Universidad Central "Marta Abreu" de Las Villas
Facultad de Ingeniería Eléctrica
Departamento de Telecomunicaciones y Electrónica

TRABAJO DE DIPLOMA

"Estrategia para la Gestión de una Intranet"

Autor: *José Luis Acebo Puentes*.
Tutor: *Dr. Félix Álvarez Paliza.*
Msc. *Manuel Oliver Domínguez.*

Santa Clara
2004
"Año del 45 aniversario del triunfo de la revolución"

Hago constar que el presente trabajo fue realizado en la Universidad Central “Marta Abreu” de las Villas como parte de la culminación de los estudios de la especialidad de Telecomunicaciones y Electrónica autorizando a que el mismo sea utilizado por la Institución, para los fines que estime conveniente, tanto de forma parcial como total y que además no podrá ser presentado en eventos, ni publicados sin autorización de la Universidad.

_____

Firma del Autor

Los abajo firmantes, certificamos que el presente trabajo ha sido realizado según acuerdo de la dirección de nuestro centro y el mismo cumple con los requisitos que debe tener un trabajo de esta envergadura referido a la temática señalada.

_____ _____

Firma del Tutor

Firma del Jefe de Dpto.
Donde se defiende el trabajo

_____

Firma del Responsable de
Información Científico- Técnica

Resumen.

El presente trabajo trata sobre la Estrategia de Gestión de una Intranet y su aplicación a la red de la Universidad Central de Las Villas. En él se analizan las bases teóricas de un sistema de supervisión y de administración de los elementos activos en una red de ordenadores.

Los esfuerzos fueron dirigidos hacia la construcción de una estrategia que permita la gestión de la red UCLV, y por tanto se analizan todos los elementos que influyen de una manera u otra en la administración del equipamiento y de los servicios.

También se muestran resultados de pruebas de tráfico, aplicadas en algunos de los enlaces de la red UCLV en diferentes condiciones, en los que se muestra el cambio de la velocidad y latencia de paquetes. El perfeccionamiento realizado al ancho de banda es indispensable para la transmisión de la información de gestión manejada a nivel de Intranet.

Índice.

Introducción.

Con el paso del tiempo la humanidad se ha ido desarrollando dentro de un entorno completamente ligado a las computadoras, el uso de sistemas de esta índole, y el respaldo de la Inteligencia Artificial para realizar las más disímiles tareas se ha convertido, más que un lujo, en una necesidad para todos y cada uno de nosotros.

Existe además una ola inminente en el aumento de las velocidades de transmisión, volúmenes de datos y cantidad de estaciones utilizadas hoy en día en las redes de ordenadores, lo cual ha incrementado también la necesidad de que todos los elementos de una estructura de este tipo trabajen correctamente.

Es evidente que en el entorno de las redes de computadoras existe mucho que perder si alguno de los puntos que las conforman deja de trabajar o lo hacen con cierta oscilación en su estabilidad. Este es un costo que casi nunca hay que pagar pero que no se debe olvidar que existe.

Para el criterio de evaluación sobre la estabilidad de una red, la opinión del usuario final es el elemento de más peso, puesto que este se sirve de las posibilidades que toda red de computadoras brinda, y por tanto, la supervisión de los servicios y la pronta atención y reparación de estos, en caso de que existan interrupciones, es un factor crucial en el desempeño de la estructura, cualquiera que esta sea.

La red de campus UCLV cuenta hoy en día con más de 1150 computadoras y un directorio de al menos 7200 usuarios a tiempo completo, a estos se le agregan de forma ocasional otros 3000 usuarios que, como bien expresa la palabra, no están activos todo el tiempo. Durante el período de crecimiento de la red las condiciones en las cuales esta se ve comprometida a trabajar son cada vez más exigentes, de manera que se necesita un esfuerzo y sacrificio adicional por parte del personal que trabaja directamente en la administración de la red.

Es de destacar que durante el proceso evolutivo de la red universitaria las tareas en cada facultad han estado guiadas por los administradores correspondientes, lo cual indica que la homogeneidad en las políticas y equipamiento del sistema como conjunto no era un tema sólido para resaltar la unidad de la estructura como un todo.

Hoy en día representa un problema a nivel universitario la falta de una estrategia de gestión que pueda brindar los elementos necesarios para la supervisión y control del equipamiento de la red, y de la información que por ella viaja.

Al cuestionarse el problema planteado anteriormente surgen a nuestro paso las siguientes interrogantes:

- ¿Cuáles son las condiciones en las que se encuentra cada facultad para formar parte de una estrategia de gestión a nivel centralizado?
- ¿Existen en los locales, destinados para la instalación de los dispositivos de la red, condiciones favorables para la pronta instalación del equipamiento adquirido?
- ¿Cómo se puede lograr una mejor supervisión y control de la red de computadoras mediante las posibilidades que los propios equipos de conmutación brindan?

De aquí se deriva el objetivo central de este estudio y consiste en la elaboración de una estrategia de gestión para la intranet UCLV, que sea capaz de facilitar la supervisión y el control de los elementos interconectados a ella, para lo cual se toma como punto de apoyo las tareas mostradas a continuación:

- Caracterizar el estado actual del *backbone* UCLV.
- Configurar los *switch* gestionables desde el punto de vista de los servicios que se implementan en cada uno de los módulos de software.
- Valoración y Configuración del *Nagios* como plataforma de gestión a nivel de Intranet.

- Evaluar los resultados obtenidos en las pruebas de tráfico, aplicadas a diferentes enlaces de fibra, durante el perfeccionamiento del *backbone*.
- Documentar el procedimiento seguido en los estudios para la implementación y prueba del equipamiento.

Este trabajo consta de una introducción, tres capítulos que definen y abarcan las tareas propuestas anteriormente, conclusiones, recomendaciones, referencias bibliográficas, glosario y anexos necesarios para el entendimiento del estudio. Se muestra a continuación un resumen de la información abordada en cada uno de los capítulos.

En el primer capítulo se tratan temas de actualización sobre el estado del arte de la gestión de redes de computadoras en el mundo, se aborda con profundidad el modelo SNMP (*Simple Network Management Protocol*) así como las partes que componen un sistema de gestión y la comunicación entre estas. Se abarcan elementos importantes sobre el monitoreo remoto de equipos en la estructura así como los recursos que se distribuyen entre ellos. La bibliografía referenciada en cada caso se encuentra al alcance de todo el que desee profundizar más sobre un tema específico.

