

C:\>

Utilizando la opción –s:

C:\>windump -i \Device\NPF_{B68F11BE-FA4A-4595-905E-3FB117C5898E}

-s 1500

windump: listening on

\Device\NPF_{B68F11BE-FA4A-4595-905E-3FB117C5898E}

17:24:01.052544 802.1d config ffff.00:a0:d1:e7:25:d8.8002 root

ffff.00:a0:d1:e7:25:d8 pathcost 0 age 0 max 6 hello 1 fdelay 4

17:24:01.066120 IPX 00000000.00:00:74:82:da:0e.4100 >

00000000.ff:ff:ff:ff:ff:ff.0452: ipx-sap-nearest-req FileServer

17:24:02.052525 802.1d config ffff.00:a0:d1:e7:25:d8.8002 root

ffff.00:a0:d1:e7:25:d8 pathcost 0 age 0 max 6 hello 1 fdelay 4

17:24:02.066392 (NOV-ETHII) IPX 00000000.00:00:74:82:da:0e.4100 >

00000000.ff:ff:ff:ff:ff:ff.0452: ipx-sap-nearest-req FileServer

17:24:02.506830 IP (tos 0x0, ttl 128, id 29989, offset 0, flags [DF],

proto: TCP (6), length: 180) imit01.xxxxxxxxxx.int.1674 >

SRVDAT01.445: P 3408381699:3408381839(140)

ack 3380703080 win 16116

17:24:02.507378 IP (tos 0x0, ttl 128, id 57859, offset 0, flags [DF],

proto: TCP (6), length: 79) SRVDAT01.445 >

imit01.xxxxxxxxxx.int.1674: P, cksum 0x53b2

(correct), 1:40(39) ack 140 win 64875

17:24:02.508616 IP (tos 0x0, ttl 128, id 29990, offset 0, flags [DF], proto: TCP (6), length: 180) imit01.xxxxxxxxxx.int.1674 > SRVDAT01.445: P 140:280(140) ack 40 win 16077

17:24:02.509052 IP (tos 0x0, ttl 128, id 57860, offset 0, flags [DF], proto: TCP (6), length: 79) SRVDAT01.445 > imit01.xxxxxxxxxx.int.1674: P, cksum 0xa010 (correct), 40:79(39) ack 280 win 64735

8 packets captured

11 packets received by filter

0 packets dropped by kernel

Una vez recopilada la información, debemos saber leerla, para sacar el mejor provecho de ella. Entre los paquetes que podemos encontrar en una captura tenemos TCP, UDP, ARP y RARP, vamos a revisar la estructura de cada uno de ellos.

La estructura de un paquete típico TCP, se puede observar en la Figura 3.1.: Estructura Paquete TCP.

En algunos casos el paquete se puede complementar con dos datos adicionales que son:

- urgent: Existen datos urgentes.
- options: Indica la existencia de opciones. En caso de que haya van entre < y >.

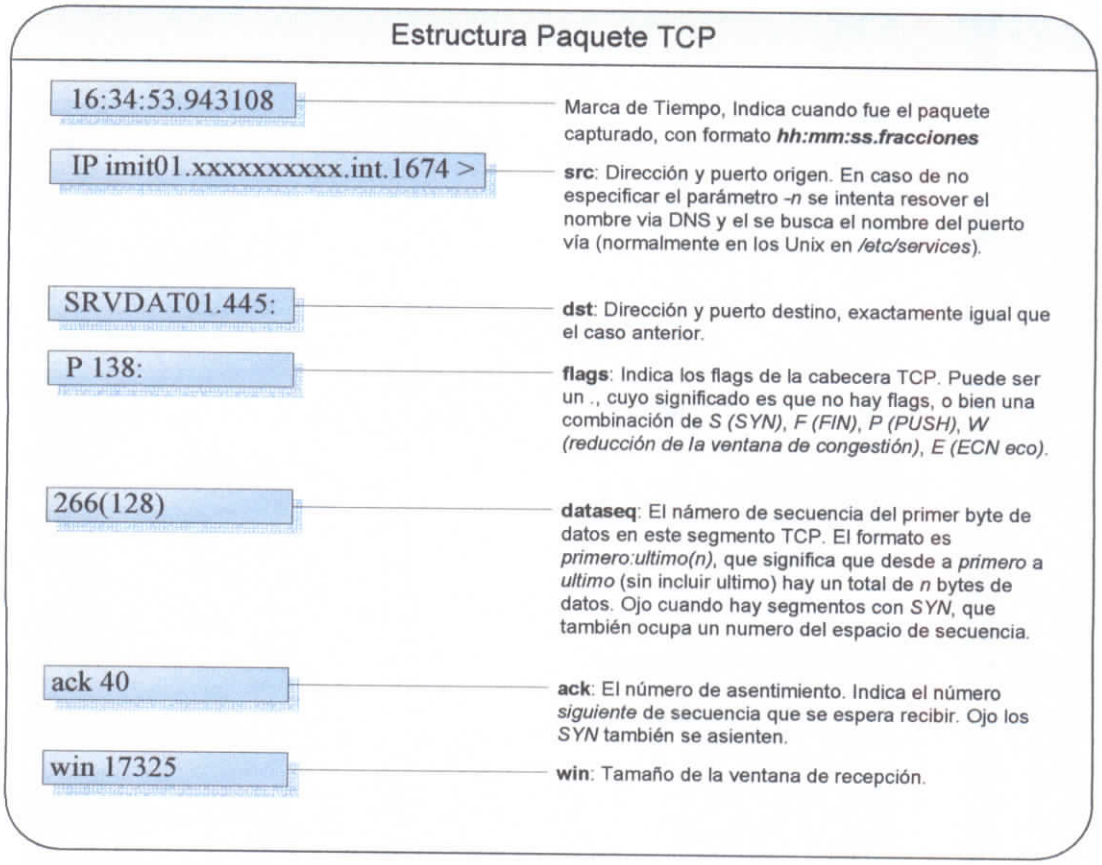


Figura 3.1. Estructura Paquete TCP

El protocolo ARP/RARP, normalmente genera dos tipos de paquetes, uno de requerimiento de información, en el que un equipo hace una consulta, y uno de respuesta en el que el equipo que ha procesado el requerimiento responde.

En la Figura 3.2.: Estructura Paquete ARP, podemos observar los dos paquetes tanto el de requerimiento como el de respuesta, si se desea profundizar en el manejo de este paquete se pueden referir para ARP en RFC 826 y para RARP en RFC 1293.

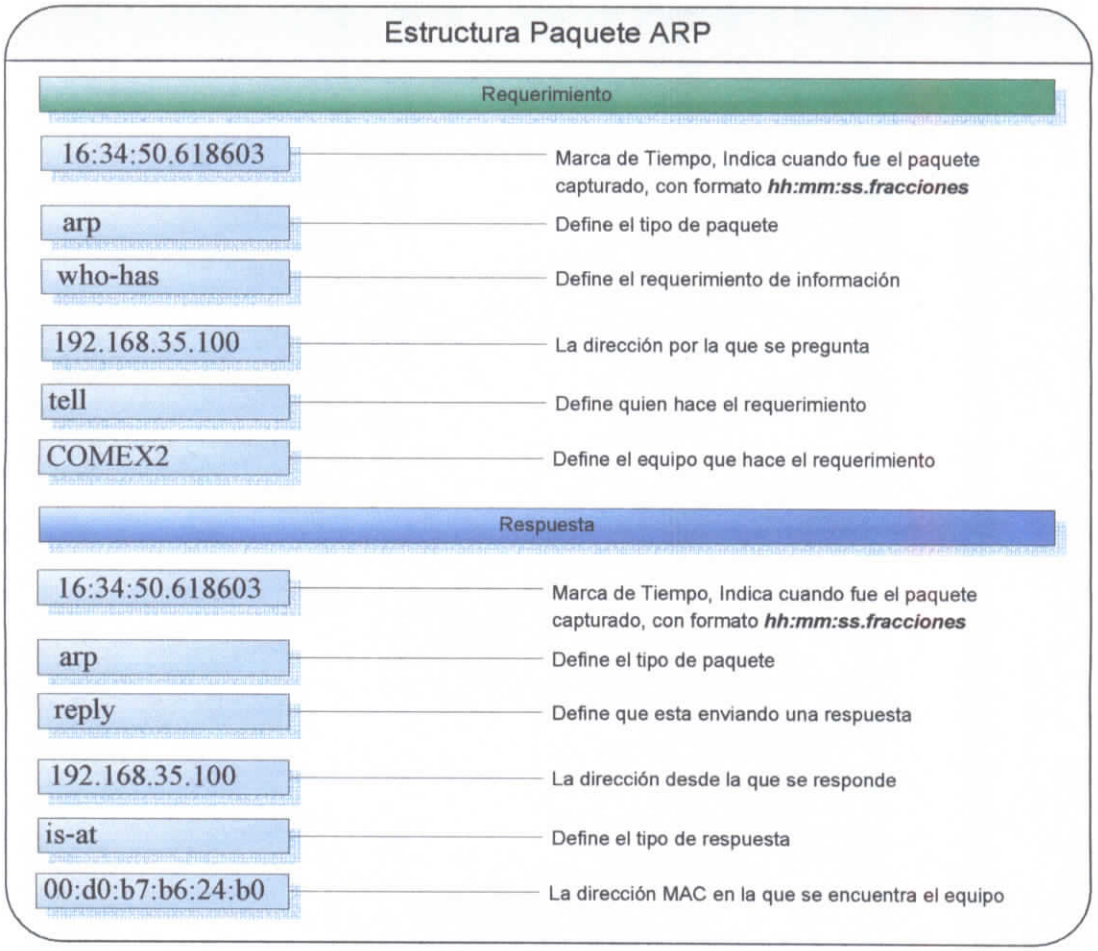


Figura 3.2. Estructura Paquete ARP

Un paquete UDP tiene la estructura que se puede observar en la Figura 3.3.: Estructura Paquete UDP.

Como hemos podido observar en los ejemplos entregados, el volumen de información obtenido puede ser enorme, lo cual si se desea realizar un análisis detallado y a su vez específico puede ser complejo el procesar toda la información dada.

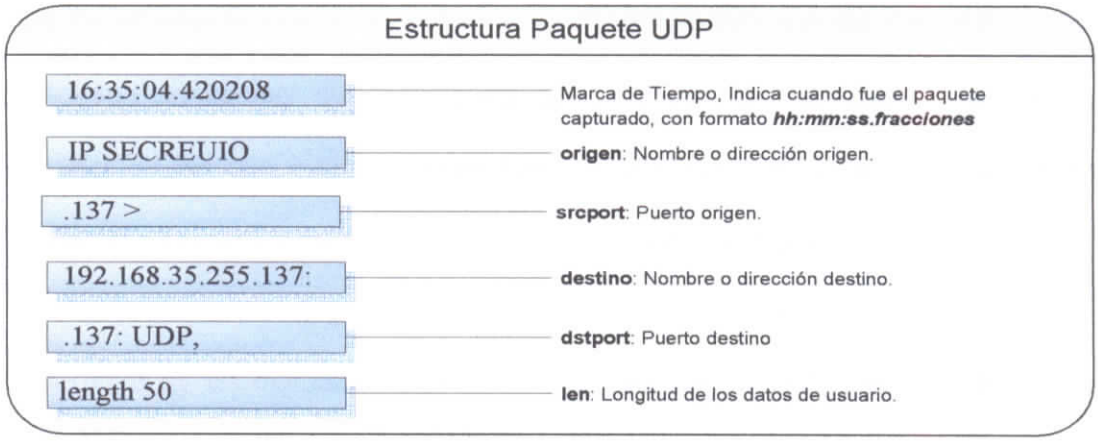


Figura 3.3. Estructura Paquete UDP

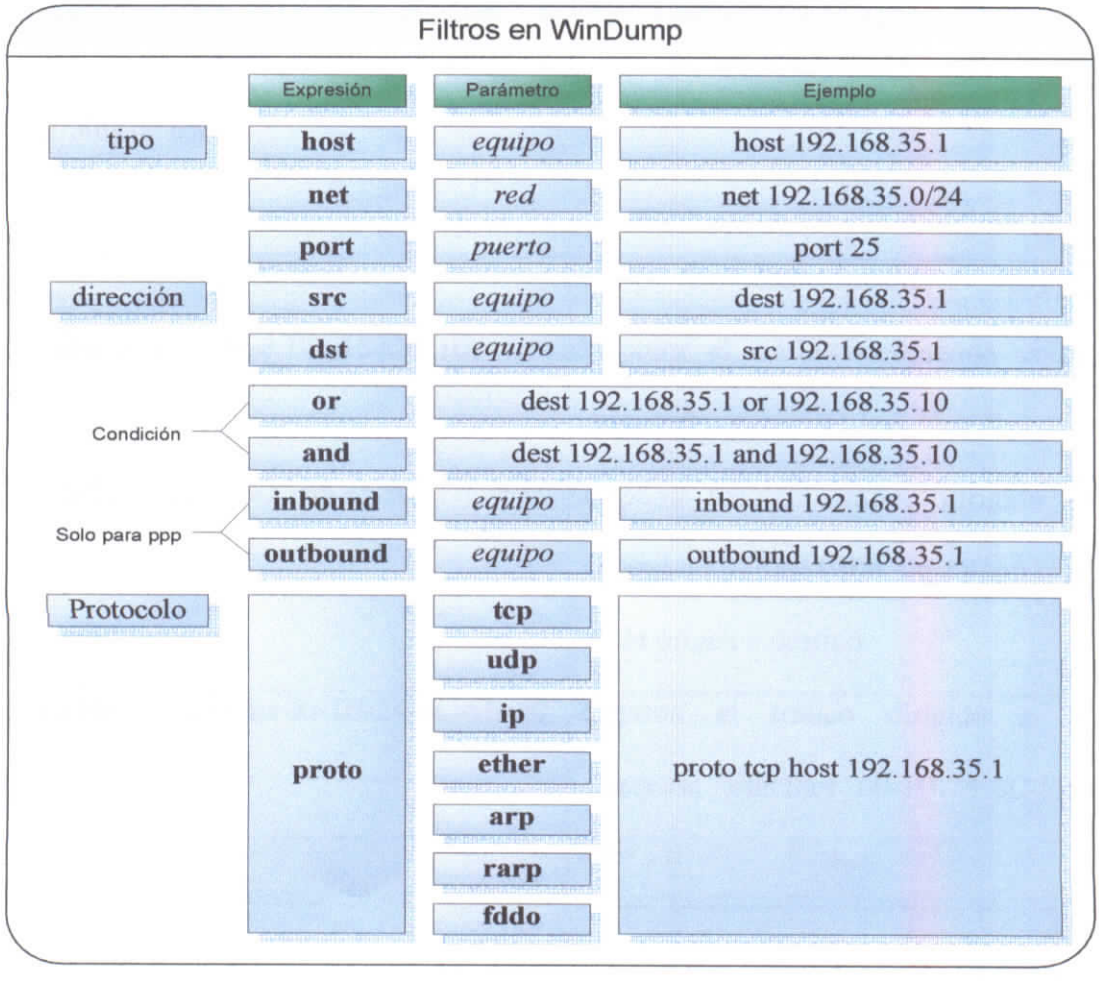


Figura 3.4. Filtros en WinDump

3.1.4. PCAP

PCAP, es la interfaz que es utilizada por una herramienta o aplicación para capturar paquetes de una red. En Linux la interfaz se denomina libpcap y en Windows WinPcap.

Como se indico esta interfaz es utilizada por una aplicación para capturar los paquetes que viajan por la der de datos y en las últimas versiones tiene ya implementada la capacidad de transmitir paquetes directamente a la capa de enlace, así como capturar y listar las interfaces habilitadas para su uso con la interfaz.

Esta interfaz es utilizada por WireShark y WinPump para su implementación de captura de paquetes.

3.2. Look@LAN

Look@LAN es un escáner de red diseñado para monitorear la red en rangos específicos de direcciones IP. Proporciona datos detallados de cada uno de los host que corresponden a cada dirección.

Entre otras cosas permite:

- Monitorear y obtener toda la información de la red.
- Reporte de todos los cambios que se presenten en los diferentes nodos.

- Monitoreo en Tiempo Real
- Se ejecuta en cualquier nodo de la red.
- Reportes gráficos.

3.3. QCheck

Qcheck es una herramienta diseñada para medir en rendimiento y conectividad de una red de datos fácilmente. Es un producto desarrollado por IXIA. Por su arquitectura, permite ser ejecutada en segundo plano, sin que interfiera con otras aplicaciones de tráfico, de tal forma que se pueda medir la red de datos en condiciones reales de funcionamiento.

CAPITULO IV

4. CASO PRÁCTICO: Análisis de la Red Actual de la Red de Datos de la Empresa y Presentación del Diseño Óptimo de acuerdo a los resultados del mismo.

4.1. Descripción del Análisis a Ejecutar

El objetivo principal de nuestro análisis es determinar si la estructura actual de transporte de información es la adecuada. El análisis de datos se centrará específicamente en la información relacionada con Correo Electrónico, Internet y demás servicios que dependen de este, y estructura del direccionamiento IP. Los datos que se recopilarán a nivel de tráfico están centrados en trafico relacionado con el protocolo TCP/IP.

4.2. La Empresa

La empresa es una Compañía Agroindustrial, domiciliada en la ciudad de la Concordia, provincia de Esmeraldas, las Oficinas Administrativas se encuentran ubicadas en la Ciudad de Quito, su principal actividad es enlatar y embasar productos agrícolas, destinado para el consumo local e internacional. En la actualidad el 100% de su producción está destinado a la exportación a diferentes países, ubicados en

Europa, Norte América, Sud América, Asia y Medio Oriente. Proyectan en los próximos meses iniciar ventas en el mercado local.

El contacto con sus clientes y proveedores es por vía electrónica utilizando principalmente correo electrónico y otras herramientas similares que la complementan.

4.3. Descripción de la Red Actual

La red de datos está integrada como se muestra en la Figura 4-1: Distribución Actual de la Red de Datos.

Como podemos observar la red de datos está distribuida en dos segmentos, uno ubicado en la ciudad de Quito el en cual se concentran todos los servidores y servicios, así como también un grupo de clientes, y el segundo ubicado en la ciudad de la Concordia en el cual se concentran únicamente clientes que acceden a los diferentes servicios de Quito.

4.4. Listado, Descripción de Equipos Existentes

4.4.1. Servidores.

Existen varios equipos que fungen como servidores distribuidos de la siguiente forma:

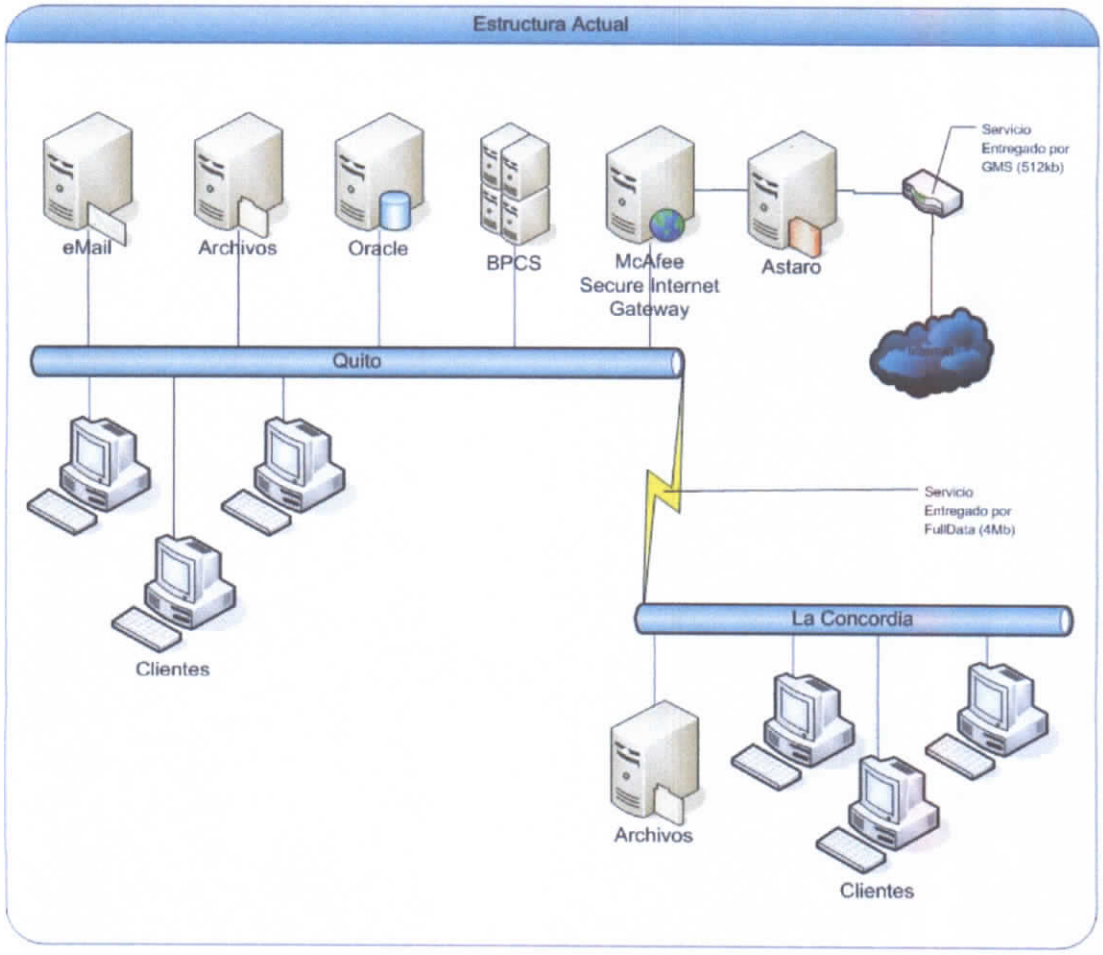


Figura 4.1. Distribución Actual de la Red de Datos

1. ***Servidor Dell:*** Dedicado a mantener los servicios que utilizan las aplicaciones de gestión que posee la compañía.

Equipo	
Concepto	**Detalle**
Marca	Dell
Modelo	PowerEdge 1800
Memoria	4Gb.

Sistema Operativo	Microsoft Windows 2000 5.00.2195 SP4
Procesador	2 x Intel Xeon 3.2Ghz
SCSI and RAID	DELL PERC 4/DC RAID Controller
DVD/CD-ROM	IIT-DT-ST DVD-RAM GSA-H20N
Discos Duros	4 x 33.87 Gb. Hot Swat

Servicios	
Concepto	**Detalle**
Base de Datos	Oracle 8i Enterprise Edition Release 8.1.7.4.1 – Production With The Objects Option
Esquemas Levantados	CBM_ISO_MANAGER GMS REAL SISMAC SPYRAL TPLUS WORKFLOW
BPCS Session Manager	BPCS Client/Server V6.1.02
Servicios BPCS Server	eBPCS Batch Service eBPCS Environments eBPCS Launcher Service eBPCS License Manager

2. ***Servidor Intel:*** Dedicado al manejo de Correo Electrónico

Equipo	
Concepto	**Detalle**
Marca	Intel
Modelo	
Memoria	2 Gb.
Sistema Operativo	Linux Red Hat
Procesador	
SCSI and RAID	
DVD/CD-ROM	
Discos Duros	

Servicios	
Concepto	**Detalle**
Correo Electrónico	Squirrel Mail

3. **Servidor de Archivos:** Sirve para mantener todos los documentos de trabajo de los diferentes departamentos, es utilizado además para mantener respaldos de los archivos que maneja cada uno de los funcionarios de la organización.

Equipo	
Concepto	**Detalle**
Marca	Intel

Modelo	
Memoria	3 Gb.
Sistema Operativo	Microsoft Windows 2003 Enterprise Ed.
Procesador	Intel Core 2 Quad CPU Q6600 2.4 Ghz.
SCSI and RAID	
DVD/CD-ROM	TSSTcorp CD/DVDW SH-S182F
Discos Duros	4 x SATA 698.63 Gb.

Servicios	
Concepto	**Detalle**
Archivos Compartidos	Archivos Compartidos de Windows 2003 Server

4. **McAfee Secure Internet Gateway:** Dedicado al control de Seguridad Perimetral, ubicado entre el Firewall y la red de datos.