El segundo capítulo caracteriza la “Red UCLV” con el fin de conocer las propiedades de la estructura a gestionar. Se toman en cuenta las ineficiencias que influyen de una forma u otra en el desarrollo del sistema de gestión de la Intranet. Se tratan las prestaciones de los dispositivos gestionables adquiridos en el centro como el elemento básico para trazar la estrategia de administración.

Por último, en el tercer capítulo, se abarca la configuración de los *switches*, desde el punto de vista de los servicios que son implementados en cada modulo de software. Se establece un software libre, *Nagios*, como plataforma de gestión a nivel global, con el objetivo de homogenizar el trabajo de administración, se muestran sus potencialidades y las funciones que realiza. Se realizan pruebas para valorar y evaluar los cambios producidos en el desempeño del ancho de banda de la red. De esta manera queda conformada una estrategia basada en equipamiento de punta para la gestión y supervisión de la Intranet UCLV.

CAPÍTULO I: Gestión en redes de Computadoras.

En las complejas redes de hoy en día pudiera parecer una tarea imposible controlar todos los dispositivos en red, y lograr no solo que estos trabajen sino que lo hagan de forma óptima. La gestión de redes es la encargada de facilitar esta tarea, de ahí la necesidad de conocer, estudiar y dominar lo relacionado con esta materia.

Se entiende por gestión de redes la supervisión, la obtención de información y el control de dispositivos inteligentes distribuidos a lo largo de una red de computadoras. Para lograr esto se crea un canal de gestión, que está compuesto por un agente (*agent*) y una estación de monitoreo que se comunican mediante un protocolo preestablecido conocido como SNMP (*Simple Network Management Protocol*). El agente es generalmente un equipo electrónico (*hardware*) y corresponde a un programa de computación (*software*) desempeñar el rol de estación de monitoreo. [Stallings, 1998]

SNMP es considerado uno de los protocolos que más se conocen y usan en el mundo para la administración, supervisión y monitoreo en redes de computadoras. La mayoría de las firmas de prestigio que producen equipos de comunicación gestionables brindan soporte para SNMP, esto se debe a la robustez con que fue construido el protocolo desde sus inicios y a la minuciosidad con que se han realizado las ampliaciones y correcciones en las versiones posteriores; la popularidad ha sido otro factor importante que ha contribuido a su evolución. [Westerinen, 2003].

La información a gestionar y las funciones de los elementos involucrados en un canal de gestión pueden ser vistas a través del modelo de gestión de redes que define la ISO (*Internacional Organization for Standarization*). [Westerinen, 2003]. En él se agrupan las áreas consideradas claves en la administración de redes. Estas áreas son: Administración de Fallas, Administración de Cuentas, Administración de Configuración y Nombres, Administración de Desempeño y Administración de Seguridad (*Fault Management,*

Accounting Management, Configuration and Name Management, Performance Management, Security Management), por sus nombres en inglés. Este modelo tiene una gran importancia, pues al igual que el modelo OSI de siete capas para el estudio de redes de computadoras brinda los fundamentos teóricos de cualquier sistema de gestión. [Westerinen, 2003].

I.1 Introducción al modelo SNMP

El modelo SNMP fue introducido en 1988 para satisfacer la creciente necesidad de un estándar para gestionar dispositivos que soportaran tráfico IP (*Internet Protocol*). Este modelo está compuesto por la definición de las partes involucradas y el protocolo que utilizarán para comunicarse, también llamado SNMP. Este protocolo brinda a los usuarios un conjunto muy simple de instrucciones que permiten que los dispositivos que lo soporten sean gestionados de forma remota. [Stallings, 1998]

La idea central de SNMP es dar a los administradores la posibilidad de cambiar el estado de dispositivos que soporten este protocolo. Por ejemplo se puede usar SNMP para apagar un *router* o para deshabilitar un puerto de un *switch*. Con SNMP se podría incluso monitorear la temperatura de una impresora y enviar una advertencia en caso de que fuera muy alta.

Sucede con mucha frecuencia que el SNMP se asocia solo a *routers* gestionables, pero es importante entender que se pueden gestionar muchos tipos de dispositivos. Mientras que su predecesor SGMP (*Simple Gateway Management Protocol*) [Thottan, 2003] fue desarrollado para controlar *routers*, SNMP puede ser usado para gestionar sistemas basados en UNIX o en Windows, impresoras, *Rack* de MODEM o fuentes de respaldo por solo citar algunos ejemplos. La lista no se limita solo a dispositivos de *hardware*, también pueden ser supervisados servidores de Web, de archivos o de bases de datos.

Otro aspecto dentro de la temática de la gestión es el monitoreo de la red. Esto consiste en la supervisión de la red como un todo, no solo de las partes que la componen por separado. Para esto fue desarrollado el protocolo RMON (*Remote Network Monitoring*) que ayuda a los administradores a entender cómo la red se encuentra funcionando, así como las implicaciones que tienen los dispositivos por separados en un correcto o incorrecto funcionamiento. [Thottan, 2003].

I.2 Necesidad de la Gestión de Redes.

Para comprender exactamente la necesidad que tiene una red de ser gestionada podemos tomar en cuenta el ejemplo siguiente:

En una red de computadoras, por lo general, existe una total dependencia por parte de los usuarios de la disponibilidad de información para realizar su trabajo, ya esté contenida en un servidor WEB, FTP, de impresión o de bases de datos; ahora bien, ¿Qué sucedería si uno de los servidores de ficheros quedara fuera de servicio? Esto no sería un gran problema si fuese en horario de trabajo en el que el administrador estaría disponible para solucionarlo; pero la situación seria muy distinta si esto ocurriese en otro momento en el cual las consecuencias suelen ser mucho mayores.

Si consideramos, además, que la red pertenece a una empresa de negocios que brinda servicio a usuarios en Internet puede predecirse que las pérdidas pudieran ser enormes y esto constituye un gran problema, que afectaría incluso la supervivencia de la empresa. Este es el punto donde SNMP entra a jugar un papel determinante.