Equipo	
Concepto	**Detalle**
Marca	McAfee
Modelo	3000
Memoria	2Gb
Sistema Operativo	Linux Red Hat
Procesador	1 Dual Core x86/x64

SCSI and RAID	
DVD/CD-ROM	1 CD/ROM
Discos Duros	120 Gb

Servicios	
Concepto	**Detalle**
Servicios	E-Mail Anti-Spam Web Filtering

5. **FireWall:** Equipo dedicado al control de acceso desde Internet hacia la red local y viceversa .

Equipo	
Concepto	**Detalle**
Marca	Intel
Modelo	
Memoria	2Gb
Sistema Operativo	Linux – Astaro Security Gateway V7
Procesador	1 Dual Core 3Ghz
SCSI and RAID	
DVD/CD-ROM	TSSTcorp CD/R-RW
Discos Duros	120 Gb

Servicios	
Concepto	**Detalle**
Servicios	Firewall ASTARO

4.4.2. Clientes

Los clientes todos son equipos que manejan Windows XP Professional con Service Pack 2.

4.4.3. Comunicaciones

Las Comunicaciones se manejan con los equipos que se detallan a continuación:

1. **Switch DES1228:** De la familia Web Smart II de D-Link, es una solución costo efectivo para pequeñas y medianas empresas que requieren de una fácil administración con características avanzadas como segmentación de VLAN, Calidad de Servicio QoS, seguridad 802.1x autentificación de usuario, fácil de administrar y configurar. Este Switch incorpora 24 puertos 10/100Base-TX, 4 puertos Gigabit 1000Base-T y 2 puertas 1000BASE-T/SFP tipo Combo para flexibilidad de conexión en fibra o cobre, para áreas de almacenamiento de la red o servidores. La interfaz gráfica para usuario (GUI), permite implementar Calidad de Servicio (QoS), VLANs y seguridad sin la necesidad de accesar a un sistema complejo de administración basado en líneas de comando usado generalmente en otros switches administrables.

El Switch DES-1228 incorpora avanzados mecanismos para detectar un ataque contra la unidad central de procesamiento (CPU) del switch y así, tomar una acción correctiva sobre la plataforma de ataque. Cuando una denegación de servicio (DoS) es removida frente a un ataque contra el DES-1228, la aplicación D-Link Safeguard Engine detecta la amenaza y previene la sobrecarga de datos en la CPU, de este modo, asegurando la integridad de la red y ayudando a mantener abiertos los canales para el ancho de banda.

El Switch Smart DES-1228 soporta puertos trunk hasta 6 grupos de 8 puertos por equipo. Los puertos pueden ser interconectados a través del uso de link aggregation para ampliar el ancho de banda hacia servidores o hacia el backbone de la red. Esto permite eliminar los cuellos de botella entre los switches que estén cascadeados.

Soporta la creación de VLAN´s para mejorar la seguridad y la utilización del ancho de banda. Las VLAN´s trabajan a través de segmentación de dominios, de este modo reduciendo la congestión de la red. El uso de redes virtuales puede ser configurado para segmentar los recursos de una red departamental. Por ejemplo, las VLAN´s pueden ser implementadas sobre una red en empresas medianas y pequeñas, para asegurar al departamento de Marketing beneficios de acceso seguro a los recursos de cada uno de los grupos departamentales.

El Switch Smart DES-1228 soporta SNMP v.1 (Simple Network Management Protocol) como una poderosa herramienta en administración y control para todos los dispositivos de red que soporten SNMP. Esto permite al DES-1228 ser

elegido para proveer de información valiosa sobre el estatus de cada dispositivo en la red. El acceso a esta vital información de administración permite ahorrar tiempo y dinero en la gestión.

La función de Spanning Tree provee protección frente a loops formados de manera no intencional en la infraestructura de la red. Estos loops son peligrosos cuando ellos crean un círculo interminable donde el tráfico de broadcast y multicast se propaga a través de la red formando un loop infinito, sin llegar a un ningún destino con la información. Esto crea una tormenta en el tráfico que congestiona la red y hace que ella funcione más lenta. Por tanto, detecta y destruye estos loops, asegurando el tiempo de respuesta.

Tiene Incorporada la función IGMP Snooping, que permite asegurar tráficos de información tales como registros de audio, video, voz, sin incrementar la congestión de broadcast en la red. Así, el DES-1228 de manera inteligente, habilita el acceso o reenvía dicha información sólo a los miembros o usuarios que estén dentro de tales aplicaciones.

Cuenta con Autentificación de usuario 802.1x que provee de un medio seguro para permitir a los usuarios registrarse en la red. Cuando esto es usado en conjunto con un Servidor RADIUS, la autentificación requiere que cada usuario inscrito en el DES-1228 provea de un nombre de usuario y password para acceder a los beneficios de la red de área local.

Ficha Técnica:

PUERTOS	- 24 puertas 10/100 Base-TX - 2 puertos 10/100/1000 Base-T - Auto MDI-MDIX - 2 Puertos Combo 1000Base-T/SFP
ESTÁNDARES	- IEEE 802.3 - IEEE 802.3u - IEEE 802.3x, Flow Control - IEEE 802.3ab - IEEE 802.3z - ANSI/IEEE 802.3 Nway auto-negotiation
MÉTODO DE SWITCHING	- Store-and-forward
SWITCHING CAPACITY	12,8 Gbps
MAC ADDRESS TABLE	8K.
JUMBO FRAME	Hasta 9,216 Bytes
MAX. FORWARDING RATE	9,52 Mpps
PACKET BUFFER MEMORY	128 KB
SDRAM FOR CPU	8 MB
FLASH MEMORY	2 MB
VLAN	- IEEE 802.1Q Tagged VLAN - Max. Número de VLANs: Total 256 - Configurable ID: 1-4094
QOS (CALIDAD SE SERVICIO)	- 802.1p Priority Queues - Max. N° de colas por puerto: 4

	- Support WRR mode in queue handling
IGMP SNOOPING	- 64 static multicast address - Modo Tráfico Multicast: flooding
PORT MIRRORING	- One to One - Many to One - Soporta modo TX, RX y Both
SEGURIDAD PARA EL ACCESO A LA RED	- Static Mac - Control de Acceso 802.1x port-based - Control Tormenta Broadcast: Rangos de 8/16/32/64/128/256/512/1,024/2,048/4,096 Kbps - D-Link Safeguard Engine: Protect CPU, Broadcast/Multicast/Unicast flooding - Port Access Control
SPANNING TREE	- 802.1D STP - STP & BPDU forwarding
STATIC PORT TRUNK	- Number of trunking group: 6 (max.) - Number of ports per trunk: 8 (max.)
TOPOLOGÍA	Estrella

FUNCIONES DE ADMINISTRACIÓN	Administración - SNMP v.1 - SNMP Traps: Destination IP, System Events, Fiber Port Events, Twisted-Pair Port Events. - Web-based management - Switch Discovery/Management Utility(Name is SmartConsole)- RMON monitoring - DHCP client MIBs Soportadas - MIB-II RFC 1213 - D-Link Enterprise Private MIB
FIRMWARE UPGRADE	Via SmartConsole Utility
LEDS INDICADORES	Por dispositivo: - Power - CPU Por puerto 10/100 Mbps: - Link/Act - 100Mbps Por puerto 10/100/1000 Mbps:

	- Link/Act - 1000Mbps - 100Mbps Por puerto SFP: - FX Link - Link/Act - 1000Mbps - 100Mbps
FUENTE DE PODER	Interna Universal, 100 a 240 VAC, 50/60 Hz
CONSUMO	18,35 Watts
HEAT CONSUMPTION	62.57 (btu/hr)
MTBF	326.647 Horas
TAMAÑO	Montable en rack estándar de 19", 1 U
DIMENSIONES	440mm x 140mm x 44mm
PESO	2.08 Kg (solo el equipo)
TEMPERATURA DE OPERACIÓN	0°C a 40°C
TEMPERATURA DE ALMACENAJE	-10°C a 70°C
HUMEDAD DE OPERACIÓN	10% a 90 % no condensada
HÚMEDAD DE ALMACENAJE	5% a 90 % no condensada

EMISSION(EMI)	FCC Class A, CE Class, VCCI Class A
SEGURIDAD	cUL, UL

2. **Switch DGS1024D:** General: Una vez más D-Link entrega respuesta a los requerimientos de los usuarios, incorporando la tecnología Gigabit Ethernet al segmento SOHO.

El switch desktop de 24 puertas 10/100/1000Mbps NWay de D-Link, es una excelente opción para pequeños grupos de trabajo, ya que permite conectar en forma simple cualquier puerta de 10Mbps, 100Mbps ó 1000Mbps, satisfaciendo las demandas de tráfico de cualquier usuario.

Principales Características y Facilidades:

- 24 puertas 10/100/1000Mbps NWay
- Todas las puertas soportan MDI/MDIX
- 48 Gbps de Backplane
- Flow Control IEEE 802.3x
- Fácil Instalación, plug and play
- Kit de montaje, para instalación en rack estándar de 19"
- Comprensivos leds indicadores
- Alto Rendimiento, y
- Fácil integración en red.

Ficha Técnica

PUERTAS	24 Puertas RJ-45 1000BASE-T
ESTANDARES	• IEEE 802.3 10BASE-T Ethernet (twisted-pair copper) • IEEE 802.3u 100BASE-TX Fast Ethernet (twisted-pair copper) • IEEE 802.3ab 1000BASE-T Gigabit Ethernet (twisted-pair copper) • ANSI/IEEE 802.3 NWay auto-negotiation • IEEE 802.3x Flow Control
TASA DE TRANSFERENCIA DE DATOS	• Ethernet: 10Mbps (half-duplex), 20Mbps (full-duplex) • Fast Ethernet: 100Mbps (half-duplex), 200Mbps (full-duplex) • Gigabit Ethernet: 2000Mbps (full duplex)
CABLES DE RED	- 10BASE-T: UTP Cat. 3, 4, 5 (100 m max.), EIA/TIA-586 100-ohm STP (100 m max.) - 100BASE-TX, 1000BASE-T: UTP Cat. 5, Cat. 5e (100 m max.), EIA/TIA-568 100-ohm STP (100 m max.)

MÉTODO DE ACCESO	CSMA/CD
MEDIA INTERFACE EXCHANGE	Auto MDI/MDI-X en cada puerta
TWISTED-PAIR RX REVERSE POLARITY	Auto-corrección en cada puerta
MÉTODO DE TRANSMISIÓN	Store-and-Forward
TOPOLOGÍA	Estrella
MAC ADDRESS LEARNING	Actualización Automática
MAC ADDRESS TABLE	8K por switch
RAM BUFFER	512KB
BACKPLANE (SWITCH FABRIC)	48 Gbps
PACKET FILTERING RATE	- 10BASE-T: 14,880 pps por Puerta (half-duplex) - 100BASE-TX: 148,810 pps por Puerta (half-duplex) - 1000BASE-T: 1,488,100 pps por Puerta (half-duplex)
PACKET FORWARDING RATES	- 10BASE-T: 14,880 pps por Puerta (half-duplex) - 100BASE-TX: 148,810 pps por Puerta (half-duplex) - 1000BASE-T: 1,488,100 pps por Puerta (half-duplex)

LEDS INDICADORES	Por Puerta: Link/Actividad, velocidad 10/100Mbps (10/100Mbps ports), velocidad 1000Mbps (10/100/1000Mbps) Por Switch: Power
FUENTE DE PODER	Interna, Universal 100 –240 VAC, 50/60 Hz, 0.3 A
CONSUMO	37,5 Watts Max.
TAMAÑO	Desktop
DIMENSIONES	280 x 180 x 44 mm
PESO	1,8 Kg..
TEMPERATURA DE OPERACIÓN	0°C a 40°C
TEMPERATURA DE ALMACENAJE	-10°C a 55°C
HUMEDAD	5% - 95% no condensada
EMISIÓN	FCC Class A, CE Class A, VCCI Class A
SEGURIDAD	CSA

3. **Radios Lobometrics:** Radios Lobometrics Modelo 954, utilizados como Routers y que permiten el enlace entre los dos sitios geográficos de la empresa Quito – La Concordia, contando con un punto de repetición en el Atacaso.

4.5. Configuración de Equipos Existentes

Debido a que se trata de realizar un análisis de la configuración de la Red de Datos de la Compañía nos concentraremos en la configuración relacionada con la integración de la red. Para esto utilizaremos la herramienta Look@LAN, para la recopilación de la información requerida.

La información de configuración se la realiza siguiendo el Esquema de Red que se muestra en la Figura 4.2.: Esquema de Red.

De cada uno de los equipos analizados se tomará la siguiente información, activando el servicio SNMP, así como la ficha de revisión del sistema Look@LAN:

- Detalles del Sistema
- Interfaces de Red
- Redes TCP/IP
- Rutas
- Información del Sistema

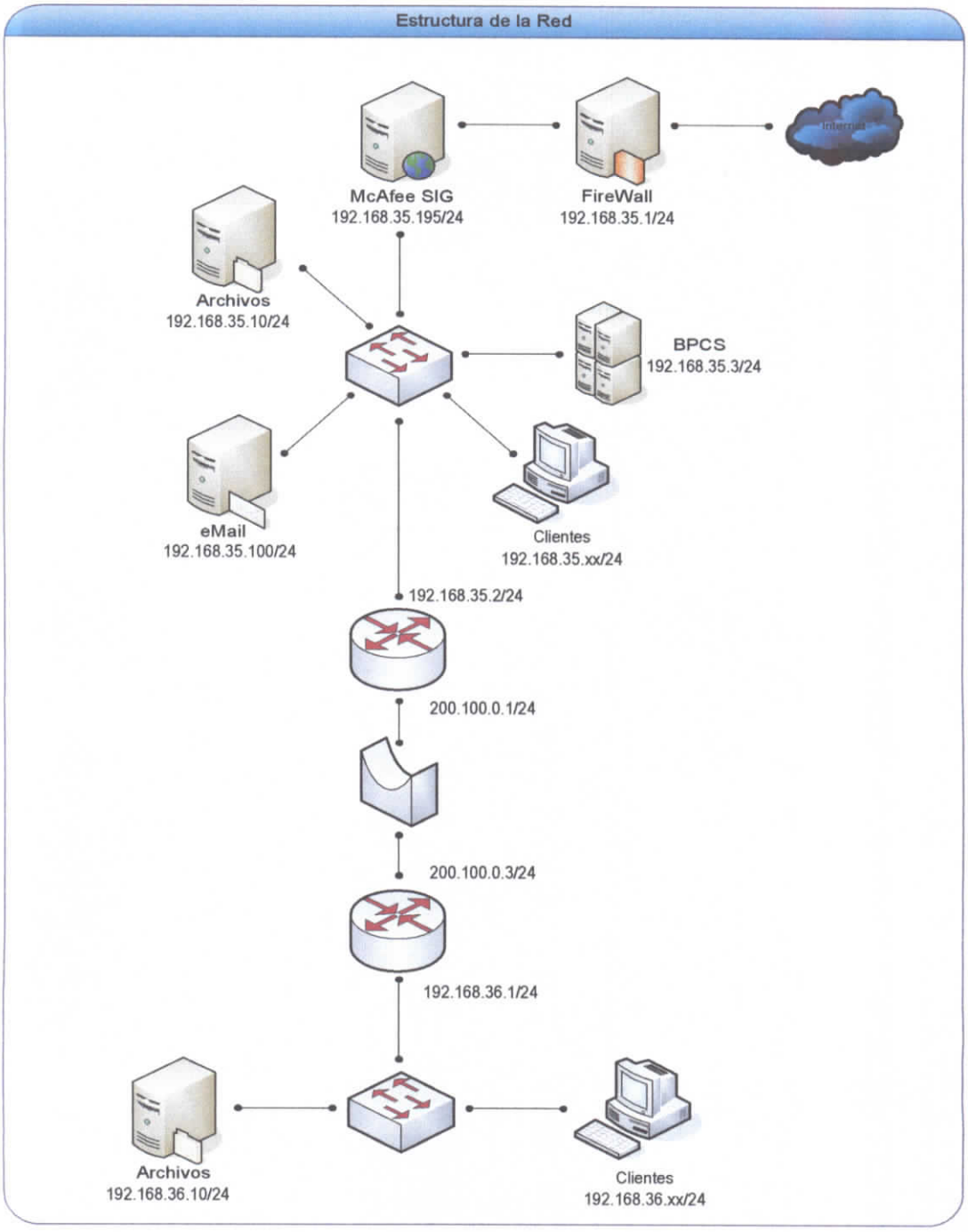


Figura 4.2. Esquema de Red

Look@LAN, cuando se realiza una captura del protocolo SNMP, presenta una ficha similar a la que se observa en la Figura 4.3. La ficha que presenta el SNMP se observa en la figura 4.3.: Ficha de Información SNMP presentada por Look@LAN.

A continuación se presentan las configuraciones de todos los elementos de red que intervienen la las comunicaciones de la organización, en los que no se dispone de monitoreo SNMP, se han capturado las pantallas propias de los sistemas de administración de los dispositivos:

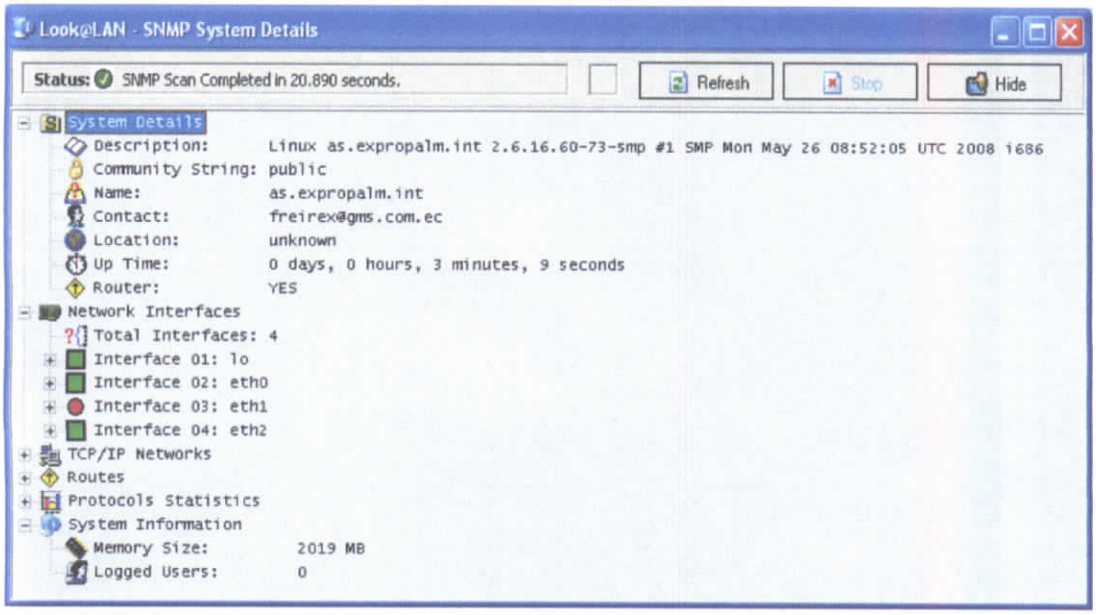
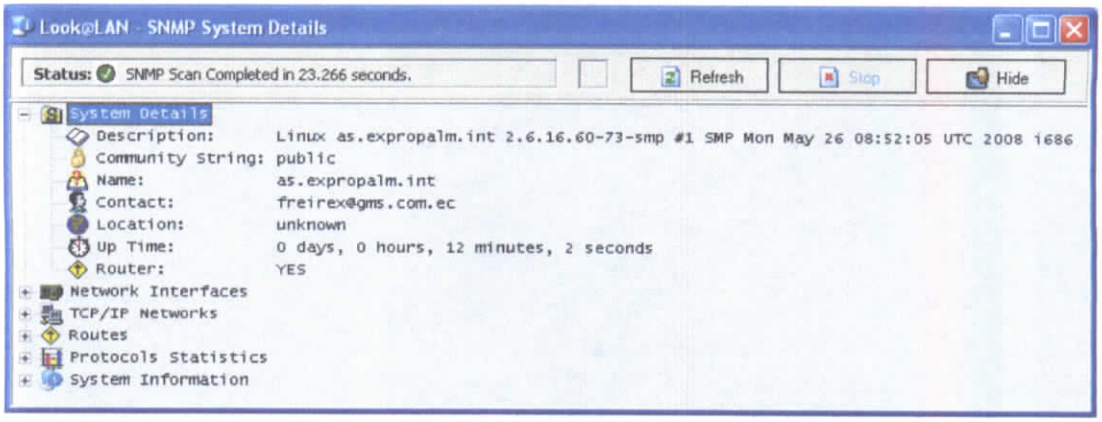


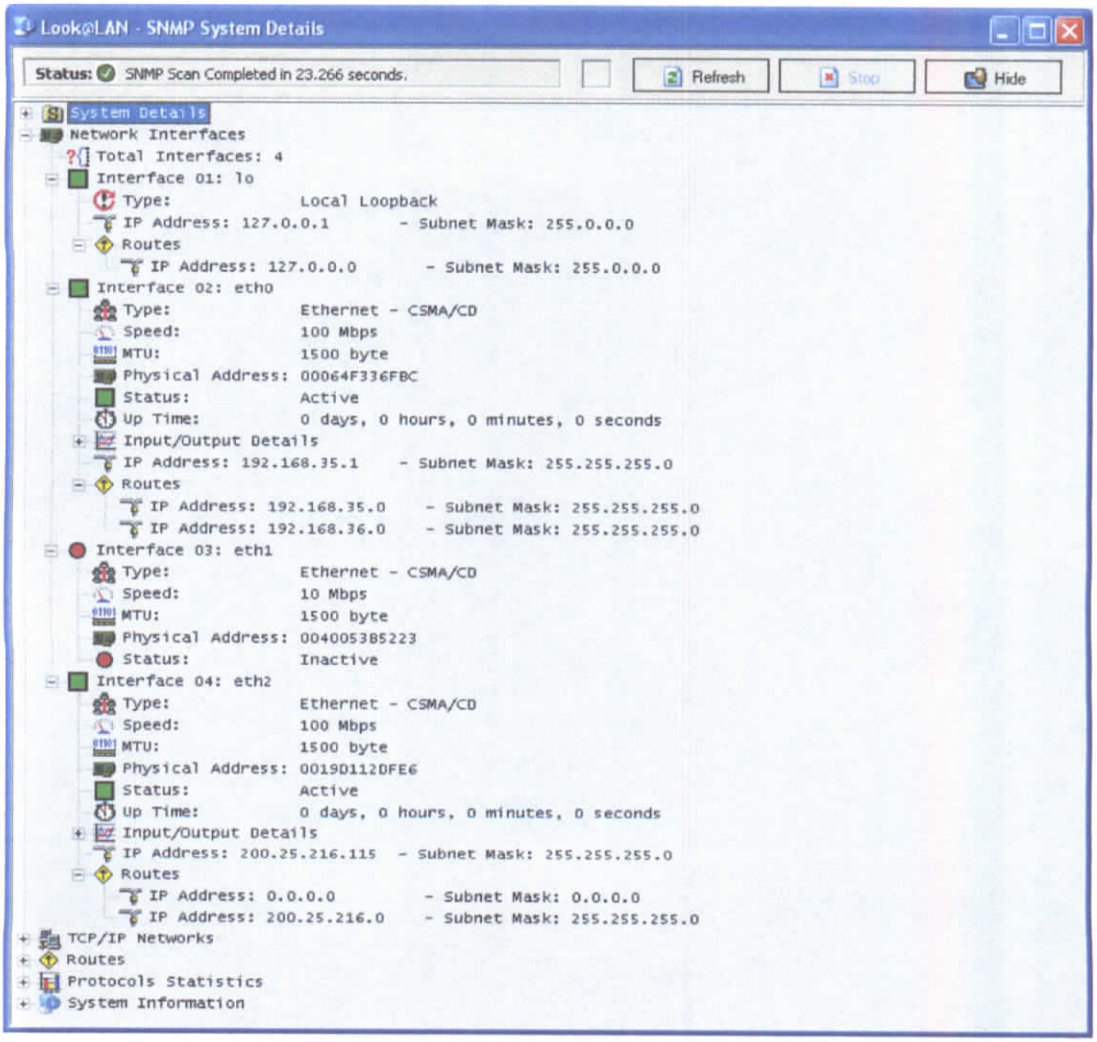
Figura 4.3. Ficha de Información SNMP presentada por Look@LAN

1. **Firewall (192.168.35.1):** La configuración del firewall se muestra a continuación:

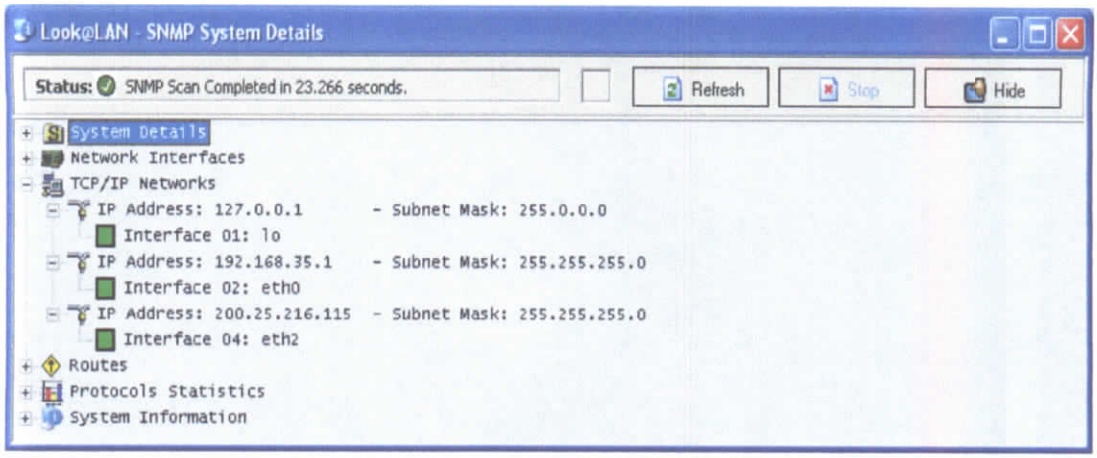
- Detalles del Sistema



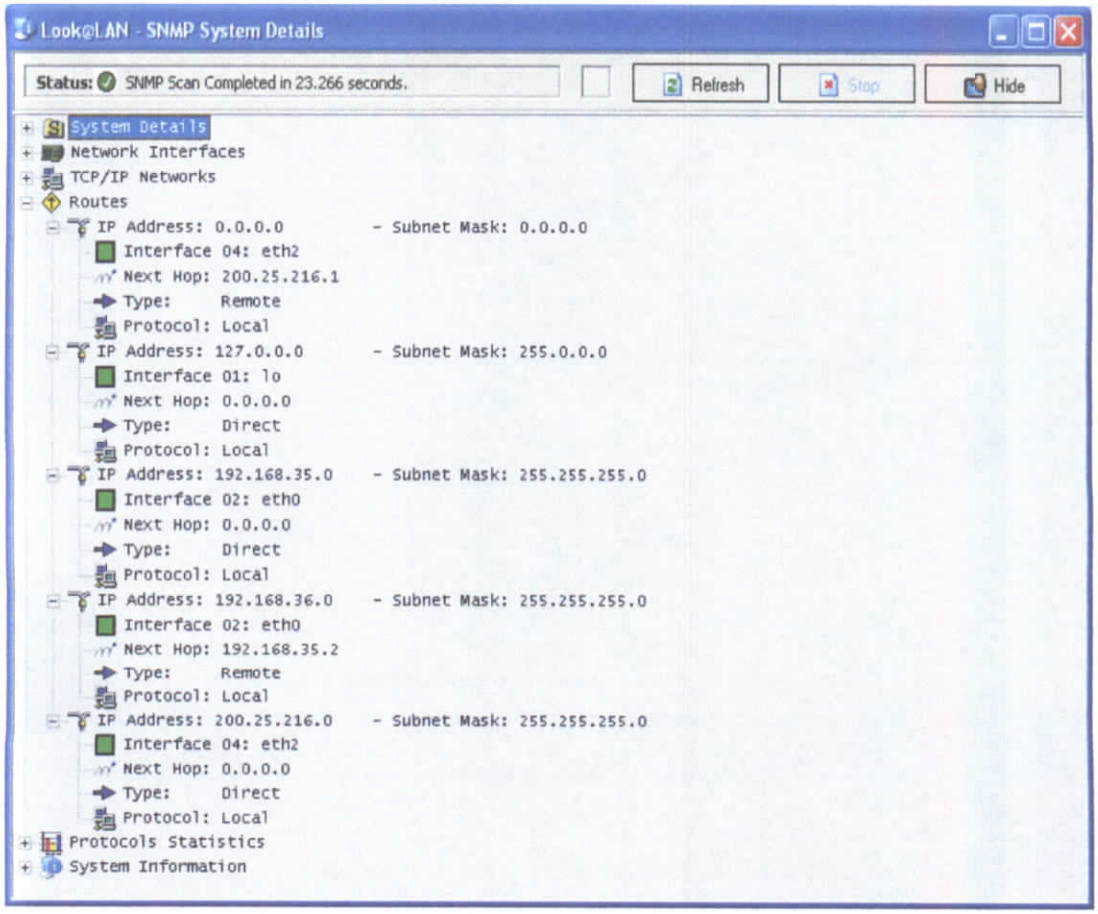
- Interfaces de Red:



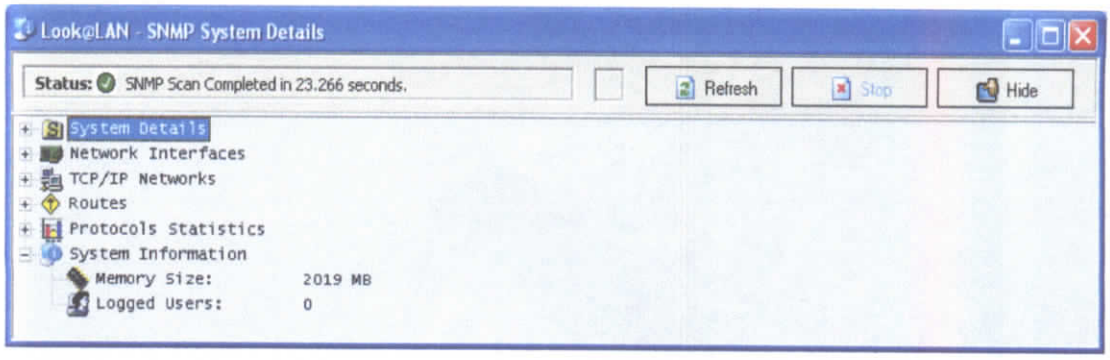
- Redes TCP/IP



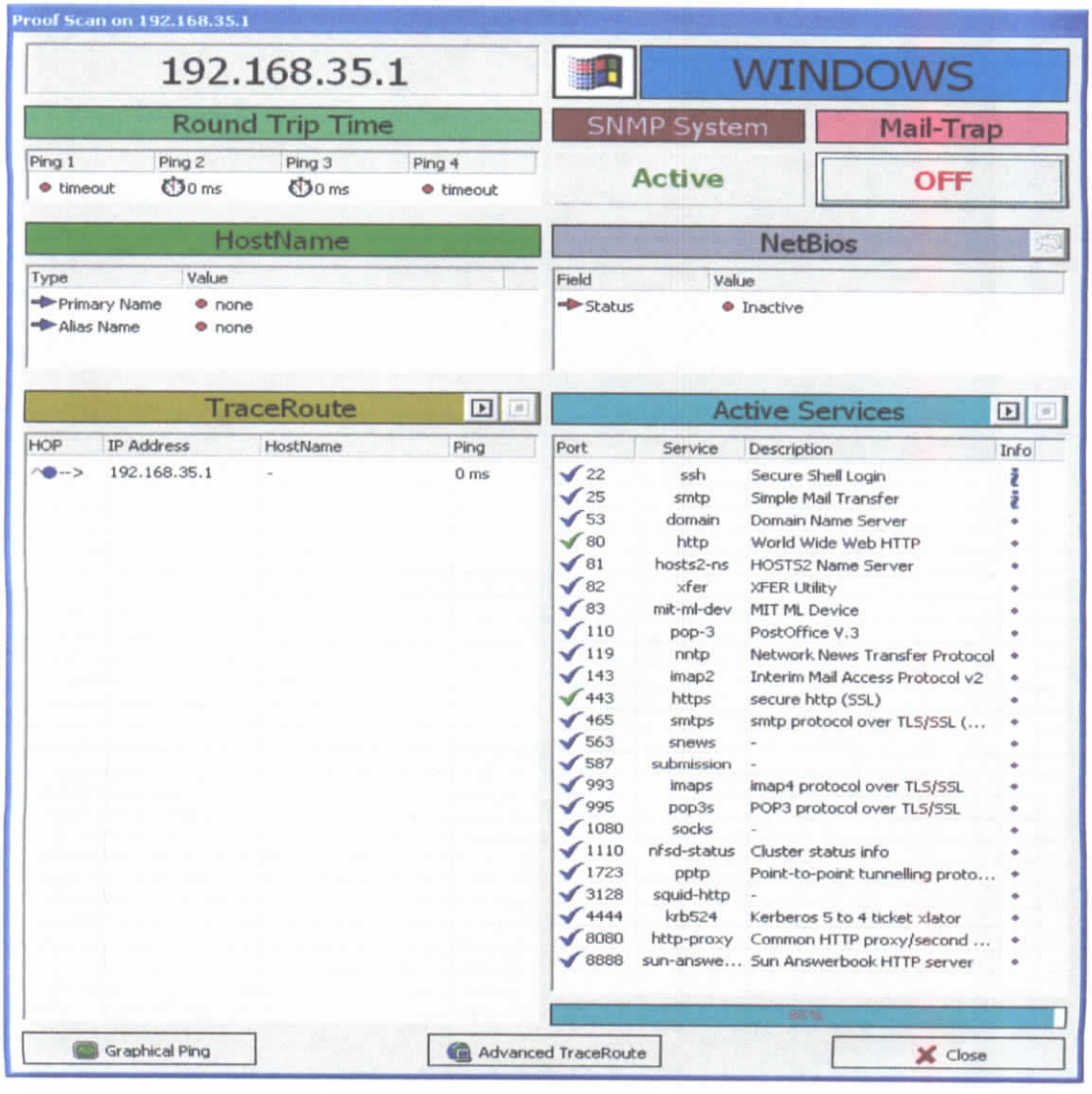
- Rutas:



- Información del Sistema

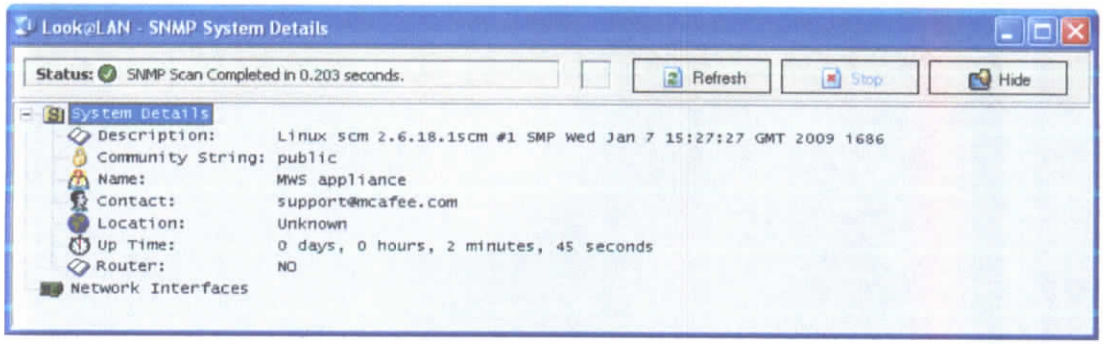


- Servicios Activos

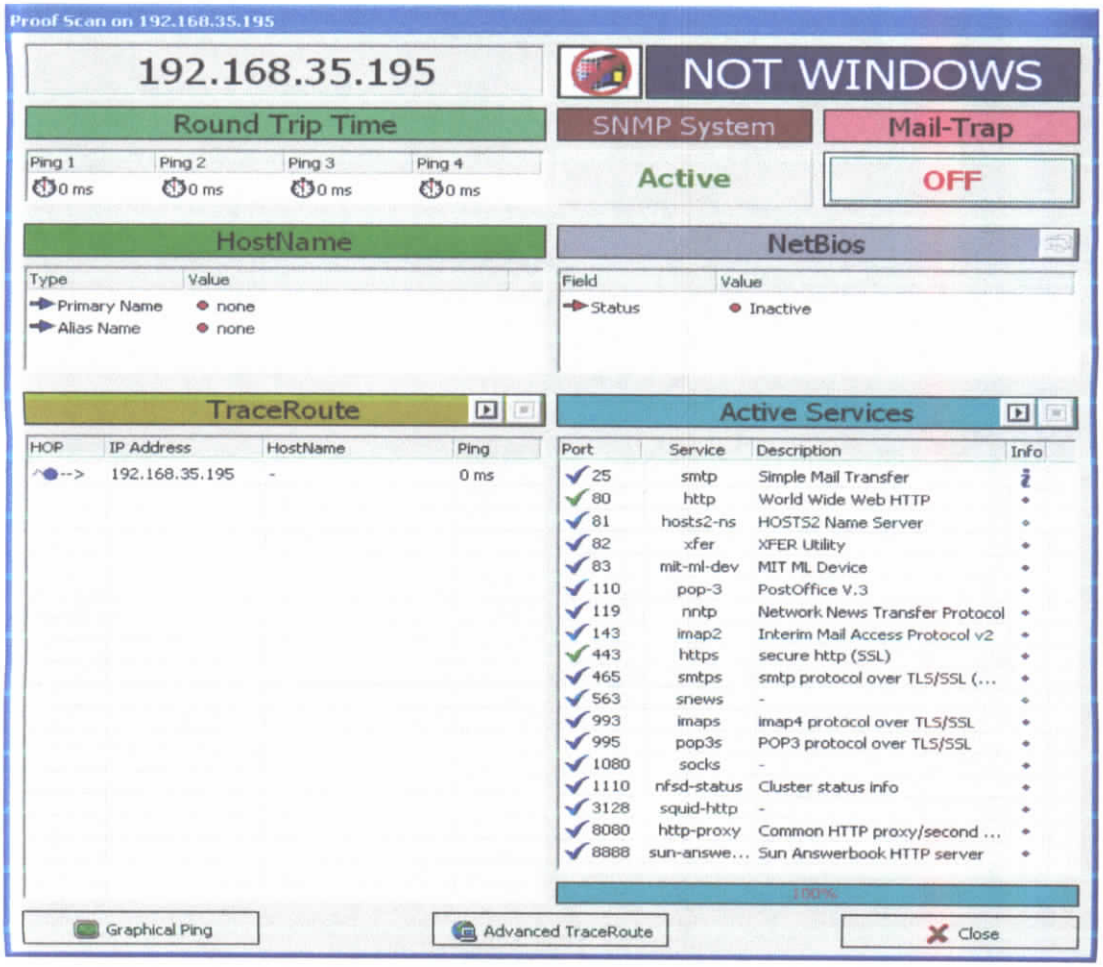


2. **McAfee Secure Internet Gateway (192.168.35.195):** La información del dispositivo de seguridad perimetral se muestra a continuación:

- Detalles del Sistema

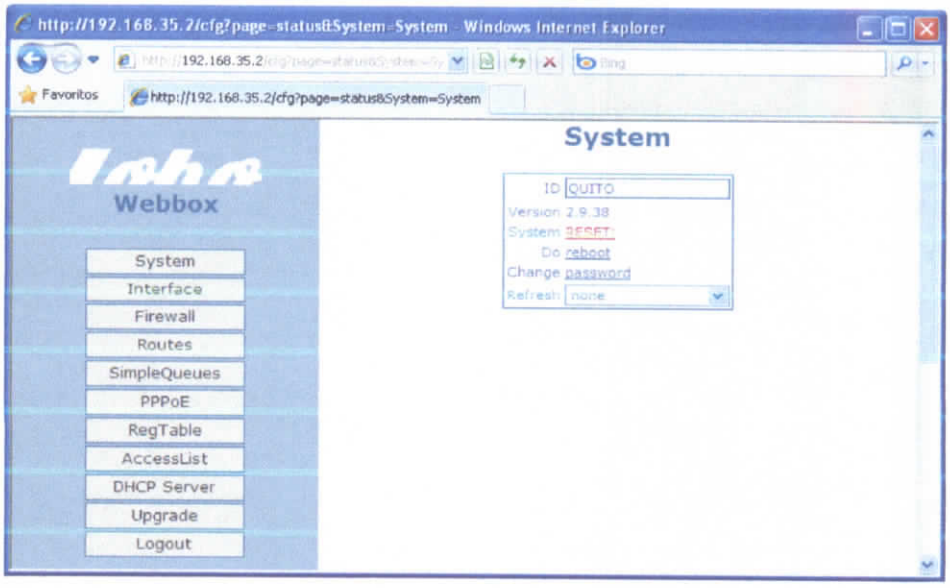


- Servicios Activos

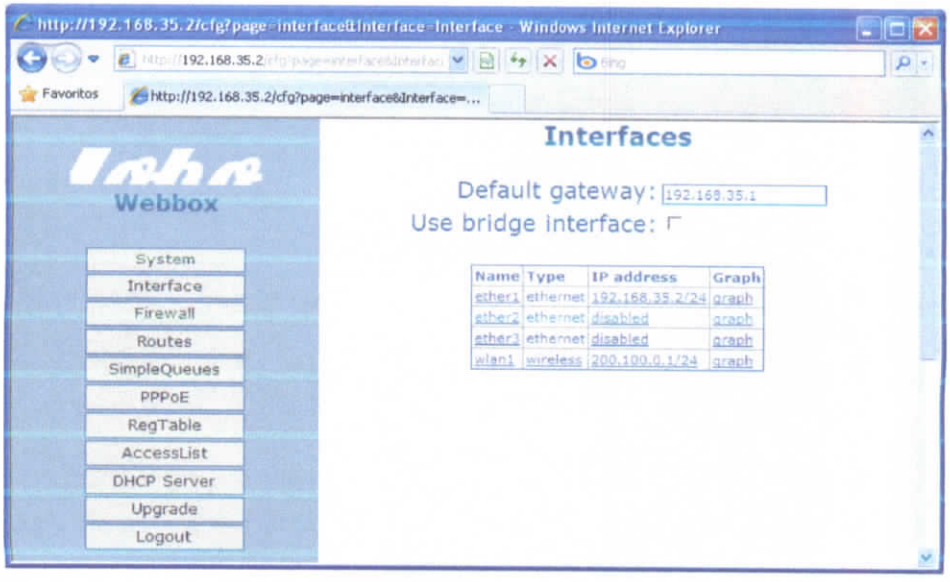


3. **Lobometric 954 (192.168.35.2):** La configuración del Equipo de Comunicaciones Lobometrics, que realiza las funciones de radio enlace y tiene incorporadas funciones de ruteo se muestran en las pantallas obtenidas del sistema de configuración del Equipo:

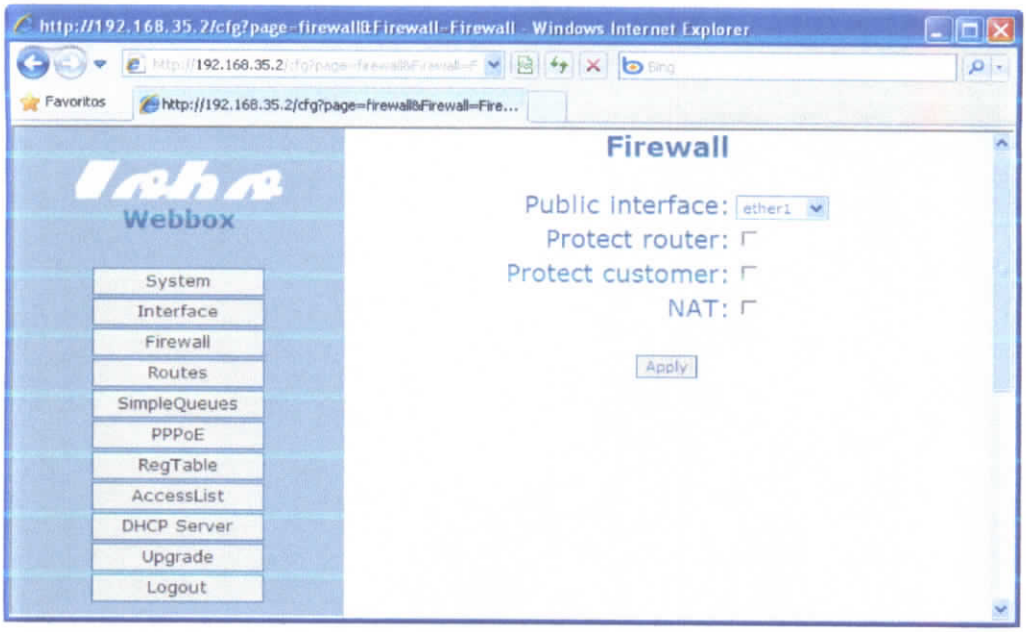
- Información del Sistema:



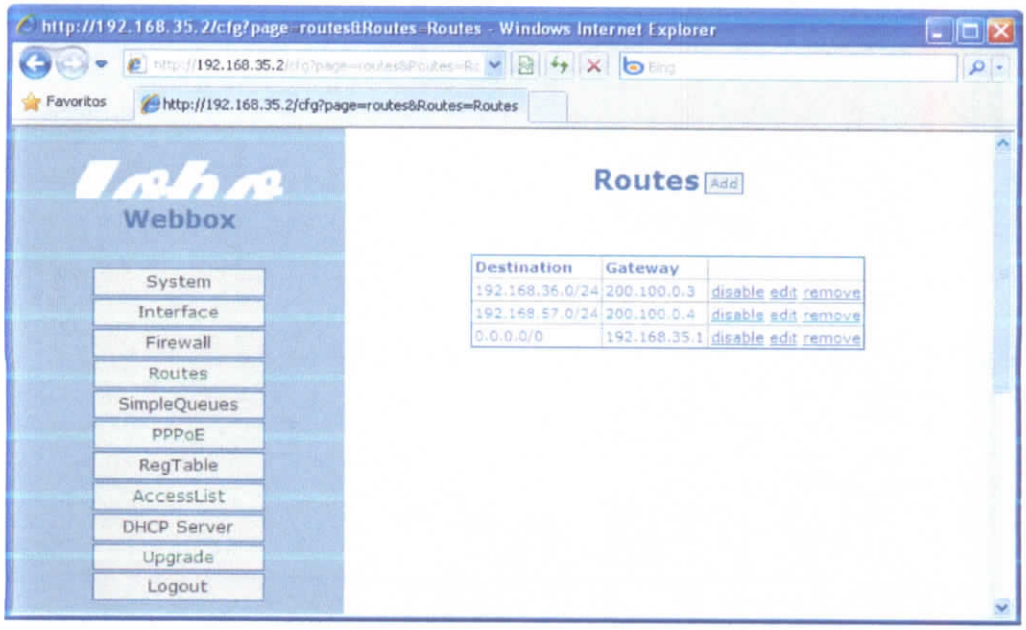
- Interfaces



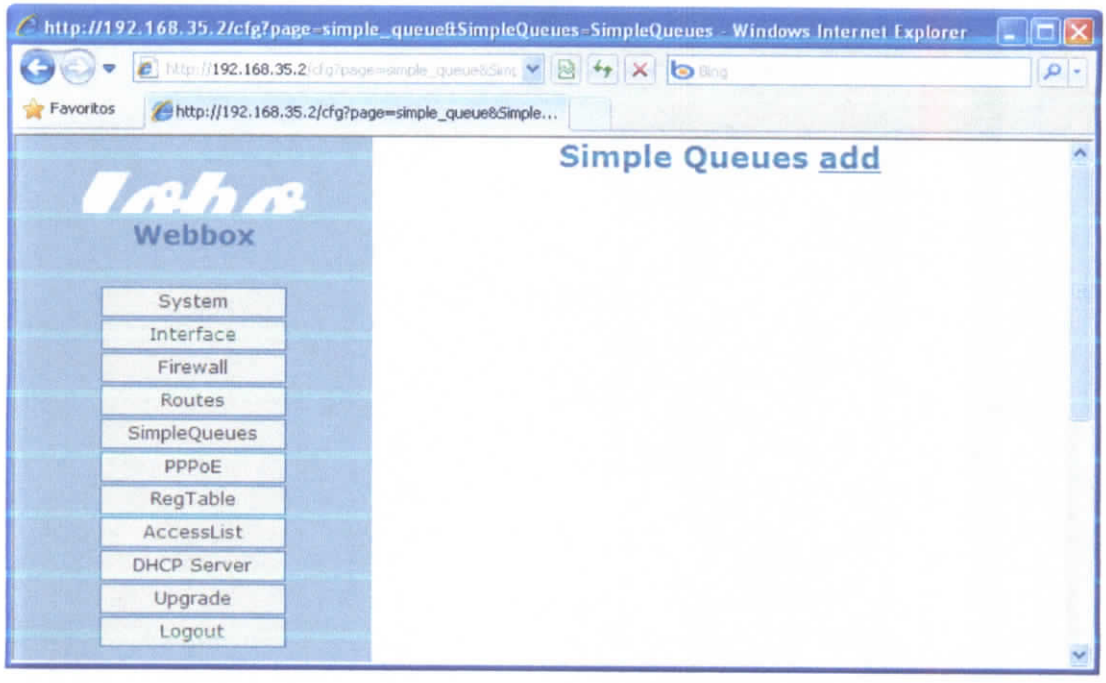
- Firewall del Equipo



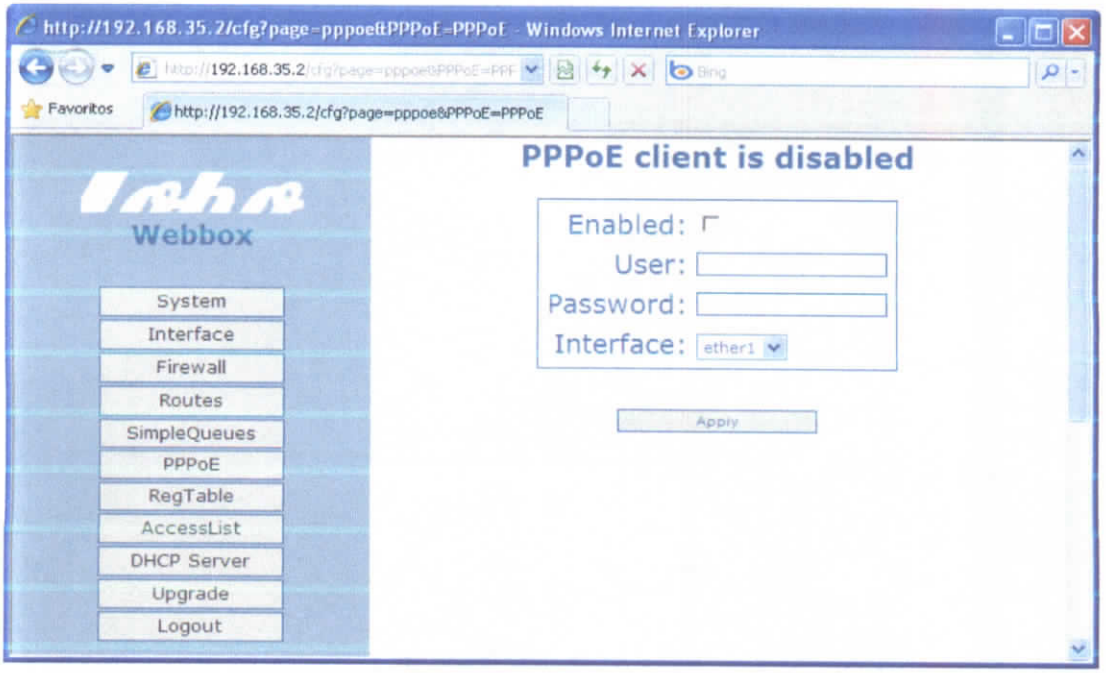
- Rutas



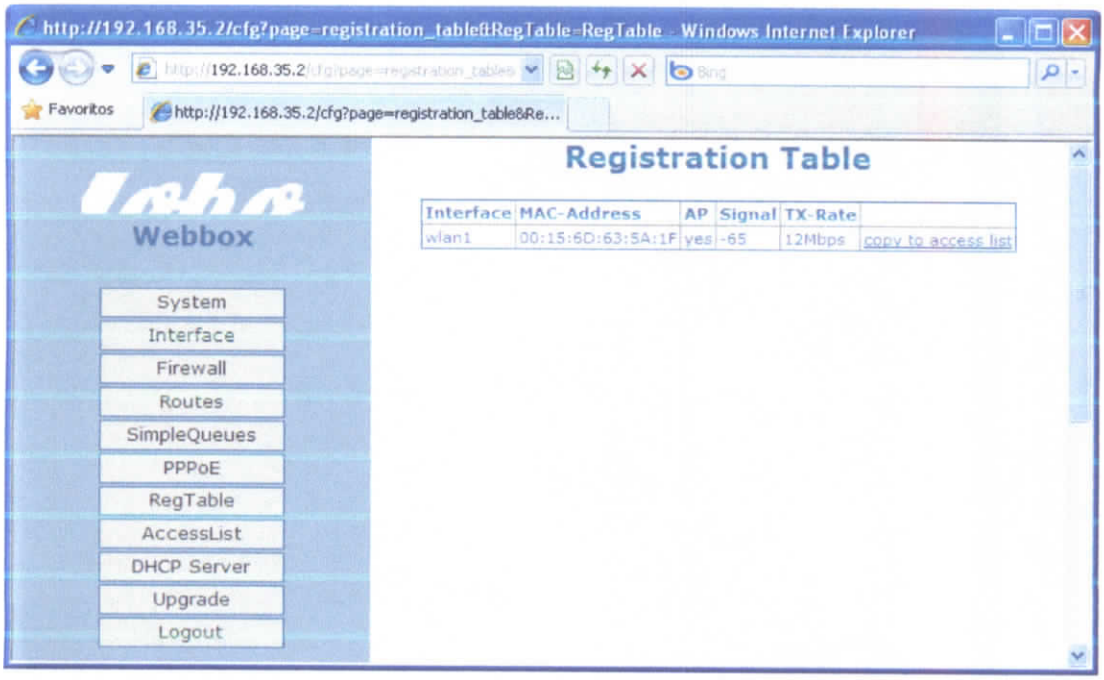
- Colas Simples:



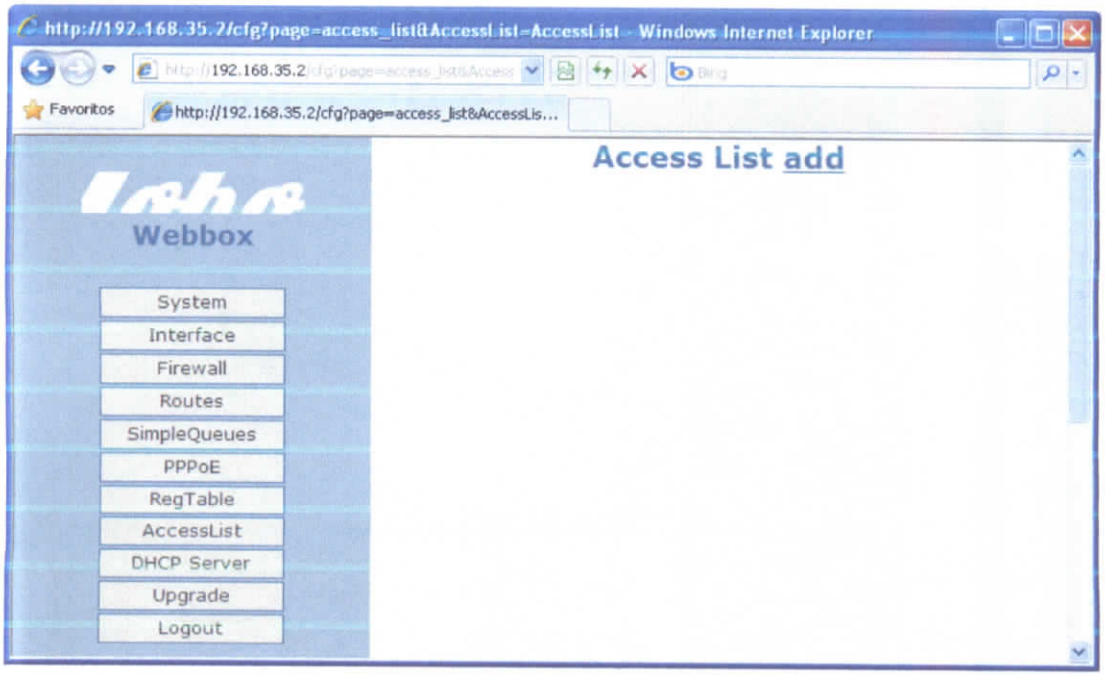
- Cliente PPPoE



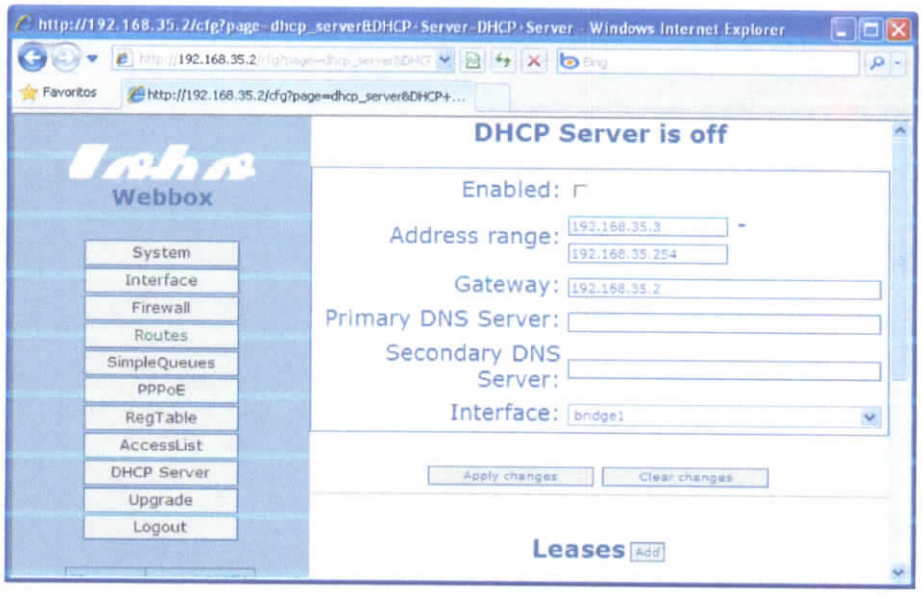
- Tabla de Registro



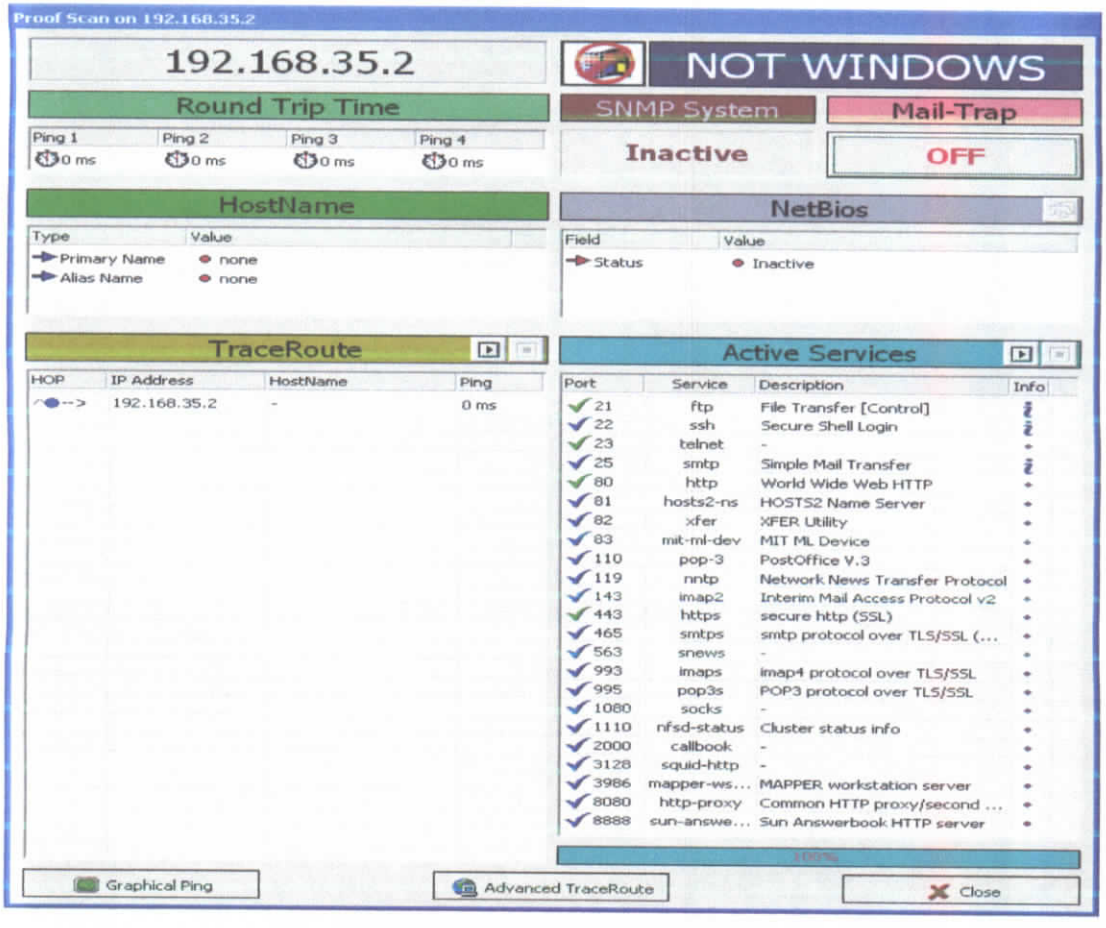
- Lista de Acceso



- Servidor DHCP Incorporado

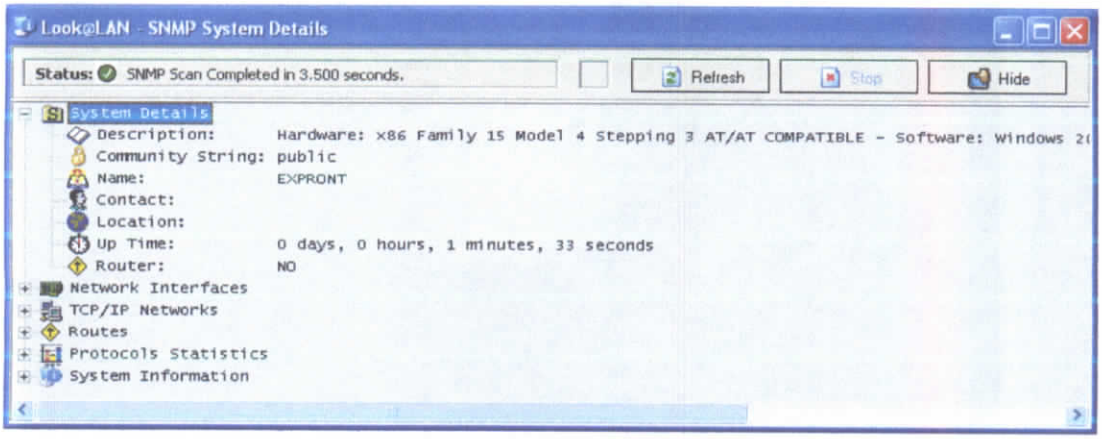


- Lista de Servicios

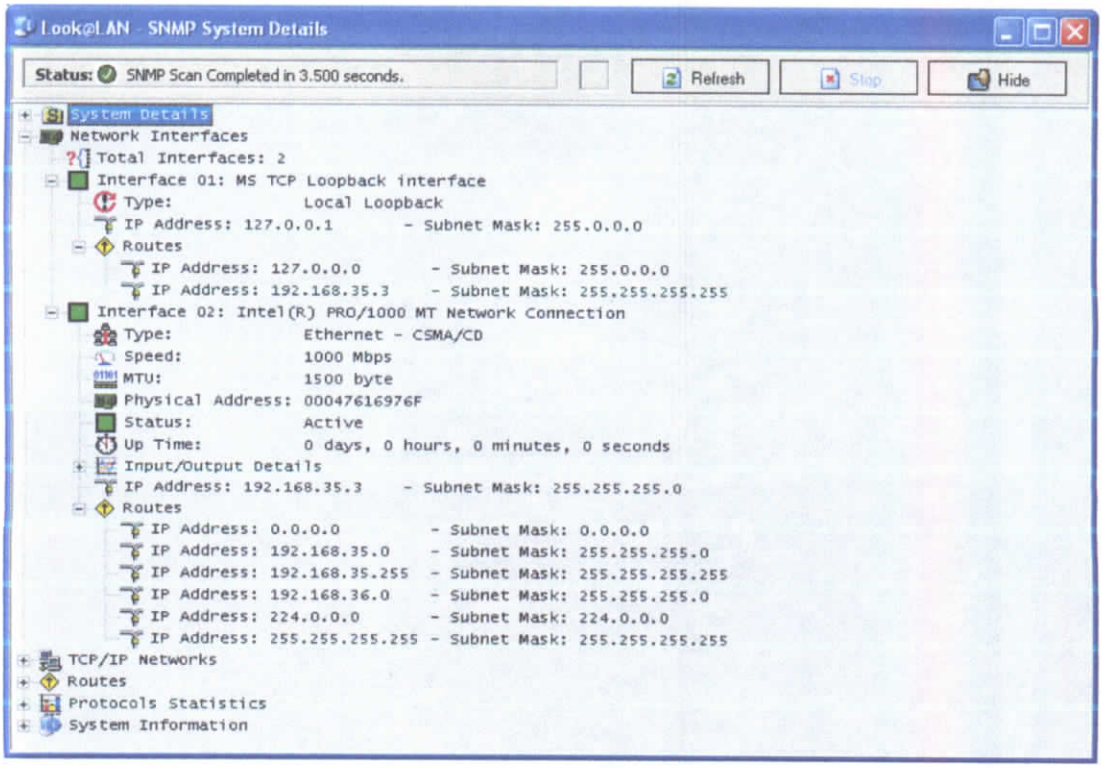


4. **BPSC (192.168.35.3):** La configuración del Servidor BPCS, se muestra a continuación:

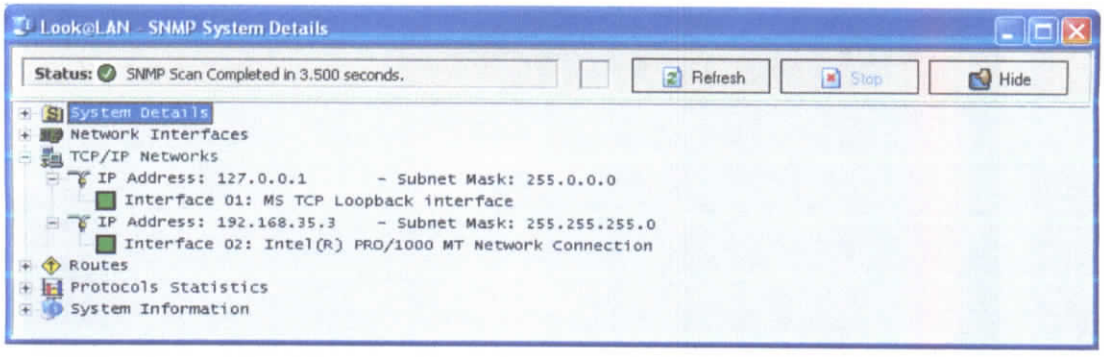
- Detalles del Sistema



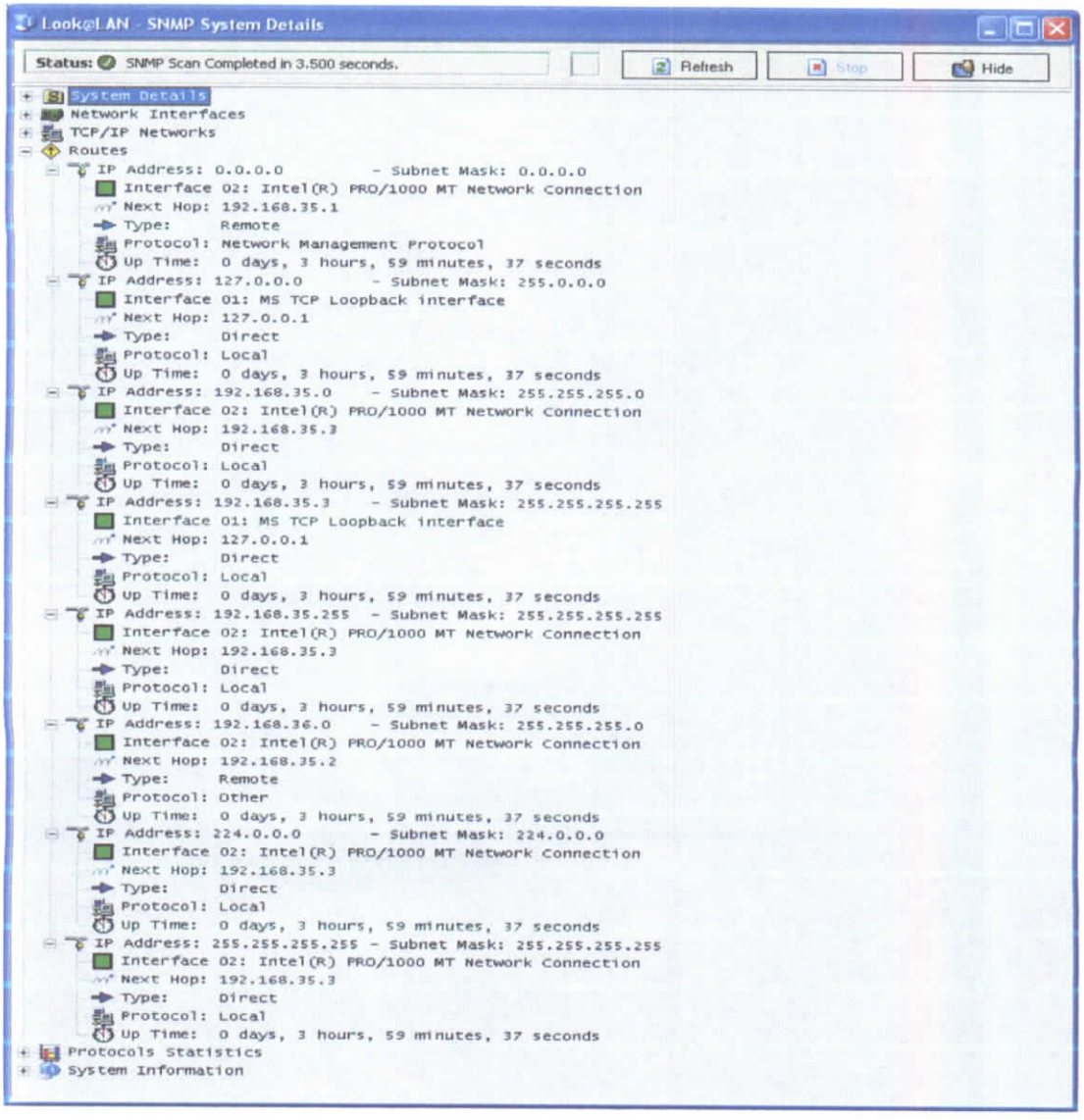
- Interfaces de Red



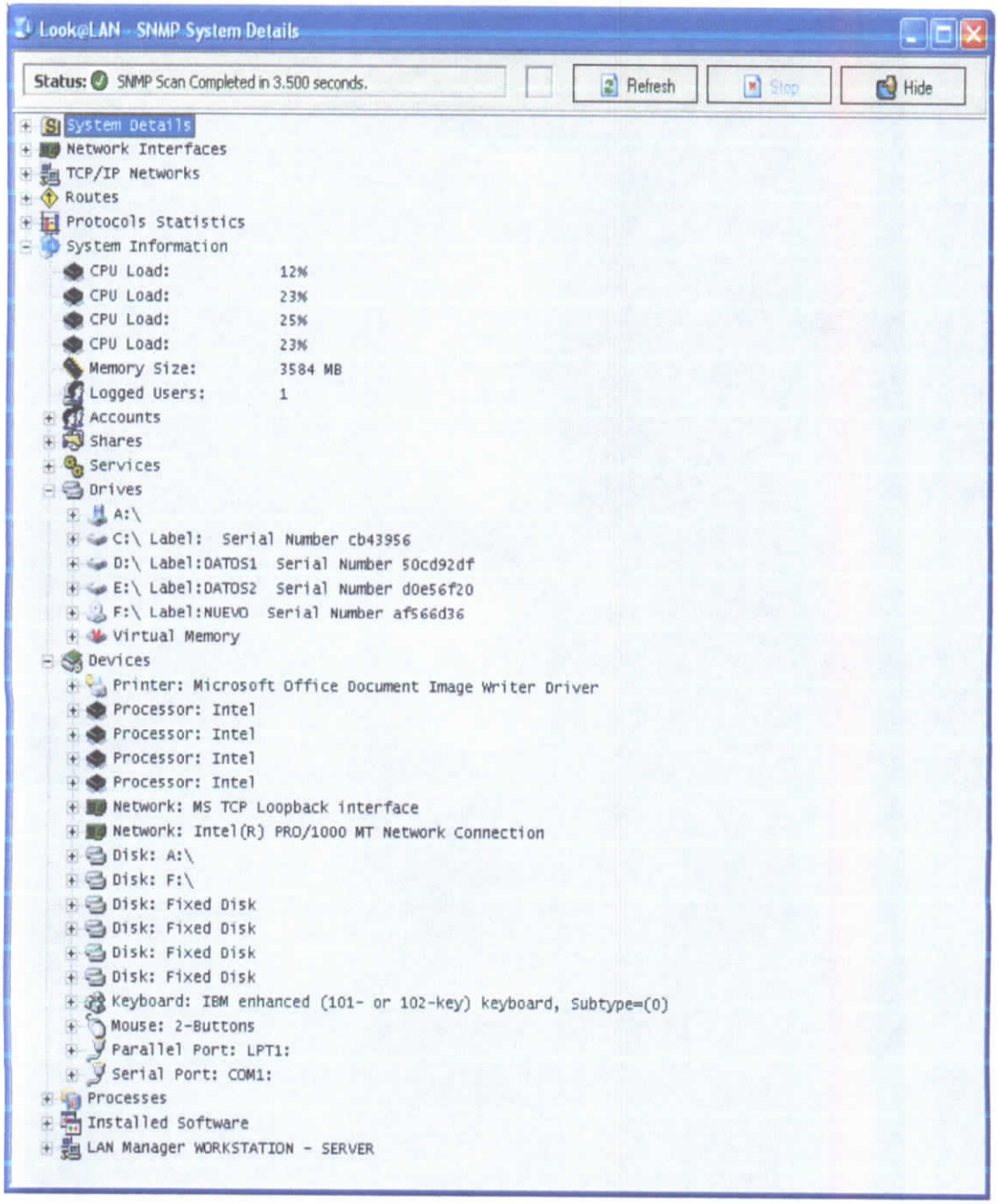
- Redes TCP/IP



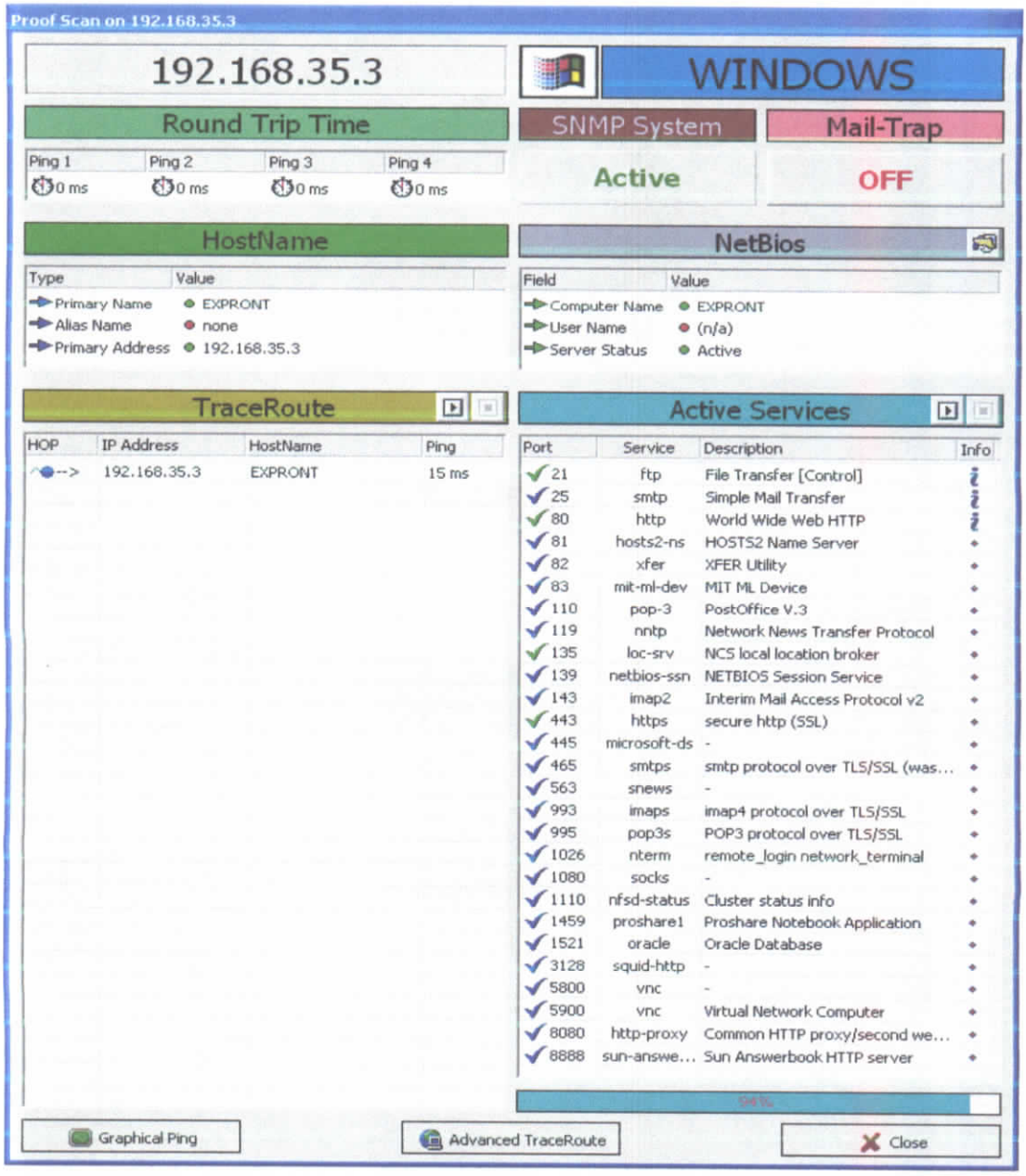
- Rutas



- Información del Sistema

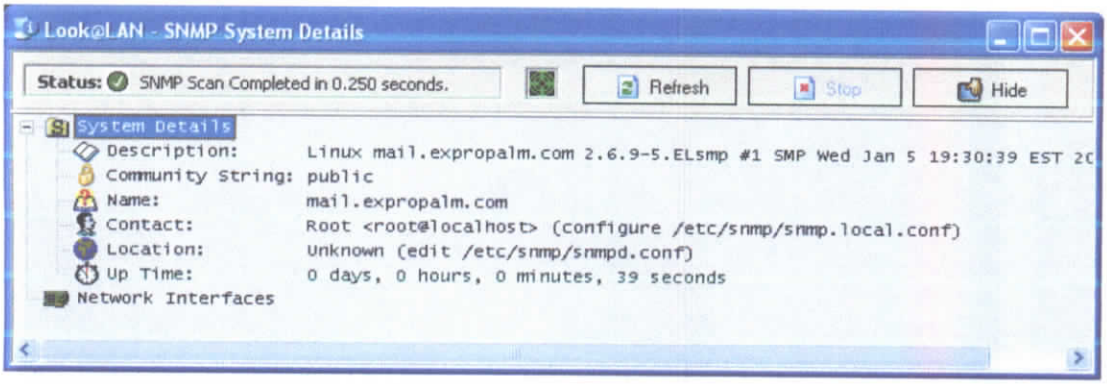


- Servicios Activos

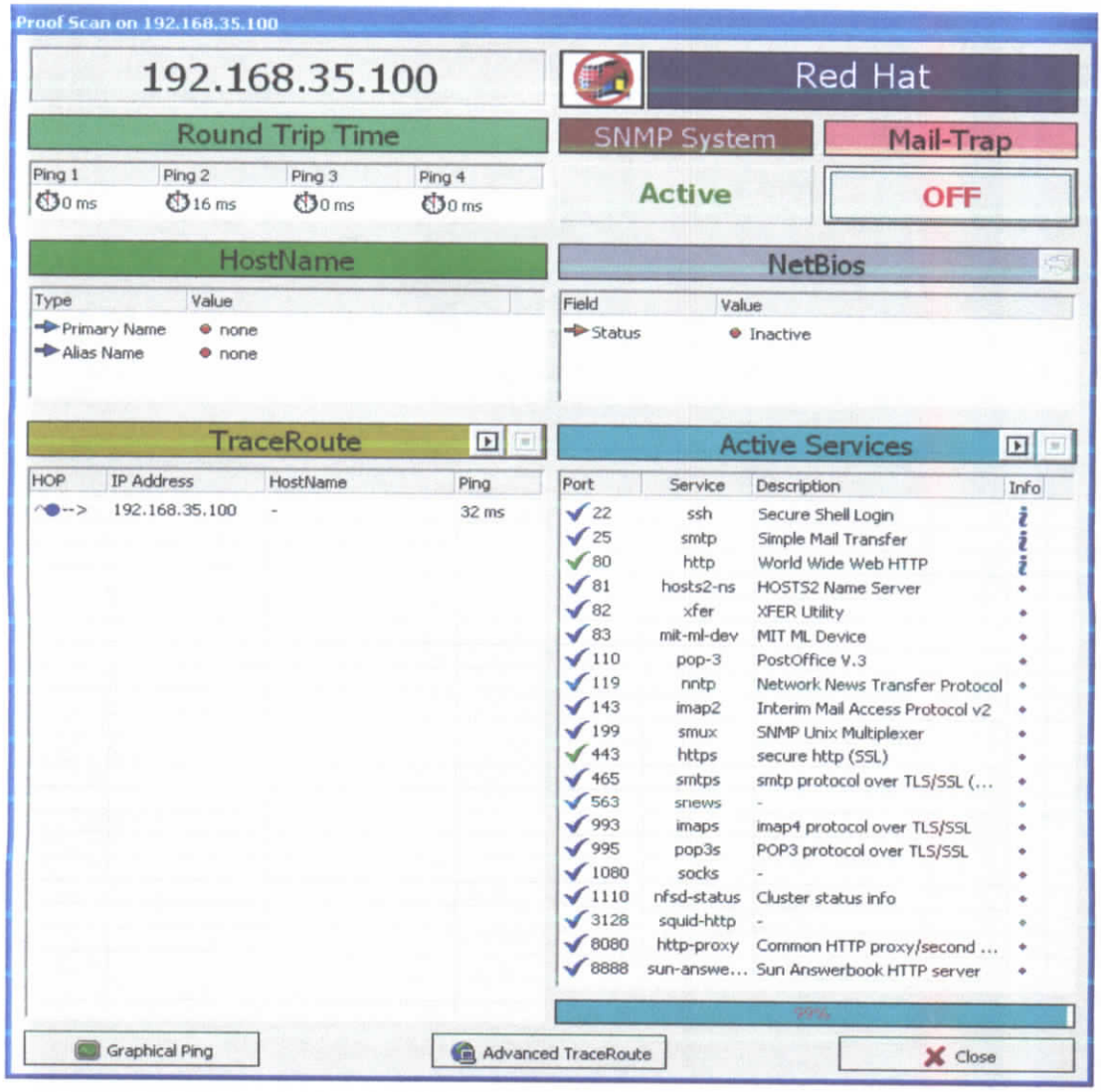


5. **Mail Server (192.168.35.100):** A continuación se presenta la configuración del Servidor de Correo Electrónico:

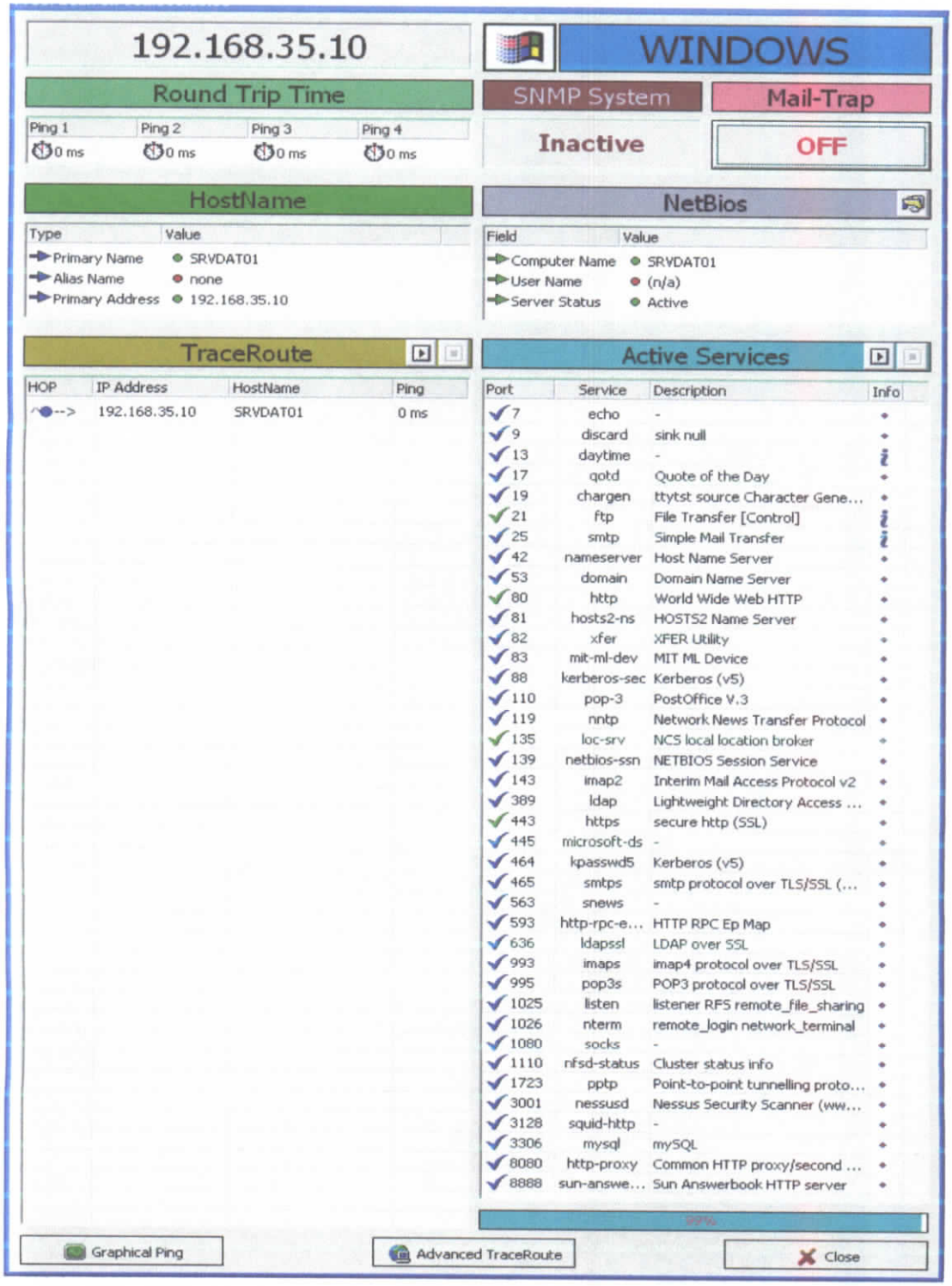
- Detalles del Sistema



- Servicios Activos



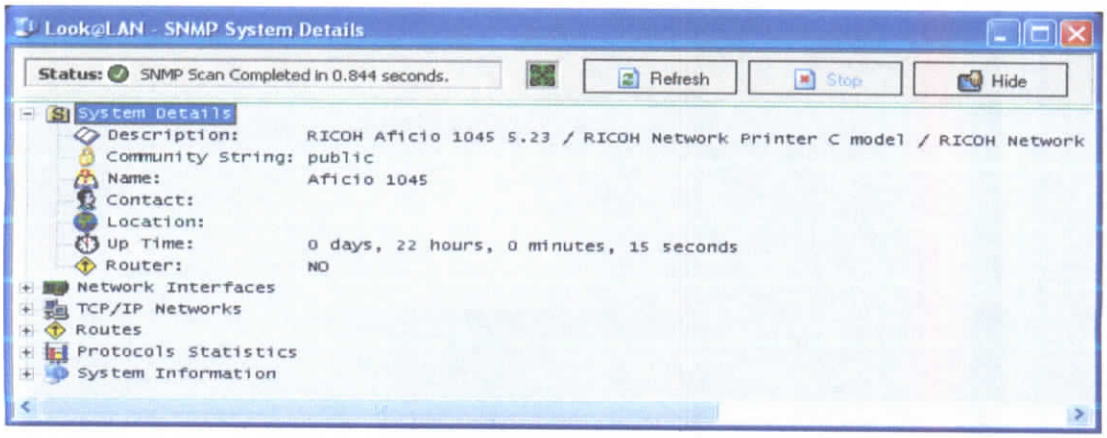
6. **Archivos (192.168.35.10):** Se presenta únicamente Servicios Activos Debido a la imposibilidad de Activar el Protocolo SNMP:



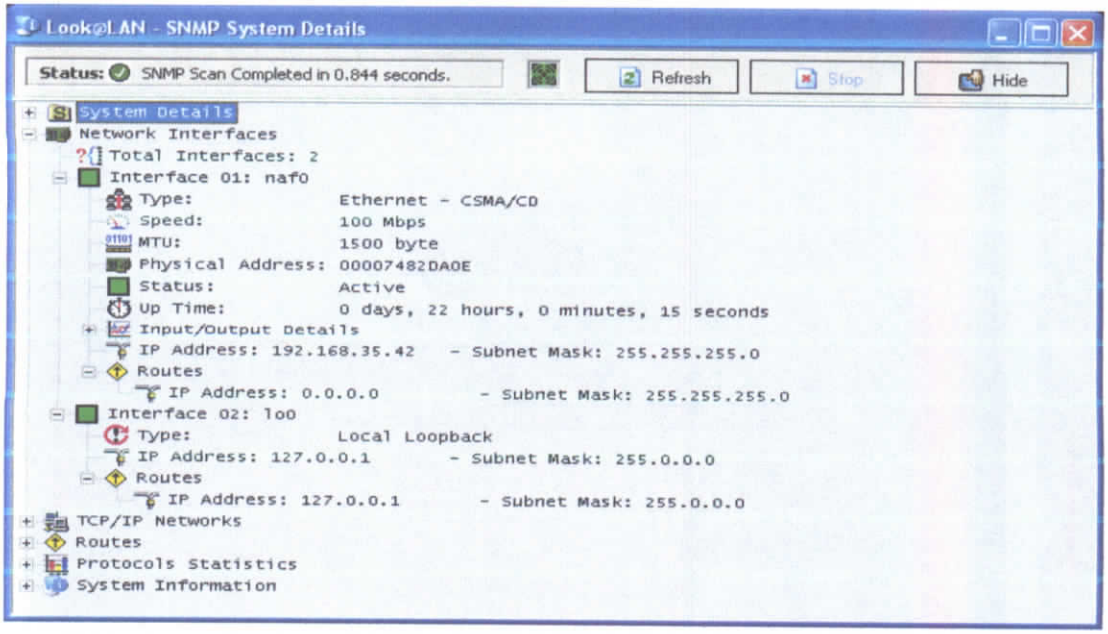
7. **Otros Dispositivos:** Se presenta a continuación la configuración de otros dispositivos, que sin ser parte de la infraestructura de comunicaciones atienden a todos los usuarios y demandan recursos del sistema:

- Impresora de Red Aficio (192.168.35.42)

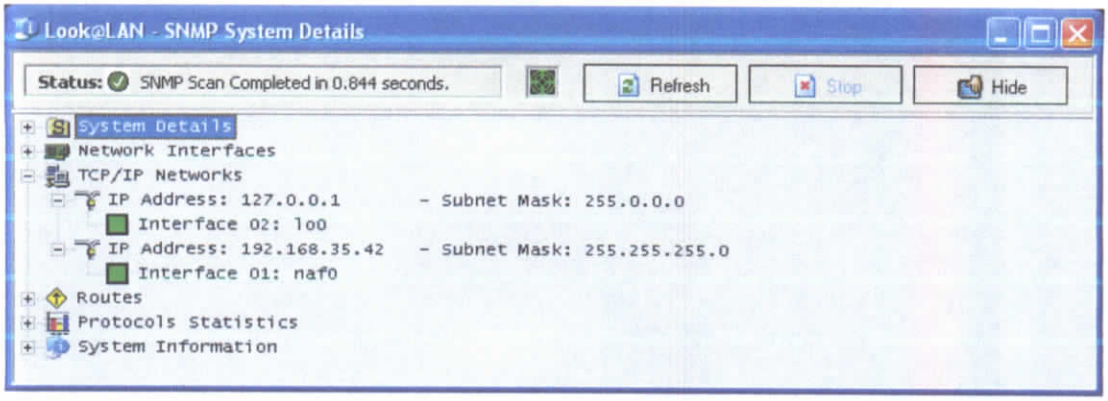
Detalles del Sistema



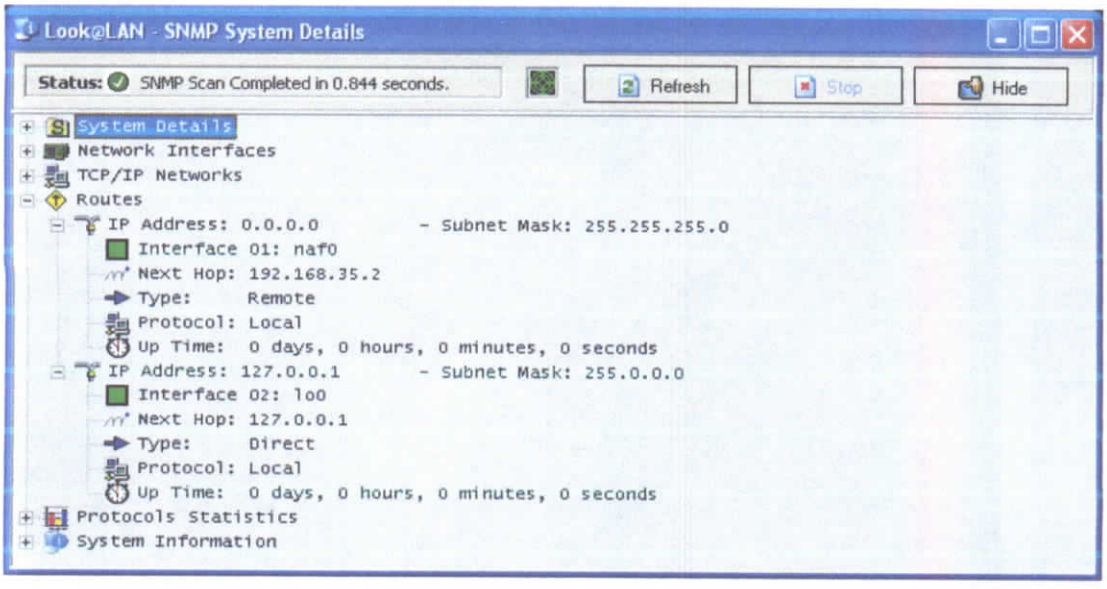
Interfaces de Red



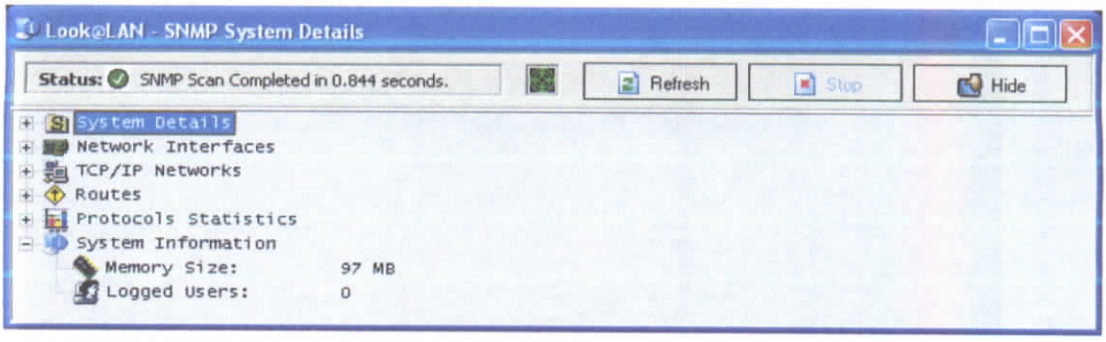
Redes TCP/IP



Rutas:



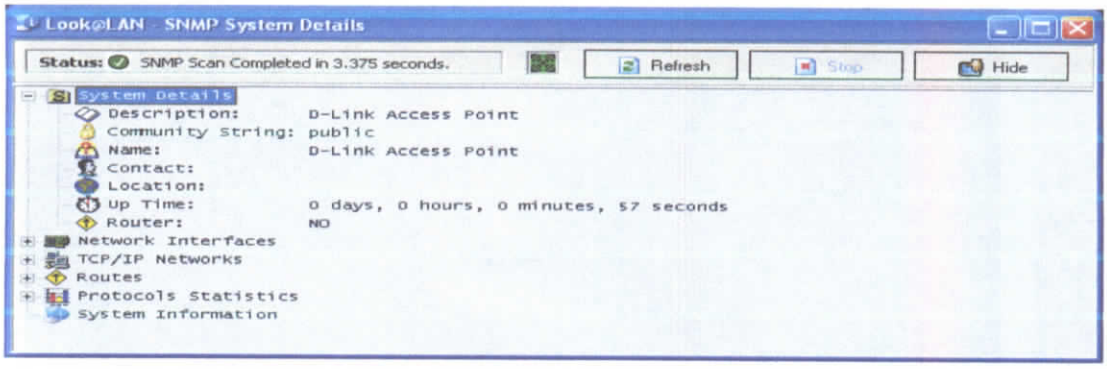
Información del Sistema:



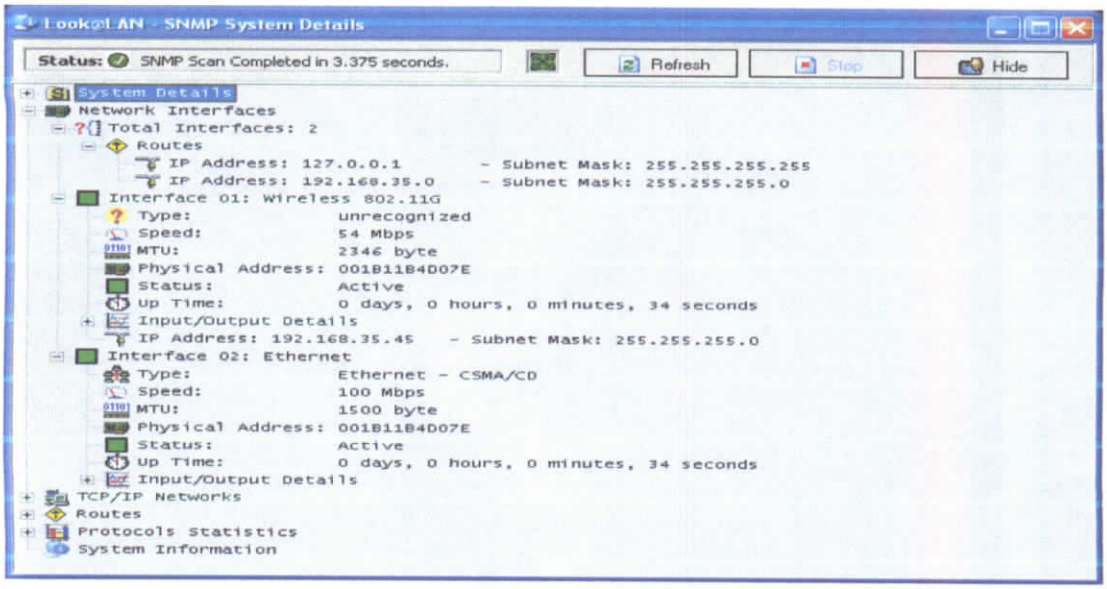
Servicios Activos:

- Wireless Access Point (192.168.35.45)

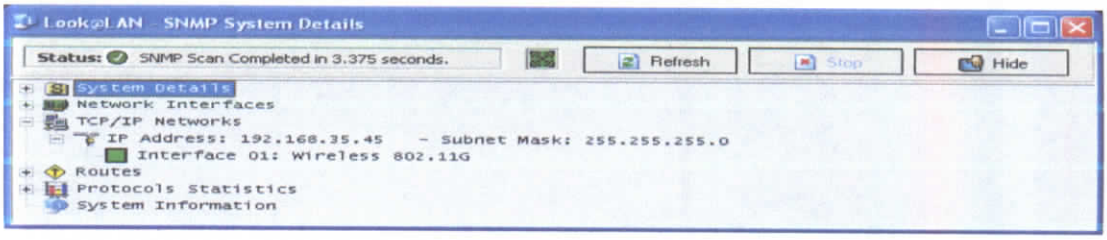
Detalles del Sistema



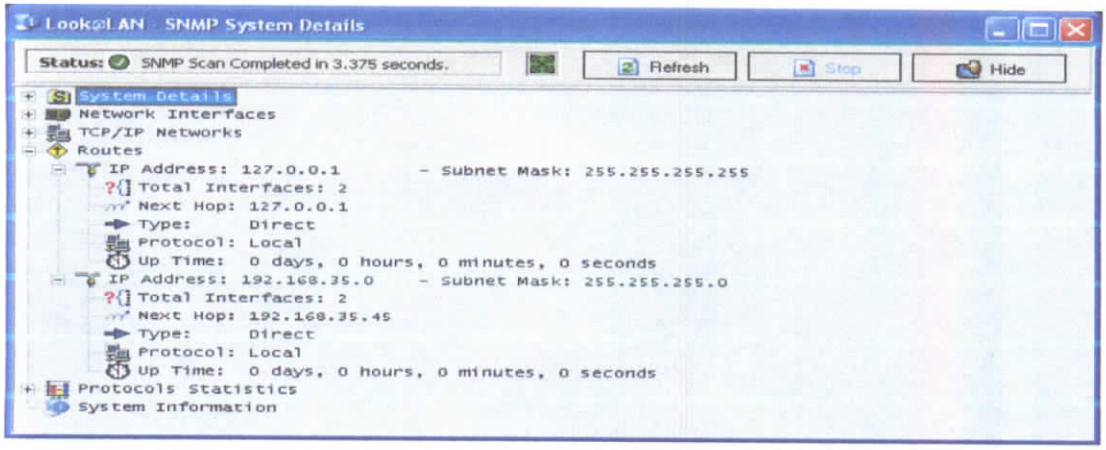
Interfaces de Red



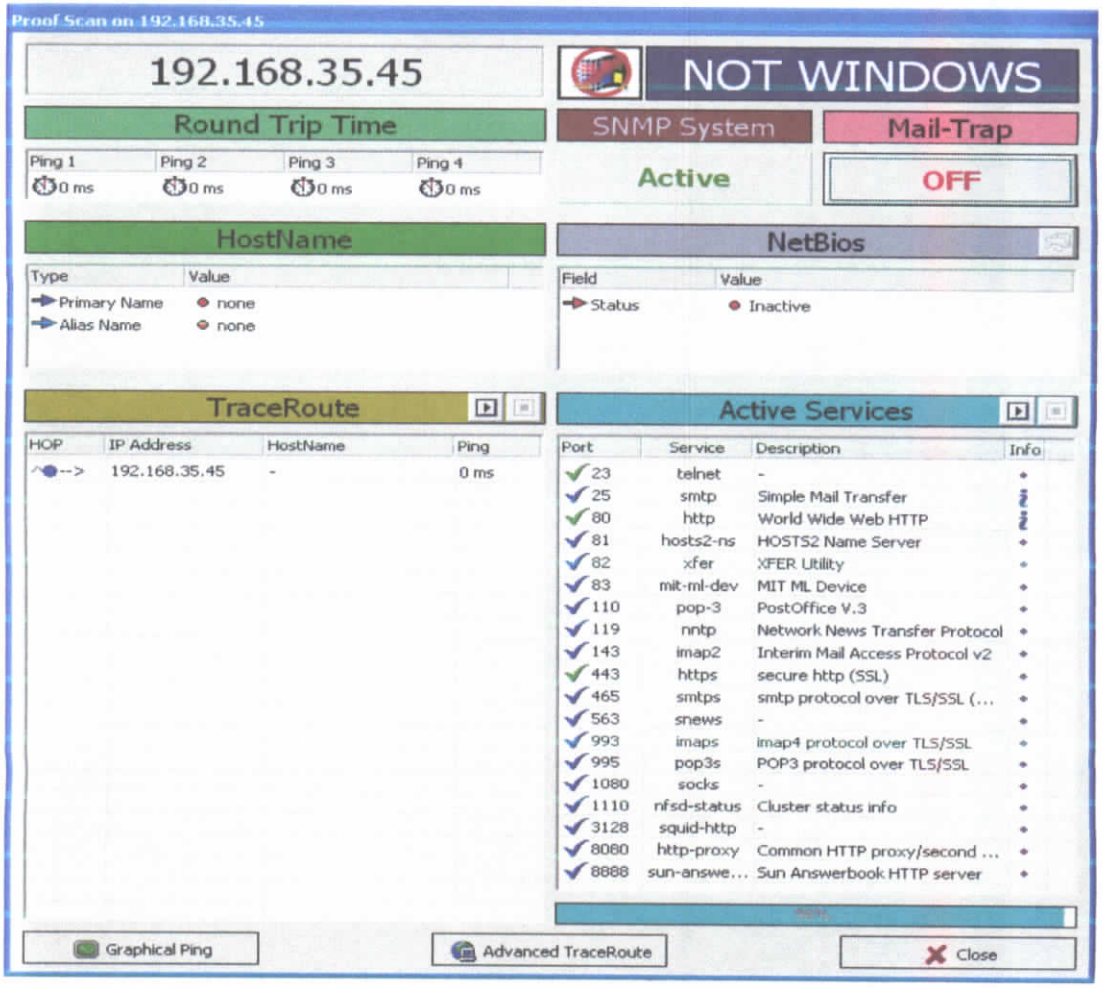
Redes TCP/IP



Rutas

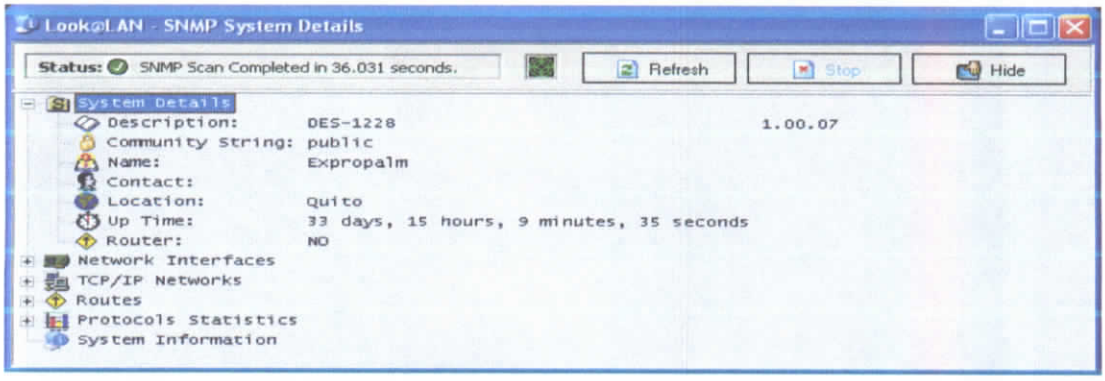


Servicios Activos

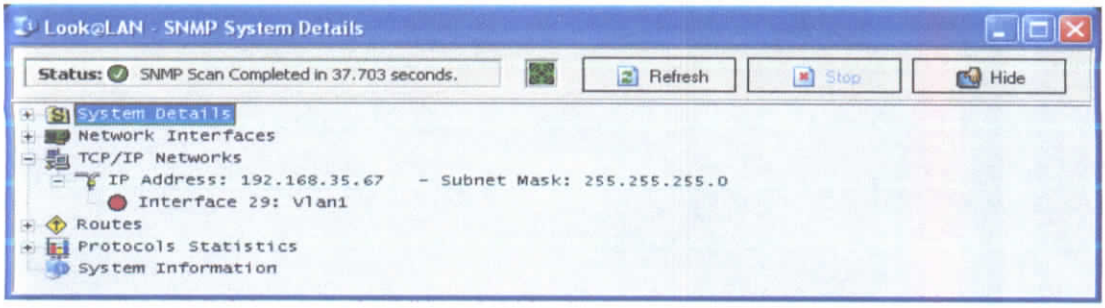


- Switch DLink 1228 (192.168.35.67)

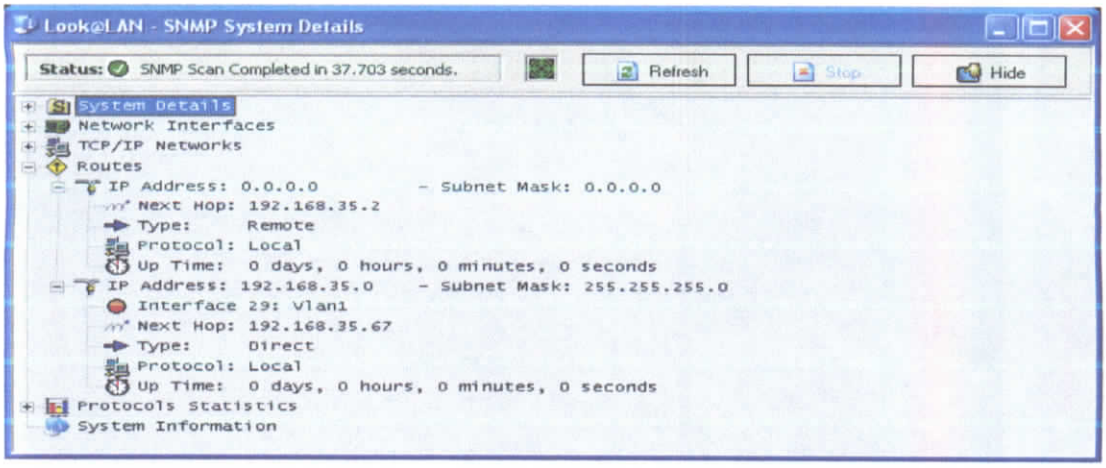
Detalles del Sistema



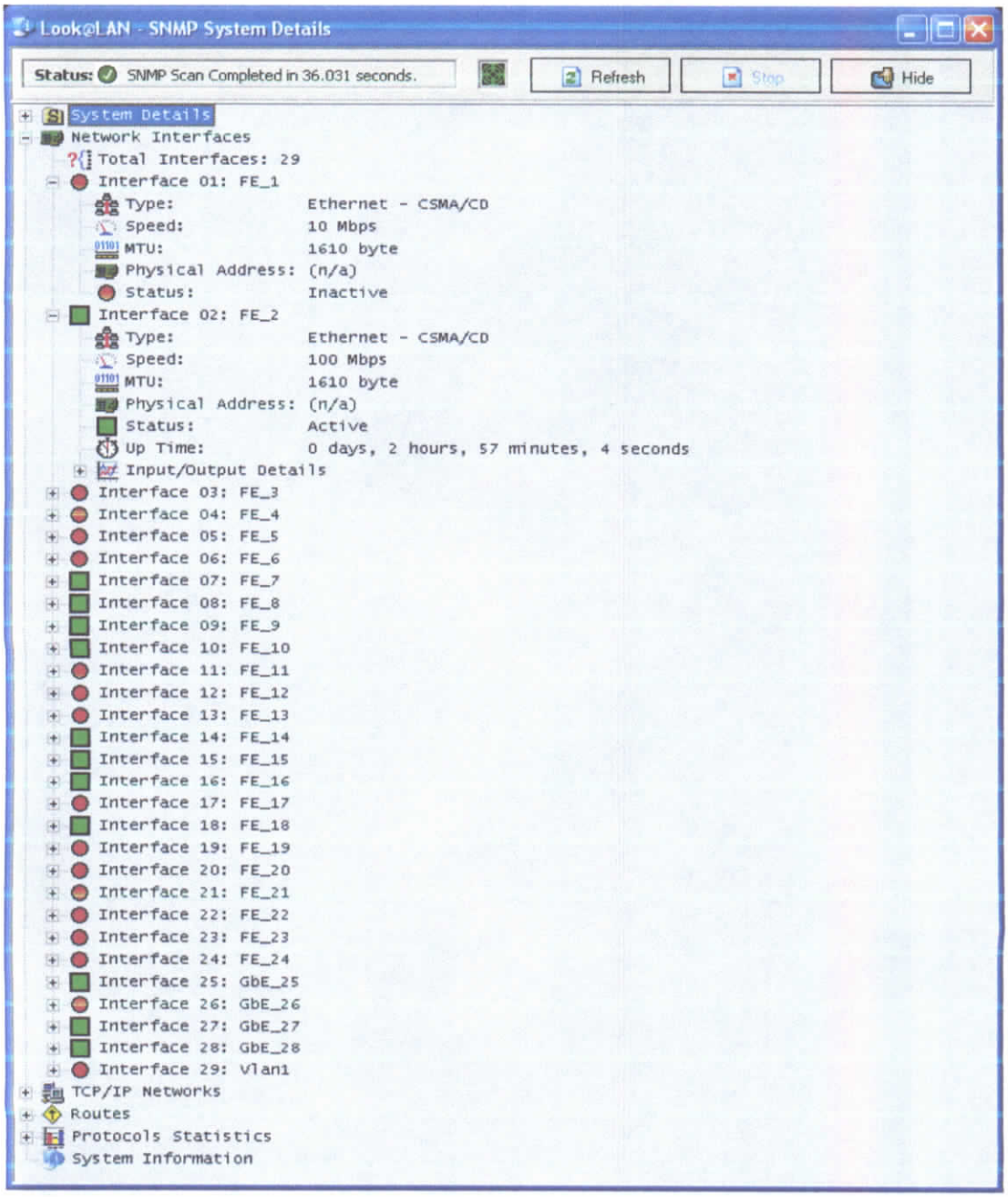
Redes TCP/IP



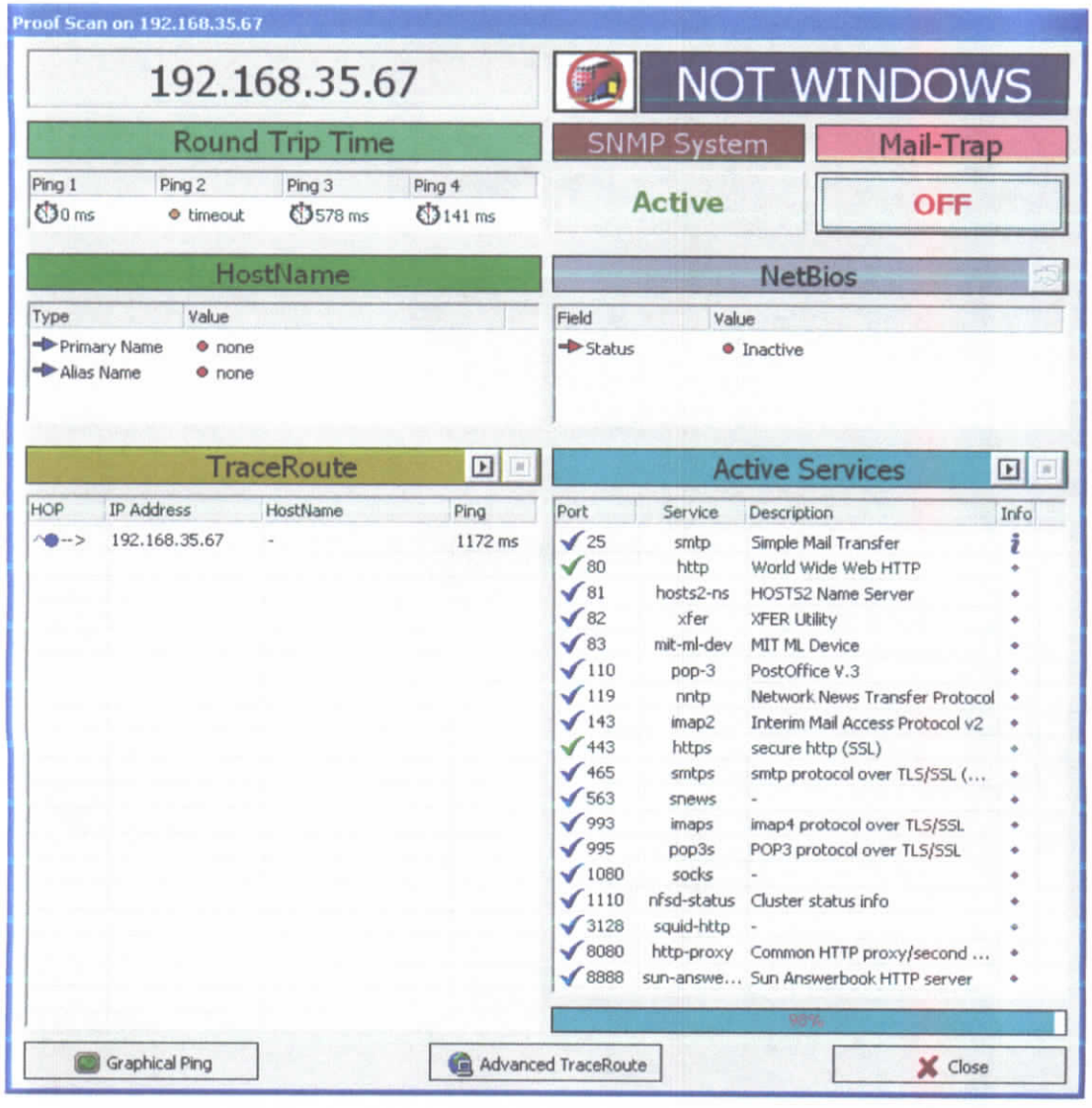
Rutas



Interfaces de Red



Servicios Activos



4.6. Recopilación de Datos de Tráfico de la Red

La recolección de Datos se la realizó durante 24 horas, en cada uno de los dos switch que concentran los equipos que integran la red de datos de la compañía, en días diferentes. Se utilizó el programa Wireshark para capturar todo el tráfico que reciba la interfaz de red LAN existente en el equipo.

4.6.1. Análisis de la información

Como punto de partida de nuestro análisis tomaremos los puntos de concentración de datos como son el acceso a Internet, los switchs y los routers, que permiten el enlazar las dos redes locales con las que dispone la empresa, para determinar la mejor opción de configuración de los mismos.

4.6.2. Acceso a Internet

El acceso a Internet esquematiza en la Figura 4.4.: Esquema de Acceso a Internet

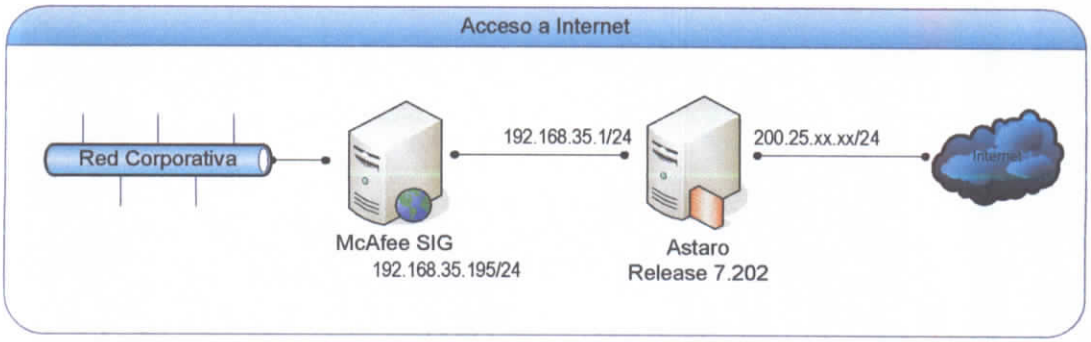


Figura 4.4. Esquema de Acceso a Internet

Se dispone de un computador personal en el cual se ha instalado como firewall el Software de Seguridad Astaro, como se puede observar en la figura 4.5: Configuración de Astaro Release 7.202, se dispone de tres interfaces de red Ethernet, de las cuales dos están activas, la una como Interna y la otra como Externa, la tercera interfaz se encuentra deshabilitada.