Generalmente en una red no gestionada cuando ocurre una falla casi siempre es detectada por los mismos usuarios, luego se busca a la persona encargada de corregirla. En una red gestionada se pueden monitorear elementos especificados y en caso de detectar cualquier anomalía en su funcionamiento se puede avisar a la persona responsable de solucionarlo mediante varias vías. [Thottan, 2003].

La situación pudiera ser incluso mejor, SNMP puede darse cuenta de que se avecina un problema, mediante ciertos patrones de comportamiento, y alertar la situación anómala antes de que ocurra en realidad. Por ejemplo si el número de paquetes con error en una interfaz aumentan rápidamente eso quiere decir que es casi seguro que esa interfaz de red está cerca de salir de servicio, se puede tomar una medida antes de que eso ocurra y así evitar consecuencias peores.

I.2.1 Recursos Humanos y su Esencia.

Otro aspecto importante a considerar es el reconocimiento social para con el administrador de la red. La administración de redes es casi siempre vista desde el punto de vista técnico, pero tiene una parte filosófica un poco distinta a lo que estamos acostumbrados a ver. Casi nunca se nota a la persona encargada de una red donde todo funciona correctamente, donde nunca existen problemas. Sin embargo todos reconocen "al que arregla rápido las cosas" y "al que soluciona rápido los problemas" en un lugar en el cual los problemas son frecuentes, y esta discriminación llega hasta el punto de que este individuo puede tener un salario mucho mayor que el "administrador que no se nota". [Mauro, 2001]. Se llama la atención sobre el siguiente planteamiento: "Puede que no exista mucha gloria en arreglar los problemas antes de que ocurran, pero tú y tus equipos podrán descansar más fácilmente. No podemos decirte cómo traducir eso en un mayor salario, a veces es mejor ser el tipo que embiste con precipitación y arregla las cosas en el medio de una crisis antes que ser la persona que se asegura que la crisis nunca ocurra." [Mauro, 2001].

Hay otros aspectos en los que se debe pensar a la hora de crear un sistema de gestión de red. La implementación de dicho sistema puede muchas veces representar un incremento en el personal que se encargará de configurar y mantener trabajando los dispositivos que se instalen. A la misma vez el correcto funcionamiento de la estructura de monitoreo y supervisión que se instale en muchos casos representará una disminución en la carga de trabajo de los administradores. [Thottan, 2003].

Las necesidades de personal definidas en [Mauro, 2001] se pueden clasificar en 3 grupos:

- Personal para mantener la estación de gestión. Este grupo contempla los técnicos necesarios para que la estación de gestión esté configurada adecuadamente para aceptar eventos generados por los dispositivos que soporten SNMP en la red.
- Personal para mantener los dispositivos que soportan SNMP. Este grupo incluye el aseguramiento a los *switches*, *routers*, servidores y estaciones de trabajo que se comunicarán con la estación de gestión.
- Personal encargado de solucionar los problemas que ocurran en la red. Este grupo es usualmente conocido como NOC (*Network Operations Center*) y es de tipo 24x7 es decir que debe estar disponible durante las 24 horas de los siete días de la semana. En redes extensas o complejas generalmente se implementan turnos en los cuales no todas las personas deben estar físicamente en la oficina, pueden estar en su casa pero siempre localizables.

Los grupos definidos aquí han pasado la "prueba del tiempo" y han demostrado ser la solución perfecta para muchas de las redes existentes, pero esto no significa que sea el único patrón existente, en redes pequeñas puede ser que solo una persona esté capacitada para resolver todos los problemas que existan. También hay redes donde lo importante no es una solución rápida del problema sino una atención al personal que usa la red, en ese caso debe crearse una cuarta división que estaría compuesta por las personas que deben dar las explicaciones y las atenciones que los usuarios requieran. [Mauro, 2001]

Se aconseja además la superación profesional de cada uno de los miembros de estos grupos de trabajo en las tareas y objetivos que cumplen los demás miembros, con la finalidad de tener mayor área de cobertura en cuanto a personal capacitado para todo tipo de trabajo, este aspecto debe ser un elemento importante a considerar por parte de la empresa o entidad en cuestión.

I.2.2 Protocolo SNMP. Características.

SNMP es un protocolo de comunicación que ha ganado una gran aceptación desde 1993 como un método para la gestión de redes basadas en TCP/IP. SNMP fue desarrollado por la IETF (*Internet Engineering Task Force*), hoy en día es también aplicable a otras redes que no están basadas en TCP/IP como IPX/SPX.

Sobre SNMP existe una inmensa cantidad de bibliografía que lo describe. La razón es que constituye un protocolo relativamente viejo, que ha sido revisado en varias ocasiones y se le han incorporado muchas mejoras desde su definición inicial. Uno de los primeros libros que describió SNMP en detalle fue "*The Simple Book*" escrito por Marshall T. Rose [Rose, 1992] y que fue publicado a principio de los años 90. Este libro estableció un método para la aplicación de SNMP en las redes de computadoras que aún hoy es respetado y referenciado. [Westerinen, 2003]

El protocolo SNMP está definido sobre un modelo cliente/servidor. El programa cliente, también conocido como administrador de red (*Network Manager*) o estación administrativa (*Network Management Stations*) crea conexiones virtuales hacia un programa servidor llamando *SNMP agent* (agente de SNMP) el cual se ejecuta en un dispositivo de red remoto y brinda información al *manager* sobre su estado. La base de datos, controlada por el agente es conocida como MIB (*Management Information Base*) y es un grupo estándar de valores con fines estadísticos o de control. SNMP permite la extensión de estos valores considerados estándares con variables que sean específicas a un agente a través de la definición de una MIB privada. [Stallings, 1998]

Las directivas enviadas por el cliente a un agente de SNMP consisten en los identificadores de las variables de SNMP, también conocidas como variables MIB o identificadores de objetos de una MIB (MIB object identifiers) y en una instrucción de pedir el valor (*get*) o de establecer el valor (*set*).

A través del uso de variables MIB privadas los agentes de SNMP pueden ser hechos a la medida para un gran número de dispositivos, tales como *bridges*, *gateways*, y *routers* sin que importe qué fabricante los creó. La definición de variables para MIB soportadas por un agente particular es incorporada al programa de administración a través de ficheros escritos en ASN.1 (*Abstract Syntax Notation*), lo cual hace posible que exista independencia entre el fabricante del dispositivo y el creador del programa de administración. [Thottan, 2003].

El esquema representado en la Figura 1 resume lo explicado anteriormente.

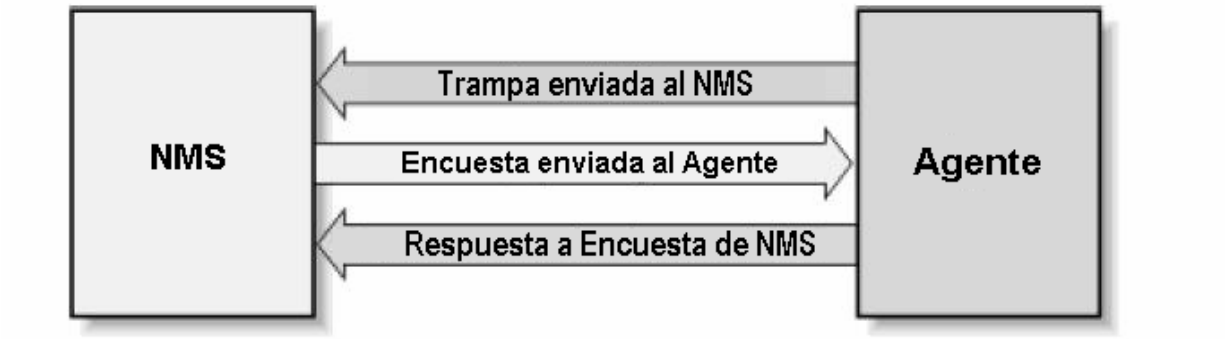


Figura 1: Relación entre un NMS y un Agente.

I.2.3 Ventajas y desventajas de SNMP

SNMP tiene muchas ventajas, pero la principal es su popularidad y ese es uno de los elementos que más ayuda a su homogeneidad en los equipos de comunicación. Los agentes de SNMP se pueden encontrar disponibles en dispositivos que van desde computadoras, *bridges*, MODEM, impresoras hasta *switches* y *routers*. El hecho de que existan tantos dispositivos que soportan SNMP es una razón que da una considerable credibilidad a su existencia. Adicionalmente, SNMP es un protocolo muy flexible y extensible. Esto se explica por la capacidad que tienen los agentes de extender su soporte a dispositivos muy específicos y por la completa capacidad que tiene un programa que se use como *manager* de un *switch* de ser, a la misma vez *manager* de una impresora. [Thottan, 2003].

Pero como toda obra, realizada por humanos, SNMP no es perfecto, tiene algunas debilidades y defectos. Al contrario de como su nombre especifica: (*"Simple" Network Management Protocol*), SNMP es un protocolo muy complicado de implementar. Una confesión de sus diseñadores admite que un nombre un poco más justo sería "*Moderate Network Management Protocol*" [Mauro, 2001] aunque incluso así no se haría justicia al nivel de complicación que implican las reglas de codificación que se usan.

SNMP tampoco es un protocolo muy eficiente si se compara con otros existentes en Internet como por ejemplo HTTP y FTP. Este genera mucho tráfico que ocupa el canal de datos existente con información que no es de ninguna necesidad, como la versión del protocolo que se está usando. [Thottan, 2003].

A las desventajas citadas se sumaba otra muy común, que era la de la falta de seguridad pero este problema ya fue resuelto en una de sus versiones posteriores.

Resumiendo se puede decir que si bien es una labor muy frustrante para los programadores crear aplicaciones que usen SNMP, debido a la complejidad de los algoritmos usados y a las estructuras de datos necesarias, todo esto se ve recompensado por la facilidad con la que los usuarios finales controlan y supervisan los dispositivos que se desean gestionar. Esto hace que las desventajas de SNMP como protocolo queden en un segundo plano respecto a las ventajas que de su uso se derivan.

I.2.4 Versiones de SNMP

De los estándares que se han dictaminado para SNMP tenemos tres versiones, las cuales se mencionan con algunos de los elementos que las identifican:

- SNMP Versión 1 (SNMPv1): es la versión estándar del protocolo SNMP. Está definida en la RFC 1157 y es un estándar completo de la IETF. La seguridad de SNMPv1 se basa en comunidades, que no son más que palabras claves, cadenas de

caracteres en texto plano que permiten a las aplicaciones basadas en SNMP ganar acceso a la información del dispositivo gestionado. Existen tres tipos de comunidades en SNMPv1: *read-only* (solo lectura), *read-write* (lectura escritura) y *trap* (trampa).[Stallings,1998]

- SNMP Versión 2 (SNMPv2): técnicamente referenciada como SNMPv2c, descrita en la RFC 1905, la RFC 1906 y la RFC 1907. [Stallings,1998]

- SNMP Versión 3 (SNMPv3): las especificaciones de esta versión fueron aprobadas, por la comisión internacional de estándares, como un estándar de Internet en marzo del año 2002; en ella se adicionan capacidades para el uso de métodos mucho más seguros para la autentificación y la comunicación entre las entidades involucradas así como para la administración remota. La versión está definida en las RFC 1905, 1906, 1907, 2571, 2572, 2573, 2574 y la RFC 2575.

En la red de UCLV no se cuenta con ningún equipamiento que soporte SNMPv3, todos los existentes soportan hasta la versión dos de este protocolo, cuestión esta por la cual no se abordan con profundidad los elementos incluidos en la versión tres.

Aunque generalmente se ve como algo muy lejano, el hecho de comprender realmente todo lo escrito y planteado en las RFC es ciertamente muy necesario a la hora de enfrentar el análisis de cualquier problema en el mundo de las redes IP con un nivel científico medianamente alto. Ver **Anexo I.**

I.3 El protocolo SNMP.

Hasta el momento se ha dado una idea de lo que es SNMP y de lo que representa para el mundo de la gestión de redes. En lo adelante se mostrará cómo es que realmente funciona este protocolo.