El enlace a Internet es de 512kb de bajada por 252kb de subida.

Para determinar la demanda a Internet por parte de la red de datos, se ha utilizado el software Look@LAN, para determinar el número de equipos activos en la red que pueden solicitar acceso a Internet, obteniendo los siguientes resultados:

Rangos de Exploración:

Scan Ranges	
FROM IP	**TO IP**
192.168.35.0	192.168.35.255
192.168.36.0	192.168.36.255
200.25.xx.xx	200.25.yy.yy

Resultado de la Exploración:

Exportation Date	01/02/2010 10:34
Total IP Addresses in list	42
Total IP Addresses ONLINE	29
Total IP Addresses OFFLINE	13

De la misma forma se utilizo la herramienta Look@LAN, para determinar el número de nodos que acceden a la red, dando como resultado un número de nodos activos e inactivos; los nodos inactivos son equipos que se activan en diferentes tiempos pero que son parte integral de la red.

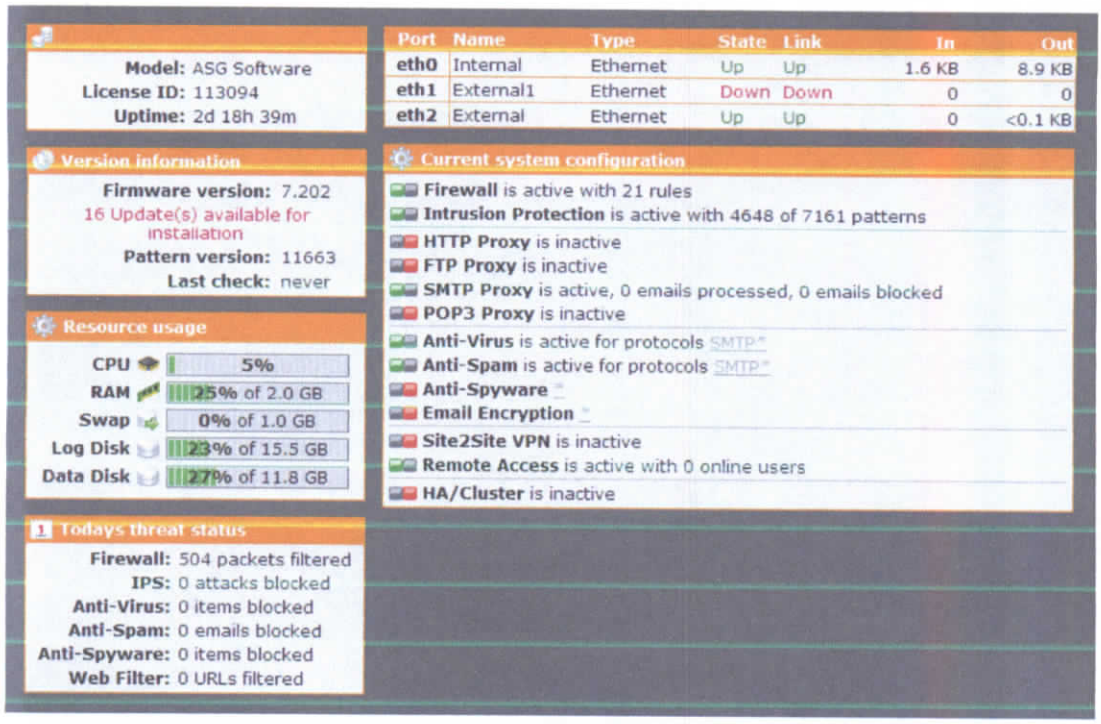


Figura 4.5. Configuración General Astaro Release 7.202

Detalle de Nodos

Status	IP Address	Distance	O.S.
	192.168.35.2	Same LAN	NOT WIN
	192.168.35.3	Same LAN	WINDOWS
	192.168.35.10	Same LAN	WINDOWS
	192.168.35.22	Same LAN	WINDOWS
	192.168.35.25	Same LAN	WINDOWS
	192.168.35.26	Same LAN	WINDOWS
	192.168.35.31	Same LAN	WINDOWS
	192.168.35.41	Same LAN	NOT WIN

	192.168.35.42	Same LAN	NOT WIN
	192.168.35.45	Same LAN	NOT WIN
	192.168.35.67	Same LAN	NOT WIN
	192.168.35.90	Same LAN	WINDOWS
	192.168.35.100	Same LAN	NOT WIN
	192.168.35.101	Same LAN	NOT WIN
	192.168.35.120	Same LAN	WINDOWS
	192.168.35.140	Same LAN	WINDOWS
	192.168.35.143	Same LAN	WINDOWS
	192.168.35.145	Same LAN	WINDOWS
	192.168.35.146	Same LAN	WINDOWS
	192.168.35.148	Same LAN	WINDOWS
	192.168.35.152	Same LAN	WINDOWS
	192.168.35.158	Same LAN	WINDOWS
	192.168.35.160	Same LAN	WINDOWS
	192.168.35.195	Same LAN	NOT WIN
	192.168.35.200	Same LAN	WINDOWS
	192.168.35.205	Same LAN	WINDOWS
	192.168.36.1	01 Hops	NOT WIN
	192.168.36.10	02 Hops	WINDOWS

	192.168.36.12	02 Hops	WINDOWS
	192.168.36.13	02 Hops	WINDOWS
	192.168.36.14	02 Hops	WINDOWS
	192.168.36.21	02 Hops	WINDOWS
	192.168.36.33	02 Hops	WINDOWS
	192.168.36.41	02 Hops	WINDOWS
	192.168.36.66	02 Hops	NOT WIN
	192.168.36.173	02 Hops	WINDOWS
	192.168.36.189	02 Hops	WINDOWS
	192.168.36.212	02 Hops	WINDOWS
	192.168.36.222	02 Hops	WINDOWS
	200.25.216.115	Same LAN	WINDOWS
	200.25.xx.xx	01 Hops	WINDOWS
	200.25.xx.xx	02 Hops	NOT WIN

Para contrastar esta información, con la configuración obtenida del Astaro, vamos a realizar un análisis de la configuración detallada del mismo.

Según la configuración de Astaro, los nodos definidos en el Firewall son las que se muestran a continuación, como se puede observar el numero de host definidos, asi como las direcciones IP asignadas, no corresponde al número de host existentes en la

red, estando definidos 59 direcciones en el Firewall frente a las 40 direcciones locales que pueden estar activas en la red.

Nro.	Astaro	
	Descripción	IP
1	192.168.35.120	192.168.35.120
2	192.168.35.150	192.168.35.150
3	192.168.35.155	192.168.35.155
4	192.168.35.158	192.168.35.158
5	192.168.35.205	192.168.35.205
6	192.168.35.210	192.168.35.210
7	192.168.36.16	192.168.36.16
8	192.168.36.173	192.168.36.173
9	192.168.36.189	192.168.36.189
10	192.168.36.190	192.168.36.190
11	192.168.36.200	192.168.36.200
12	192.168.36.204	192.168.36.204
13	192.168.36.25	192.168.36.25
14	192.168.36.40	192.168.36.40
15	192.168.36.46	192.168.36.46
16	192.168.36.49	192.168.36.49
17	192.168.36.51	192.168.36.51
18	192.168.36.98	192.168.36.98
19	ab - 192.168.35.32	192.168.35.32
20	Access Point	192.168.35.45

21	Adrian Ramirez	192.168.36.48
22	Alexandra Vaca	192.168.36.9
23	Aseguramiento	192.168.36.13
24	Asistente Compras	192.168.36.21
25	Asistente Mantenimiento	192.168.36.45
26	Blackberry	206.51.26.192
27	Bodega	192.168.36.23
28	BOL	200.107.33.161
29	cm - 192.168.35.24	192.168.35.24
30	cs - 192.168.35.152	192.168.35.152
31	David Cevallos	192.168.36.32
32	Diego Armijos	192.168.36.33
33	dn - 192.168.35.28	192.168.35.28
34	dns1	200.41.80.9
35	dns2	200.31.6.38
36	eb - 192.168.35.29	192.168.35.29
37	em - 192.168.35.22	192.168.35.22
38	Jimi Hidalgo	192.168.36.12
39	jt - 192.168.35.26	192.168.35.26
40	McAfeee Web Shield	192.168.35.195
41	mt - 192.168.35.27	192.168.35.27
42	Patricio Paucar	192.168.36.24
43	ps - 192.168.35.25	192.168.35.25
44	Rober Chavez	192.168.36.30

45	Router Planta	192.168.36.1
46	Router UIO	192.168.35.2
47	Servidor Archivos EPPNT	192.168.36.10
48	Servidor Archivos EXPNT	192.168.35.10
49	Servidor MAIL	192.168.35.100
50	Servidor NT UIO	192.168.35.3
51	Servidor PDC	192.168.35.50
52	TEMP	192.168.35.60
53	VoIP_ttorres	192.168.35.18
54	voip_ttorres2	192.168.35.17
55	vp - 192.168.35.23	192.168.35.23
56	VTT	192.168.35.7
57	wv - 192.168.36.11	192.168.36.11
58	XM - 192.168.35.31	192.168.35.31
59	yh - 192.168.35.20	192.168.35.20

De igual manera haciendo una comparación de las direcciones activas frente a las definidas no concuerdan, el riesgo de tener direcciones definidas sin que exista un nodo con dicha dirección abre una brecha de seguridad así como mantiene al firewall realizando actividades que no dan valor a la organización.

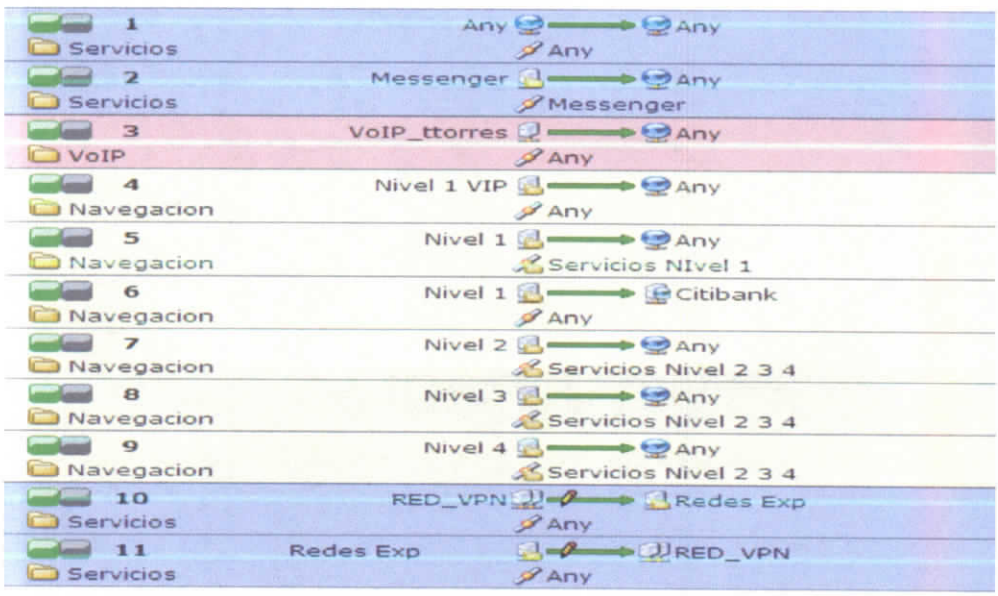
Los servicios definidos en Astaro son:

Servicio	Detalle	Protocolo	Puertos
Any	Matches any IP protocol		
AOL IM	AOL Instant Messenger using the OSCAR protocol (might also work over HTTP)	TCP	1:65535 → 5190
Apple Remote Desktop 1	Apple Remote Desktop (ARD) V1	TCP/UDP	1:65535 → 3283
Apple Remote Desktop 2	Apple Remote Desktop V2 & V3	TCP	1:65535 → 5900
Astaro Command Center (ACC)	Service to connect an ASG to an Astaro Command Center	TCP	1:65535 → 4433
Astaro Spam Release	Astaro Spam Release	TCP	1:65535 → 3840:4840
Astaro Up2Date	Services used by ASG to communicate with Astaro Up2Date Server		
Astaro WebAdmin	Astaro WebAdmin	TCP	1:65535 → 4444
CIFS	Microsoft Common Internet File System	TCP/UDP	1:65535 → 445
Citrix ICA	Citrix Independent	TCP	1:65535 →

	Computing Architecture (ICA) protocol		1494
DNS	Domain Name Service	TCP/UDP	1:65535 → 53
Email Messaging	Protocols to send and receive emails		
FTP	File Transfer Protocol	TCP	1:65535 → 21
FTP Control		TCP	1:65535 → 21
Google Talk IM	Google Talk Instant Messenger (might also work over port HTTPS) using XMPP protocol	TCP	1:65535 → 5222
GRE	Generic Routing Encapsulation used by PPTP and other procols	IP	IP Protocol 47
H323	H.323 voice over ip and multimedia conferencing	TCP/UDP	1:65535 → 1719:1720
HP JetDirect	HP Jet Direct - network print service	TCP	1:65535 → 9100
HTTP	Hypertext Transfer Protocol	TCP	1:65535 → 80
HTTP Proxy	HTTP-Proxy service or	TCP	1:65535 →

	alternative HTTP-Server service		8080
HTTP WebCache	HTTP used by web caching proxies	TCP	1:65535 → 3128
HTTP-POP3			
HTTPS	Hypertext Transfer Protocol over SSL	TCP	1:65535 → 443
ICQ IM	ICQ instant messenger using the OSCAR protocol (might also work over HTTP)	TCP	1:65535 → 5190
IMAP	Internet Message Access Protocol	TCP	1:65535 → 143

El filtrado de paquetes establecido es:

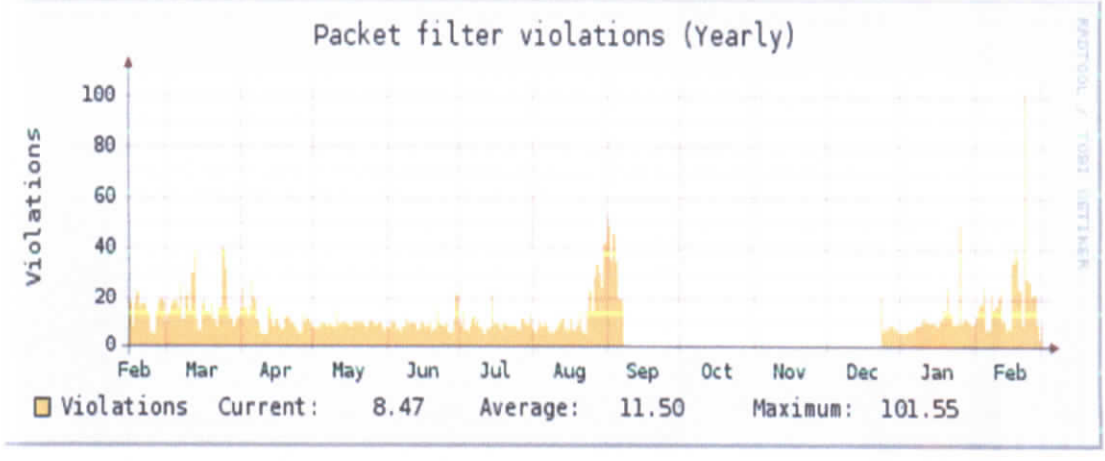


12 Broadcast	Any	Any	Internal (Broadcast)
13 Broadcast	Any	Any	External (Broadcast)
14 Broadcast	Any	Any	External1 (Broadcast)
15 MailLinux	Servidor MAIL	Any	Any
16 None	Red36	Any	Any
17 None	Internal (Network)	Any	Any
18 Servicios	GMS Network	SSH	Servidor MAIL
19 Servicios	Any	HTTP-POP3	Servidor MAIL
20 Servicios	GMS Network	Oracle Services	Servidor NT UIO
21 Broadcast	Any	Any	External1 (Broadcast)

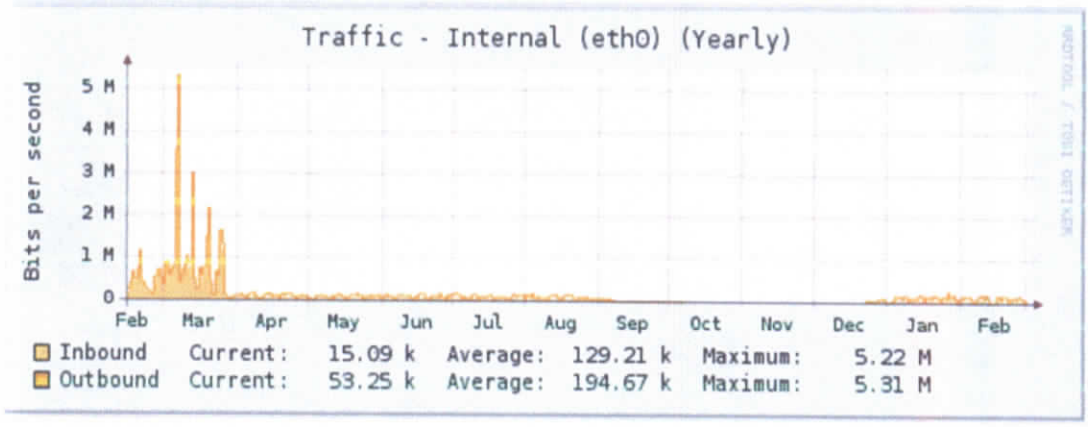
4.6.2.1. Estadísticas de Demanda y Consumo

Se han obtenido una serie de estadísticas relacionadas con el acceso a Internet y la demanda de sus servicios los cuales se presentan a continuación:

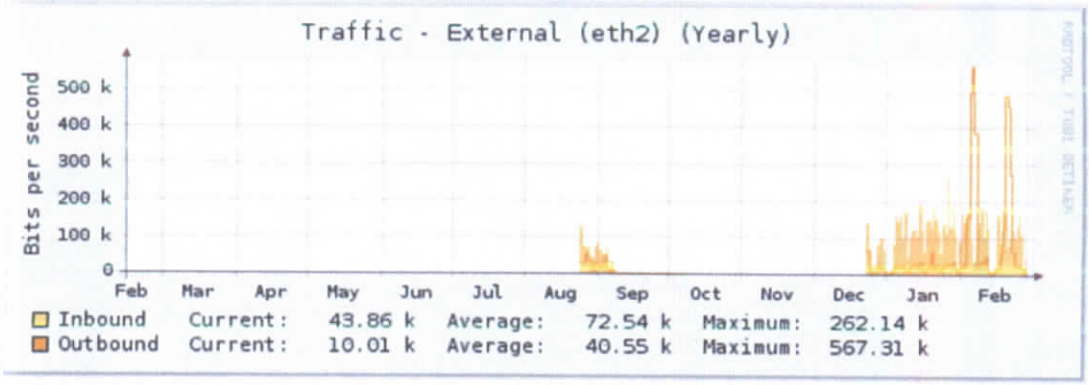
- **Violaciones al Filtrado de Paquetes (Comportamiento Anual)**



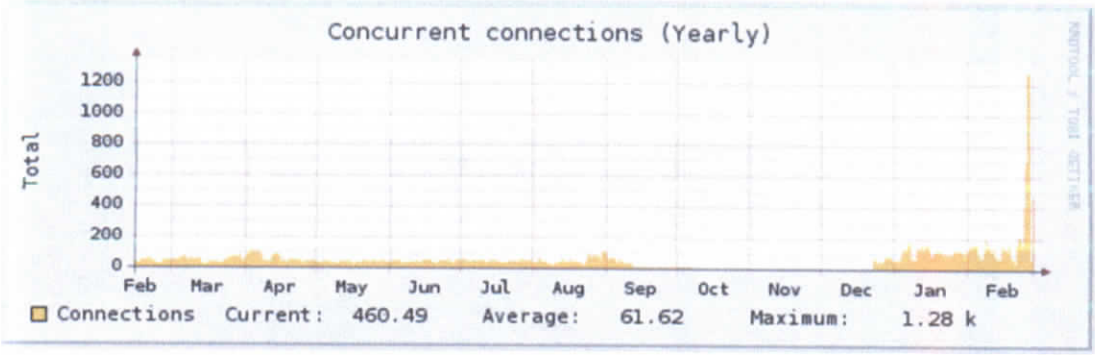
- **Tráfico Interno (Comportamiento Anual)**



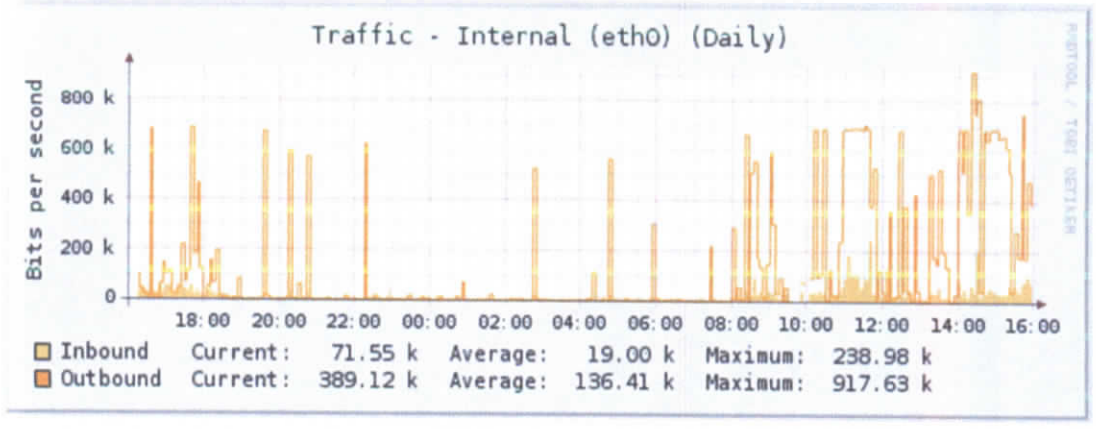
- **Trafico Externo (Comportamiento Anual)**



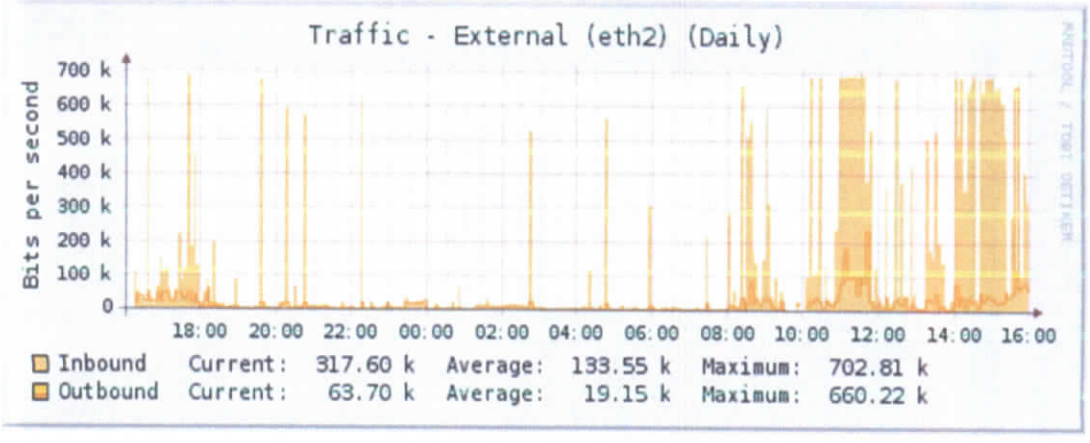
- **Conexiones Concurrentes (Comportamiento Anual)**



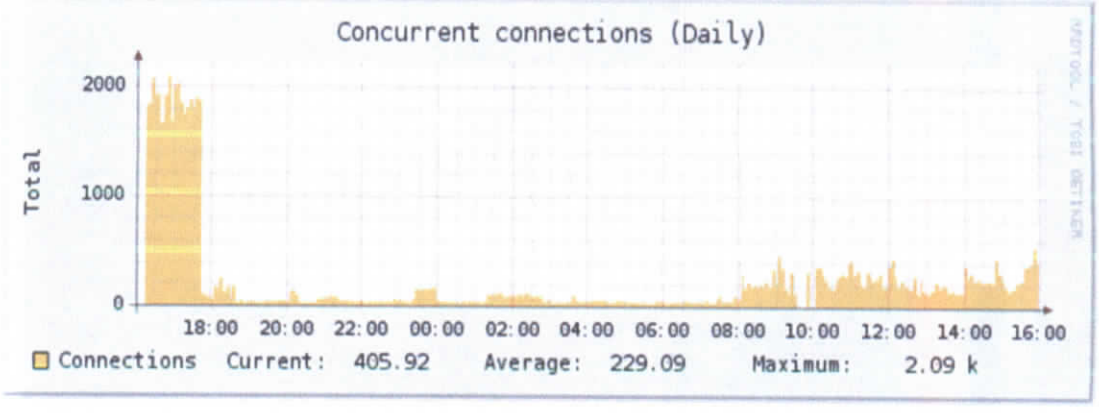
- **Tráfico Interno (Comportamiento Promedio de un Día)**



- **Tráfico Externo (Comportamiento Promedio de un Día)**



- **Conexiones Concurrentes (Comportamiento Promedio de un Día)**



4.6.3. Conclusiones y Recomendaciones

1. ***Conclusión 1- Definición de Nodos:*** Los nodos activos en la red y sus respectivas IP, no son consistentes con los especificados en el Astaro (Firewall).