SNMP usa UDP (*User Datagram Protocol*) como protocolo de transporte para intercambiar datos entre el NMS y el agente. El protocolo UDP está definido en la [RFC 768] y fue elegido para su uso porque no es orientado a conexión. Esto significa que no existe una conexión de extremo a extremo o *end-to-end* por donde los datos puedan ser enviados y recibidos. Esta característica de UDP lo hace más confiable porque no hay nunca un reconocimiento de que se pierden paquetes. Corresponde solo a las aplicaciones determinar si se están perdiendo paquetes o no, y si se puede tolerar esto o no sin dar una alarma. El método más usado generalmente es el de esperar un intervalo de tiempo por los datos (*timeout*). [RFC-1067]

Si se analiza la implicación que tiene la selección de UDP en la supervisión de un dispositivo se verá que no es mucha ya que si falla un paquete la estación administrativa (NMS) puede solicitarlo de nuevo y resolver así el problema, no ocurre lo mismo en el caso de las *traps*, las cuales se originan en el agente y este al no saber si el *manager* recibió o no los datos nunca los envía de nuevo. Por otro lado UDP representa una carga más ligera para el tráfico de la red que una conexión TCP. Existen implementaciones de SNMP sobre TCP pero son usadas en casos de agentes muy específicos. El uso de este tipo de agentes en una red de mucho tráfico no es una buena idea. Pero debe significarse que SNMP está diseñado para ser usado en redes con problemas, redes en las cuales la comunicación entre dos dispositivos es algo que puede fallar en cualquier momento, es en ese ambiente donde UDP ha demostrado su superioridad sobre TCP y si la red no fuera inestable: ¿para qué usar SNMP?

El protocolo SNMP usa por definición el puerto 161 para enviar y recibir peticiones y datos y el 162 para las *traps* [RFC-1067]. En muchas implementaciones el número del puerto puede ser cambiado pero es bueno recordar que los estándares deben ser respetados y cumplidos y que la uniformidad de la red es algo que acelera la solución de los problemas. La Figura 2 muestra la relación que existe entre SNMP, UDP e IP.

Cuando el agente o el NMS desean hacer una operación de SNMP, ya sea solicitar o establecer un valor, ocurren en las diferentes capas de este modelo (Figura 2) las operaciones siguientes:

- Aplicación (*Aplication*): La aplicación de SNMP (agente o NMS) decide qué es lo que quiere hacer, por ejemplo solicitar el valor que representa la cantidad de *bytes* enviados por una de las interfaces de un *switch*.
- UDP: Esta capa le permite a la estación que se está usando para gestionar la red comunicarse con el dispositivo que se va a encuestar. Por lo que un paquete tipo UDP es enviado al puerto 161 del *switch*.
- IP: La capa IP solo debe de tratar de entregar ese paquete a la dirección IP que tiene el dispositivo que se desea encuestar; el *Switch*, en el caso que nos ocupa.

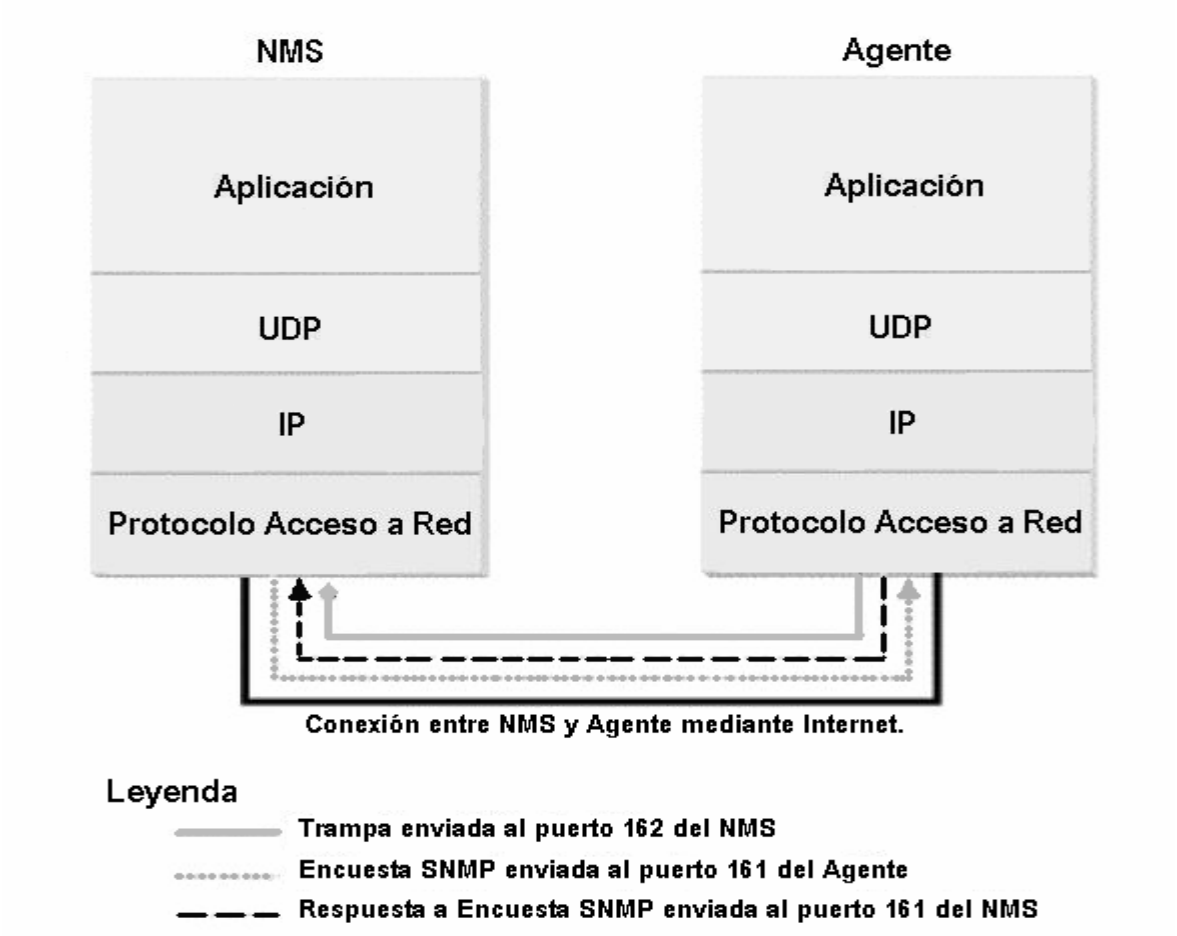


Figura 2: Funcionalidad entre TCP/IP y SNMP.

Todo este proceso y las funcionalidades de las tres capas inferiores que se muestran en la Figura 2 están perfectamente detallados en [Mauro, 2001].

I.3.1 Comunidades de SNMP

Las versiones SNMPv1 y SNMPv2 usan el concepto de comunidad para establecer la relación entre el *manager* y el agente. Un agente está configurado con tres nombres de comunidades: *read-only*, *read-write* y *trap* tal como se mencionó anteriormente. Los nombres de las comunidades son básicamente claves, no hay ninguna diferencia entre ellas y la clave que se usa por ejemplo para acceder a una computadora. Como sus nombres lo indican estas tres comunidades representan y permiten tres formas diferentes de interactuar con los datos. [RFC-1157][RFC-1905]

Muchos fabricantes de equipos que soportan SNMP brindan sus dispositivos con una comunidad llamada *public* que representa datos de solo lectura (*read-only*). Es muy importante cambiar este identificador cuando el equipo va a instalarse en un ambiente abierto por las implicaciones de seguridad que esto representa. Cuando se está configurando un agente de SNMP se puede establecer también el destino de las *traps* que no es más que la dirección IP a donde son enviados los avisos por parte del agente. Es una buena práctica enviar *traps* cuando alguien intente solicitar información especificando una comunidad errónea. Esto ayudaría mucho a la hora de determinar si hay intrusos tratando de acceder a recursos en la red.

El método a seguir para seleccionar el nombre de las comunidades puede ser similar al de elegir una clave para un servidor Windows o UNIX. Una combinación de números y letras en la mayoría de los casos bastará. Claro que el hecho de que el nombre de las comunidades viaje en texto plano por la red y en todos los paquetes enviados hace que sea muy fácil obtenerlo si así se desea. Para solucionar este problema SNMPv3 permite la

creación de canales seguros y de la necesidad de autentificación entre las entidades que desean intercambiar datos. Lamentablemente SNMPv3 [RFC-3411] no está tan ampliamente distribuido como las versiones anteriores, en estos casos se puede minimizar el riesgo de ataques usando *firewalls* o filtros que permitan solo el intercambio de paquetes UDP entre los agentes y el NMS evitando así que cualquier otra estación pueda enviar pedidos u ordenes a los agentes que existen.

Es bueno resaltar la idea de que todo lo que se logra con SNMP puede volverse un arma de doble filo cuando no se toman, o se practican mal, las medidas de seguridad necesarias y pertinentes. Esto es una de las responsabilidades más importantes del personal encargado de la configuración de los agentes de SNMP y no debe ser olvidada bajo ningún concepto.

Hasta este momento se ha referenciado la información que se intercambia entre agentes y NMS como datos. Estos datos son en realidad una de las partes más oscuras de SNMP. La forma en que ellos se definen y se organizan es un aspecto de enorme importancia para lograr una comprensión del protocolo SNMP. Para profundizar sobre el tema se ha dedicado el **Anexo II** a este tema

I.3.2 Extensión de la MIB.

Con el paso del tiempo los objetos definidos en la MIB estándar resultaron insuficientes para cubrir las necesidades que surgían al adicionar nuevas ideas a los trabajos relacionados con gestión de redes de computadoras. Es por ello que se define una extensión que ofrecía nuevos grupos de objetos: MIB-II por tanto una adición de nuevas “ramas” al árbol.

La MIB-II (*Management Information Base Second Part*) es un grupo muy importante de objetos gestionables porque cada dispositivo que soporte SNMP debe también soportarlos. En esta MIB se recoge información básica que cualquier agente debe brindar como, por ejemplo, cantidad de interfaces, cantidad de *bytes* enviados y recibidos. Esta MIB se

encuentra en detalle en la RFC 1213. Dada la importancia de este aspecto es bueno aclarar que un agente puede soportar varias MIBs, como por ejemplo una para ATM (RFC 2515), o la especificada en la RFC 1611 relacionada con servidores de DNS pero es de carácter obligatorio que soporte la MIB II. [Breitgand, 2002].

I.3.3 Operaciones en SNMP

Se ha visto como SNMP organiza la información, pero no se ha explicado cómo se hace la solicitud y la entrega de esta. El PDU (*Protocol Data Unit*) es el formato del mensaje que los *managers* y los agentes usan para enviar y recibir información. Existe una estructura de paquete estándar para cada una de las operaciones posibles. Estas son las que en realidad hacen todo el trabajo en una red gestionable. Las operaciones existentes son:

- get
- get-next
- *get-bulk* (SNMPv2 y SNMPv3)
- set
- *get-response*
- trap
- *notification* (SNMPv2 y SNMPv3)
- *inform* (SNMPv2 y SNMPv3)
- *report* (SNMPv2 y SNMPv3)

Todas estas operaciones se explican ampliamente en las RFCs correspondientes a las distintas versiones de SNMP y en la casi totalidad de los libros escritos al respecto. Una explicación muy clara y con ejemplos prácticos puede ser encontrada en [Mauro, 2001].

I.4 Protocolo de Monitoreo Remoto (RMON).

Cuando un administrador de red implementa el uso de conmutadores para redes LAN, sin soporte para sistemas de monitoreo remoto, con el objetivo de mejorar el desempeño de la

red, se encuentra que la solución puede ser una espada de doble filo, esto es debido a que los mismos conmutadores impiden supervisar el tráfico que circula a través de ellos, dada la ausencia del soporte para el monitoreo remoto. Esta falta de visibilidad de la red constituye una traba a la hora de optimizar el desarrollo de la red troncal en cuestión y de poder prevenirla de fallas en el futuro.

Durante años, se han estado utilizando analizadores de redes de ordenadores para supervisar el uso de la misma y solucionar los problemas que pueden surgir con el paso del tiempo. Para asegurar la lectura exacta de los datos de tráfico, los primeros analizadores de la red tuvieron que ser atados físicamente a la parte de la red, designada como objetivo de supervisión, para evitar la perdida de información importante que podría filtrarse por puentes o enrutadores, lo cual podría ser bien incomodo y poco efectivo; ahora bien, con el fin de ayudar o facilitar la actividad remota y solucionar estos inconvenientes se reforzaron los analizadores de la red subsecuentes para relevar los datos manejados a ciertas consolas centralizadas que se introducirían con un papel bien importante dentro de la administración y gestión de redes de computadoras. [Chen, 2002].