   Recomendación 1: Realizar una depuración de las direcciones a las cuales se da acceso a los servicios externos proporcionados desde el Internet.

2. ***Conclusión 2 – Definición de Filtrado de Paquetes:*** Existen 21 reglas de filtrado definidas, sin embargo entre si se anulan dejando libre acceso al servicio tanto externo como interno, como por ejemplo la primera regla definida indica que cualquier tipo de tráfico de cualquier clase sea entregado a cualquier solicitante, esta simple regla elimina la efectividad de las 20 reglas subsiguientes.

   Recomendación 2: Realizar un análisis detallado de los requerimientos de la organización y redefinir las reglas especificadas de filtrado.

3. ***Conclusión 3 – Capacidad Limitada del Canal:*** El contar con un canal tan pequeño como el que se dispone, representa que en momentos determinados como se puede observar en los gráficos relacionados con un día promedio, la demanda crece saturando en ocasiones el canal con el decremento en la calidad de servicio, determinando que para este ejemplo concreto las horas pico de demanda van desde las 10:00 a las 13h00 y las 14h00 a las 16h00.

   Recomendación 3: Definir reglar claras de acceso a los servicios de Internet para evitar la saturación en las horas pico.

4.7. Control de Contenido

Se dispone de un Email and Web Security Appliance 3000 en su versión 5.1, el cual monitorea y controla el tráfico relacionado con el enlace a Internet, del monitoreo realizado aprovechando las capacidades de reporte del producto, se han obtenido los resultados que a continuación se exponen de la demanda de la organización a nivel de seguridad perimetral.

Este dispositivo permite monitorear y controlar el tráfico hacia Internet en varios aspectos como son:

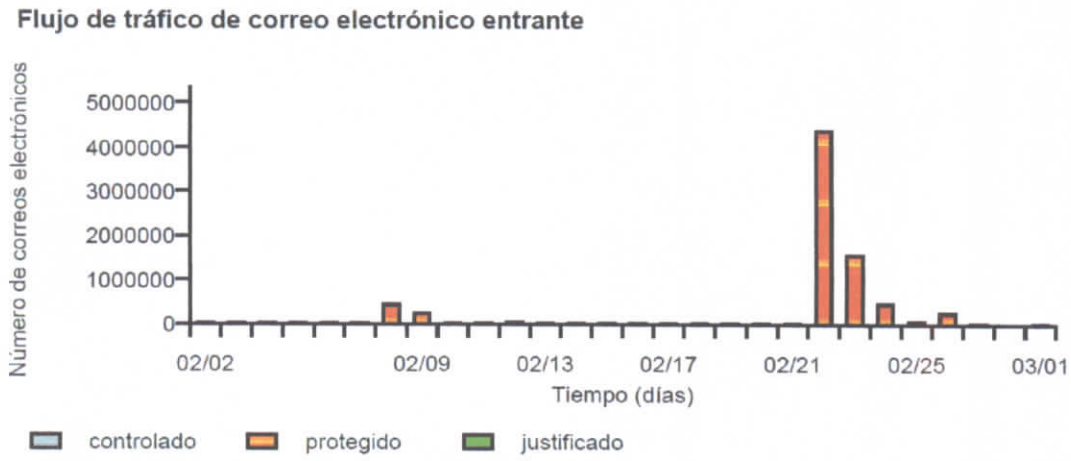
- Seguridad de Correo electrónico:

  - virus
  - programas potencialmente no deseados
  - contenido
  - spam y phishing
  - reputación y autenticación del remitente
  - otras detecciones
  - entregado (controlado o justificado)

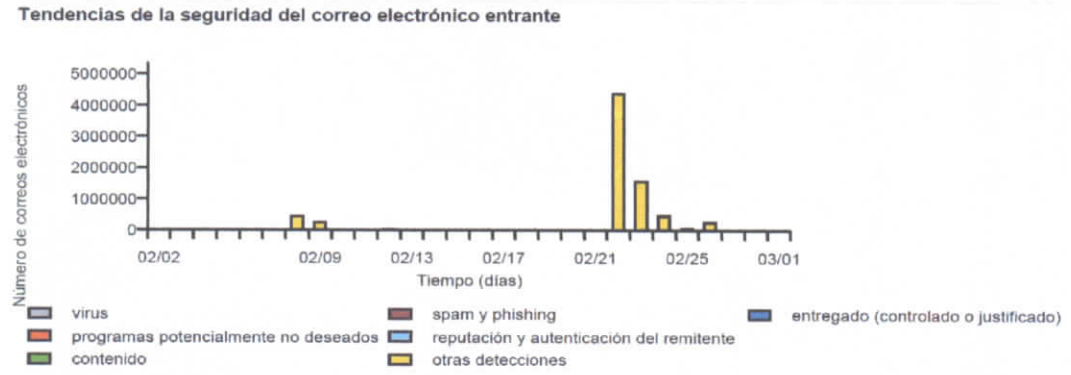
En el caso de nuestra red de datos la estadística de un mes de trabajo es la siguiente:

categoría	número de correos electrónicos
virus	0
programas potencialmente no deseados	0
contenido	0
spam y phishing	7986
reputación y autenticación del remitente	255744
otras detecciones	7280449
controlado	1279
justificado	53483

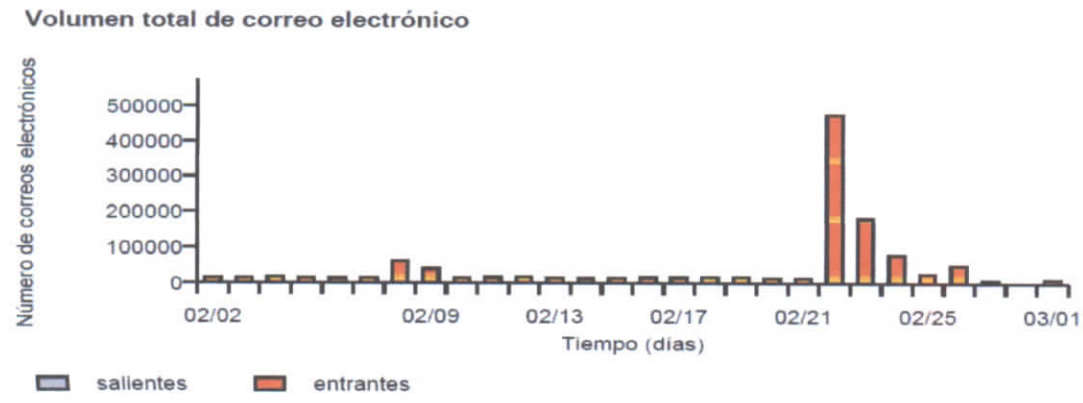
- **El flujo de tráfico de correo es:**



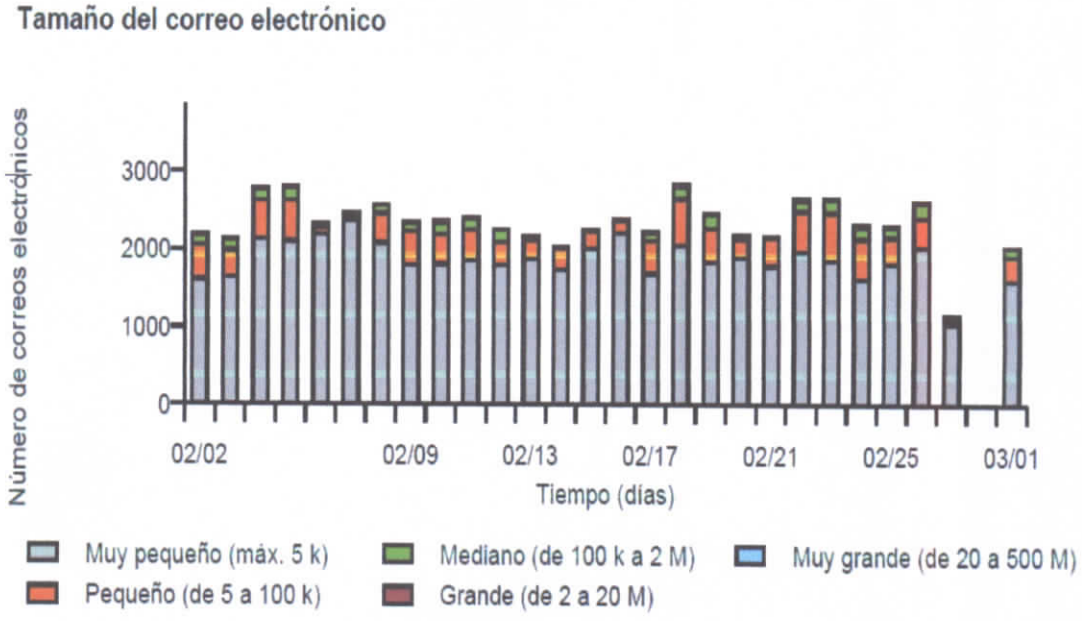
- **La tendencia de seguridad del correo entrante es:**



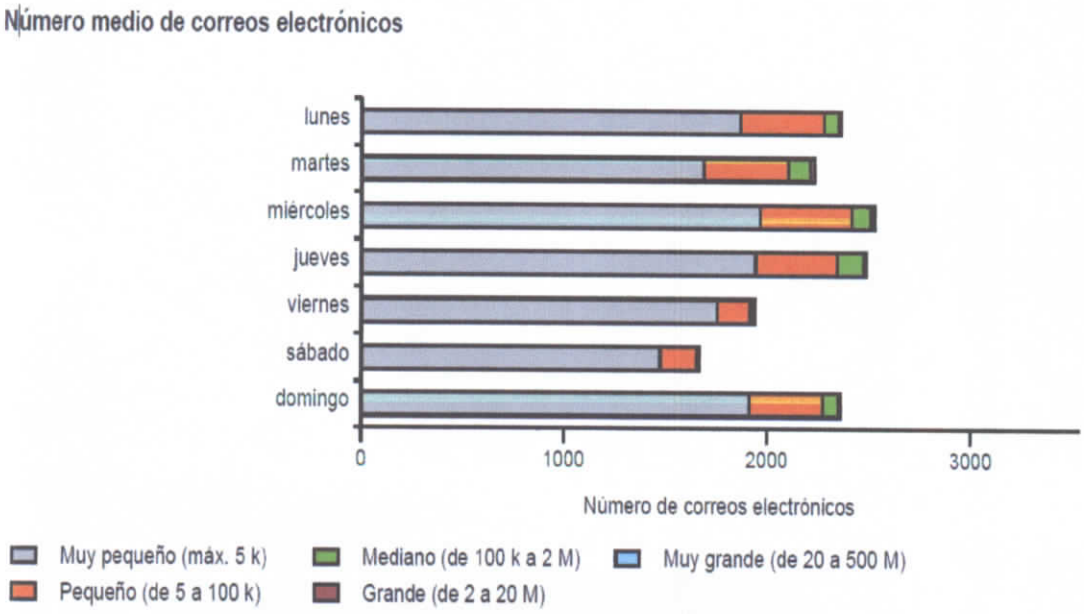
- **El volumen total de correo electrónico es:**



- **El tamaño del correo electrónico es:**



- **El número medio de correos electrónicos es:**



- **La actividad de los usuarios se resume:**

Usuarios	Numero de correos electronicos
Desconocido	49556

Principales destinatarios internos de correos electrónicos controlados o bloqueados

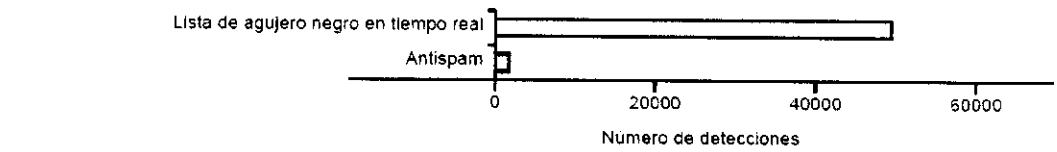
Usuarios	Numero de correos electronicos
<exp @exp .com>	310
<sales@exp .com>	309
<plant@exp .com>	252
<cminiguano@exp .com>	245
<avaca@exp .com>	217
<astaro@exp .com>	197
<logistics@exp .com>	171

Principales remitentes externos de correos electrónicos controlados o bloqueados

Usuarios	Numero de correos electronicos
Desconocido	7950
<>	323
<do-not-reply@fw-notify.net>	211
<cminiguano@ >	91
<noresponder@itargget.net>	36
<plant@ >	32
<psarango@ >	28

- **Control de seguridad AntiSpam y AntiPhishing**

Servicios de autenticación de remitente, antispam y antiphishing



	detectado
Lista de agujero negro en tiempo real	49545
Antispam	1824

- **Detecciones por Protocolo**

- **Detección de Amenazas por Protocolo**

Número de detecciones por tipo de amenaza y protocolo

	smtp	pop3	http	icap	ftp
virus	1	0	0	0	0
programas potencialmente no deseados	0	0	0	0	0
contenido	0	0	0	0	0
spam y phishing	8235	1279	0	0	0
reputación y autenticación del remitente	255744	0	0	0	0
filtro de URL	0	0	0	0	0
site advisor	0	0	0	0	0
instant messenger	0	0	0	0	0
otras detecciones	7280452	0	0	0	0

- ***Conclusiones:*** Todas las amenazas se centran en el análisis del protocolo SNMP, lo cual cubre el principal tipo de tráfico hacia el Internet.

  Recomendación: Es recomendable extender el control y análisis hacia los demás protocolos para evitar amenazas adicionales a través de Internet.

4.8. Propuesta de Reestructuración de la Red de Datos

De la información obtenida, se concluye que la empresa depende para su normal funcionamiento de los servicios que presta la red de datos, lo cual exige que la

disponibilidad de los servicios y la seguridad de la información relacionada con estos sea tomada de manera prioritaria.

El intercambio de información mediante los medios electrónicos disponibles principalmente con clientes y proveedores, exige que la disponibilidad de los mismos sea las 24 horas del día los 7 días de la semana.

La configuración actual pone a la empresa en una posición poco estratégica debido a que si falla cualquiera de los proveedores o servicios relacionados con el transporte de datos la empresa se quede imposibilitada de continuar con sus actividades normales.

Se propone establecer un esquema redundante de transporte de información por medio de un segundo proveedor de Internet, de manera tal que se forme un anillo mediante un segundo enlace activando una VPN, para garantizar el acceso a los diferentes sitios.

La información obtenida revela que la empresa no tiene activado ningún tipo de protocolo de calidad de servicio, que para la red interna no es necesario debido a que el número de nodos no saturan los servicios existentes, sin embargo, como se manifestó en la sección anterior, la configuración del Firewall debe ser replanteada, y además implementar políticas de administración del mismo para evitar que se presenten nuevamente situaciones como la indicada de configuraciones duplicadas o de especificaciones de nodos no existentes en la red.

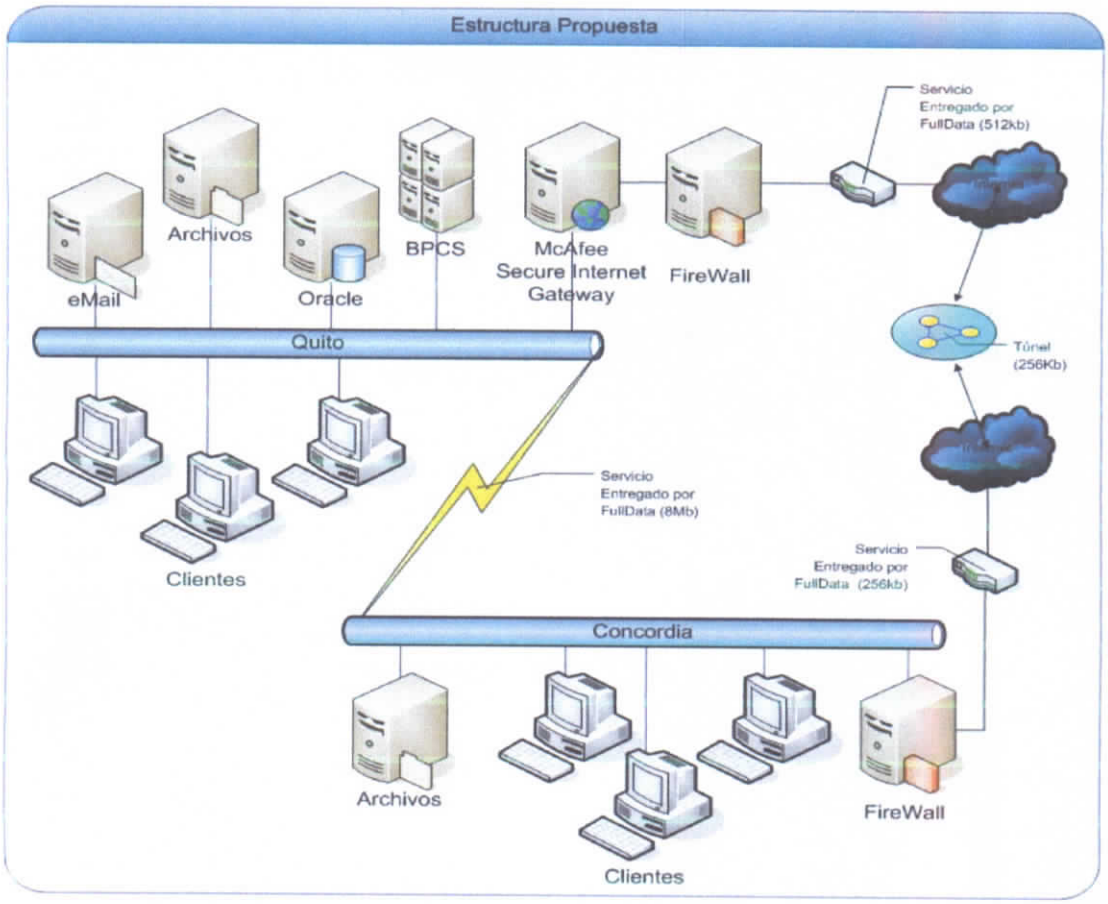


Figura 4.6. Propuesta de Reestructuración de la Red de Datos, para garantizar máxima disponibilidad

CAPITULO V

5. CONCLUSIONES Y RECOMENDACIONES

5.1. Demostración de Hipótesis

Se había establecido como hipótesis del presente estudio:

"Con un análisis de la cantidad y tipo de tráfico que transporta una red de datos, en cada uno de sus enlaces, se puede especificar la configuración óptima de los equipos para maximizar el uso de los recursos disponibles."

Como se ha establecido a lo largo del estudio, el uso de herramientas de análisis para recopilar la información tanto de las configuraciones de los diferentes elementos que integran la red de datos, así como del tipo de tráfico que circula por ella, nos ha permitido definir una propuesta de estructuración de la red, así como emitir recomendaciones que permitan optimizar el uso del recurso disponible que en este caso es limitado en relación a la capacidad del canal de comunicaciones con el Internet, quedando así demostrada nuestra hipótesis.

5.2. Conclusiones

Del análisis realizado podemos concluir:

1. La organización objeto de nuestro estudio no dispone de un enlace de respaldo para acceder al Internet y entre si los dos puntos geográficos que son parte de su infraestructura operativa.
2. No tienen establecidas políticas de calidad de servicio así como de administración de los elementos que componen la red de datos y los diferentes equipos que acceden a ella.
3. La organización depende en gran medida del acceso a Internet y de los servicios relacionados para mantener sus operaciones normales.

5.1. Recomendaciones

En relación a las conclusiones establecidas se recomienda:

1. Implementar la estructura propuesta.
2. Implementar políticas y procedimientos de calidad de servicio de preferencia guiándose de estándares como COBIT o ITIL.
3. Realizar el estudio y reconfiguración planteados de las configuraciones y permisos del firewall y elementos de conectividad existentes.

Bibliografía

Administración de Redes por Patricia Cleopatra Victoria Aguilar, **pcva_correo@hotmail.com, Febrero 2007. http://www.monografias.com/trabajos43/administracion-redes/administracion-redes.shtml**

ADMINISTRACIÓN DE REDES, Universidad de Guadalajara, Centro Universitario de Ciencias Económico – Administrativas, *REDES I,* DICIEMBRE 2000, **http://html.rincondelvago.com/administracion-de-redes.html**

Administración de Redes

http://www.cisco.com/web/LA/productos/network_mgmt.html

Analizador de Protocolos, Wikipedia

http://es.wikipedia.org/wiki/Analizador_de_protocolos

Calidad de Servicio, Gobierno de España, Ministerio de Industria, Turismo y Comercio

http://www.mityc.es/telecomunicaciones/es-ES/Servicios/CalidadServicio/Paginas/Calidad.aspx

Calidad de Servicio, Wikitel

http://www.wikitel.info/wiki/Calidad_de_servicio

Fundamentos de Gestion de TI, Osiatis

http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/fundamentos_de_la_gestion_TI/que_es_ITIL/que_es_ITIL.php

Guía de Administración de Redes con Linux

Olaf Kirch

Terry Dawson

Editado por

O'Reilly (printed version) (c) 2000 O'Reilly & Associates

Proyecto LuCAS por la traducción al español (c) 2002 HispaLiNUX

http://www.ibiblio.org/pub/linux/docs/LuCaS/Manuales-LuCAS/GARL2/garl2/

La administración de redes

Cesar ángel Tovar Flores
Cesarangel_tovar[arroba]yahoo.com.mx
Universidad de Guadalajara, Jalisco México

http://www.monografias.com/trabajos7/adre/adre.shtml

Medición de la calidad del servicio

José Antonio Mendoza Aquino
jomeaq[arroba]hotmail.com

http://www.monografias.com/trabajos12/calser/calser.shtml

Modo promiscuo,Wikipedia

http://es.wikipedia.org/wiki/Modo_promiscuo

Packet sniffer, Wikipedia

http://es.wikipedia.org/wiki/Packet_sniffer

PCAP,Wikipedia

http://es.wikipedia.org/wiki/Pcap

Tutorial de TCPDUMP, Wikilearning

http://www.wikilearning.com/tutorial/pequeno_tutorial_de_tcpdump-introduccion/6424-1

TcDump, Wikipedia

http://es.wikipedia.org/wiki/Tcpdump

Tipos de Sniffer, Wikipedia

http://es.wikipedia.org/wiki/Tipos_de_Sniffer#ETHEREAL_.28WIRESHARK.29

Wireshark, Wikipedia

http://es.wikipedia.org/wiki/Wireshark

Wireshark, Wireshark.com

http://www.wireshark.org/docs/