Un sistema de RMON básico, según RFC-1757, puede proporcionar datos tales como:

- Información que permite a administradores realizar análisis de utilización de la red, incluyendo datos y estadísticas del error.

- Información histórica para sospechar sobre la tendencia de la red y el análisis estadístico de la misma.

- Información de matrices que describen las comunicaciones entre los sistemas y la cantidad de datos intercambiados por entidades de estos sistemas.

La especificación de RMON define un grupo de estadísticas y funciones que pueden ser intercambiadas entre dispositivos que soporten este protocolo. Actualmente existen dos versiones de RMON [Stallings, 1998].

La primera versión: RMONv1 brinda a los NMS estadísticas a nivel de paquetes sobre la LAN o la WAN. La segunda: RMONv2 brinda no solo información al nivel de red sino que dispone de datos a nivel de aplicaciones. Estas estadísticas pueden ser reunidas de varias formas, una de ellas es situando "Sondas RMON" en cada uno de los segmentos de la red que se desee monitorear.

Otra de las ventajas de RMON es que se pueden ejecutar hilos que chequeen por ciertas condiciones y en caso de la ocurrencia de un error o de una alerta se avisa al NMS a través de una *trap*.

Para una mayor información pueden ser usadas las RFC-1757, 2021 y la 2819 además del libro "*SNMP, SNMPv2, SNMPv3, and RMON 1 and 2*" de William Stallings.

I.4.1 Objetivos de la Administración Remota.

A continuación brindamos algunos de los elementos que justifican la administración remota y sus objetivos.

- *Operación fuera de línea.* Existen ciertas condiciones en las que una estación supervisora no esta en contacto directo con el dispositivo de gestión al cual se debe de remitir los datos, este tipo de situación se presenta generalmente a causa de enlaces con bajas tasas de transferencia (WAN o enlaces telefónicos) y en los cuales los costos en la transferencia son bastante altos, o por fallas en la red que ocasionan la falta de comunicación entre la sonda y la estación administrativa.

Por esta razón la MIB que trata con RMON permite la existencia de unas sondas, que son configurables, para efectuar diagnósticos y recolectar estadísticas constantemente, aun cuando la comunicación no sea posible o eficiente. Estas sondas pueden notificar eventos y reportes a la estación de administración cuando ocurre una situación excepcional, incluso en circunstancias anómalas para la conexión [RFC-1757].

- *El dispositivo monitor de eventos se comporta de manera activa la mayor parte del tiempo.* En dependencia de los recursos con los cuales cuenta este dispositivo es altamente potencial que se mantenga constantemente realizando diagnósticos para registrar los eventos del desarrollo de la red, de esta manera se puede efectuar con más facilidad la notificación al administrador y se puede realizar, incluso, historiales estadísticos.

- *Detección de problemas y reportes.* El dispositivo monitor puede configurarse para reconocer condiciones que denoten la existencia de errores, y por consiguiente chequear de modo sistemático estas condiciones; cuando una de ellas se cumple entonces conlleva al registro de un evento de error que puede ser notificado mediante varias vías al centro de información.

- *Múltiples estaciones administradoras.* Se crean con la finalidad de colocar varias estaciones con el mismo objetivo funcional, de manera que se pueda proveer una recuperación de desastres. [RFC-2021].

I.4.2 Estructura de la MIB

La MIB de RMON fue diseñada para permitir a las sondas de RMON trabajar sin necesidad de contactar al NMS durante un periodo de tiempo el cual aprovechan para recolectar información. Luego la NMS puede solicitar esa información a la sonda RMON.

A continuación se muestran algunos de los grupos que conforman la MIB implementada para RMON, la formación de estos, dentro del estándar, implica la reunión de cada uno de los objetos racionalizados por funciones, y por tanto el agente que implemente el uso un

grupo debe implementar todos y cada uno de los objetos contenidos dentro de este, es importante aclarar que el uso de un grupo u otro puede ser opcional en dependencia del grupo al que sea haga referencia. [RFC-1757].

- *Estadísticas de Ethernet (Ethernet Statistics).* Este grupo contiene datos estadísticos medidos por la sonda para cada interfase Ethernet que contenga el dispositivo, consiste de una tabla de estado de Ethernet (etherStatsTable). En el futuro se deben definir otros grupos para distintos tipos de medios como Token Ring o FDDI, los cuales deben seguir el mismo modelo utilizado en este grupo en cuestión.

- *Control Histórico (History Control).* Este grupo controla el muestreo estadístico y periódico de los datos para distintos tipos de redes, este grupo consiste en una tabla de historial de control (historyControlTable).

- *Alarmas (Alarm).* En este grupo se toman muestras sistemáticas de algunas de las variables que se toman en cuenta en la sonda y las compara con niveles umbrales preestablecidos. Si la variable comparada cruza el nivel umbral se genera un evento. Este grupo consiste de una tabla de alarmas (alarmtable), y requiere de la implementación obligada del grupo de eventos (event group).

- *Ordenador (host).* Este grupo contiene información relacionada con cada ordenador encontrado en la red, este grupo descubre ordenadores en la red a partir de direcciones MAC de origen y destino que obtiene a partir de paquetes recibidos en modo promiscuo. El grupo consiste de una tabla de control de ordenadores (Hostcontroltable), una tabla de ordenadores (Hostable) y una tabla de tiempo de ordenadores (Hostimetable).

- *Grupo de Ordenamiento por Variables (Hostopn).* En este grupo se tienen los anfitriones ordenados según una variable, esto se hace a partir de las bases de datos de cada uno de los anfitriones, además, la estación administrativa puede hacer

pedidos limitados en la tabla ordenada, cuando el interés se destina a una parte especifica de la tabla manipulada, por ejemplo los veinte primeros que cumplan con una condición enviada por la estación. Este grupo consiste de la tabla de control de ordenamiento (hostTopNControlTable) y de la tabla de ordenamiento (hostTopNTable), y requiere de la implementación del grupo de ordenadores (hostgroup).

- *Grupo Matriz (Matrix).* Este grupo contiene estadísticas sobre conversaciones entre grupos de dos direcciones, cuando el dispositivo de monitoreo detecta una conversación entre entidades añade una entrada a la tabla de matriz. En este grupo se manejan tres tablas: matrixControlTable, matrixSDTable y matrixDSTable.

- *Grupo filtro (filter).* Este grupo permite que los paquetes sean filtrados según una ecuación predeterminada, de esta manera se puede racionalizar los paquetes que se pueden capturar o que pueden generar eventos. Este grupo consiste de las tablas de filtro (filtertable) y la tabla de canal (channeltable).

- *Grupo de Evento (Event).* Este controla la generación y notificación de los eventos del dispositivo monitor. Este grupo consiste de dos tablas, la tabla de eventos (eventable) y la de de registros (logtable).

I.4.3 Control de los Dispositivos de Monitoreo Remoto.

Producto de la naturaleza compleja de las funciones disponibles en los dispositivos de monitoreo, estas, a menudo necesitan de la configuración por parte del usuario o administrador; en muchos casos requieren de parámetros que deben ser asistidos para la operación de recolección de datos. Por tanto solo se puede proceder a recolectar los datos estadísticos después que se hayan establecido estos parámetros. [Chen, 2002].

Muchos de los grupos funcionales en la base de datos de administración (MIB) presentan una o más tablas que se usan para colocar o especificar los parámetros de control, además de otras tablas en las cuales se colocan los datos resultados de las operaciones. Las tablas de control con regularidad son de tipo lectura-escritura, mientras que las tablas de datos son solo de lectura, esto se debe a que los parámetros en las tablas de control con frecuencia describen resultados de los datos leídos en las tablas de datos, por tanto estos parámetros se pueden cambiar en el caso en que no se obtenga lo requerido por el usuario.

Algunos de los objetos en la base de datos proveen un mecanismo que les permite ejecutar acciones en los dispositivos de monitoreo. Estos objetos pueden ejecutar una acción como resultado del cambio en el estado del objeto; aclaremos que para estos objetos, el cambio de estado hacia el mismo estado no constituye una alteración, por tanto no resulta en una acción por parte del objeto.

Para facilitar el control mediante múltiples estaciones administradores, se deben compartir algunos de los recursos como son la memoria y las posibilidades de procesamiento que una función pudiera necesitar, por lo que el uso de estos recursos debe ser racionalizado y suministrado con cautela.

I.4.4 Manejo de Recursos entre NMS.

Cuando múltiples estaciones desean usar funciones que compiten por una cantidad limitada de recursos en un dispositivo se necesita un método para facilitar el compartimiento, puesto que pueden surgir algunos conflictos indeseables como:

- Dos o más estaciones administrativas desean usar simultáneamente recursos en un dispositivo, y juntos pueden exceder la capacidad del dispositivo.

- Una estación administrativa puede usar una cantidad excesiva de recursos durante un tiempo significativamente grande de tiempo.

- Una estación utiliza cierta cantidad de recursos y de pronto falla, olvidando liberar los recursos abarcados para que otras estaciones puedan hacer uso de estos.

Existe un mecanismo que se provee en cada función que se inicia en las estaciones para evitar estos obstáculos, y para ayudarles a resolverlos en caso de que ocurran. Cada función tiene una etiqueta identificando un inicializador (propietario) de la propia función. Esta etiqueta es colocada con varios objetivos.

- Una estación administrativa debe ser capaz de reconocer recursos por si misma, y de no necesitar de actividades terciarias.

- Un operador de red puede encontrar la estación administrativa a la cual pertenece el recurso en uso y negociar con esta para poder liberarlo.

- Puede existir compartimiento de permisos dentro del dispositivo gestionado, o sea, un operador de red puede decidir liberar recursos que otro operador no haya liberado y que no sean utilizados.

- Una vez efectuada la inicialización, una estación puede reconocer recursos que esta haya reservado en el pasado, con esta información, puede liberarlos si no los necesita por el momento.

Las estaciones administrativas y las sondas deben soportar cualquier formato de las cadenas del propietario dictadas por las políticas tomadas en las organizaciones pertinentes. Se sugiere el uso de algunos de los campos como la dirección IP, nombre de la estación administrativa, nombre del administrador de red, ubicación, o numero telefónico. Esta información es utilizada para compartir los recursos con mayor efectividad.

Los recursos en las sondas son escasos, y son destinados generalmente cuando se crean líneas de control por aplicaciones. Existen casos en los que pueden coexistir varias

aplicaciones haciendo uso de una misma sonda, la reservación indiscriminada de recursos hacia estas aplicaciones puede ocasionar escasez de los mismos en las sondas, provocando su inutilización o inactividad en un momento determinado.

I.5 Arquitecturas de NMS

Hasta este momento se han abordado las generalidades del SNMP como protocolo para supervisar y controlar una red, ahora, es necesario abordar algunas temáticas sobre las estaciones de administración.

Existen algunos aspectos relacionados al hardware que deben ser tomados en cuenta. Las redes de hoy en día cuentan en algunos casos con miles de nodos y la estación encargada de encuestar al resto deberá disponer de la velocidad y la capacidad suficiente para realizar su labor. Por ejemplo encuestar 1000 nodos cada minuto y obtener de ellos 1Kb de datos generará 1Mb de datos, 1.4Gb por día. Un disco de 40Gb se podría llenar en un mes.

En el ejemplo citado anteriormente el intervalo de 1 minuto tal vez parezca un poco pequeño, no hay necesidad de encuestar a todas las máquinas de una red y mucho menos de guardar todos los datos relacionados con ellas, no obstante, la opción del intervalo de tiempo pequeño o tal vez no tan pequeño es un recurso manejado por los administradores de red, y depende de los objetivos que prevalezcan en el momento en que se cuestione la configuración del sistema de supervisión, por esto no deben ser tomadas a la ligera las prestaciones de la estación que se elija para NMS, este es uno de los puntos claves en un sistema de gestión, además ¿cómo se puede esperar conocer si una red es estable si la estación de control es inestable?

La selección de la estación también dependerá de la arquitectura que se elija, en la Figura 3 se muestra un ambiente de gestión centralizado, donde solo una NMS se encarga de encuestar a todas las estaciones de la red. [Chen, 2002].

Esta arquitectura tiene la ventaja de que una sola persona puede controlar la red desde un solo punto eso representa ahorro de personal y de salarios, el gran problema es que si el número de nodos es muy grandes la capacidad de la NMS deberá aumentarse para soportar los niveles de procesamiento exigidos.

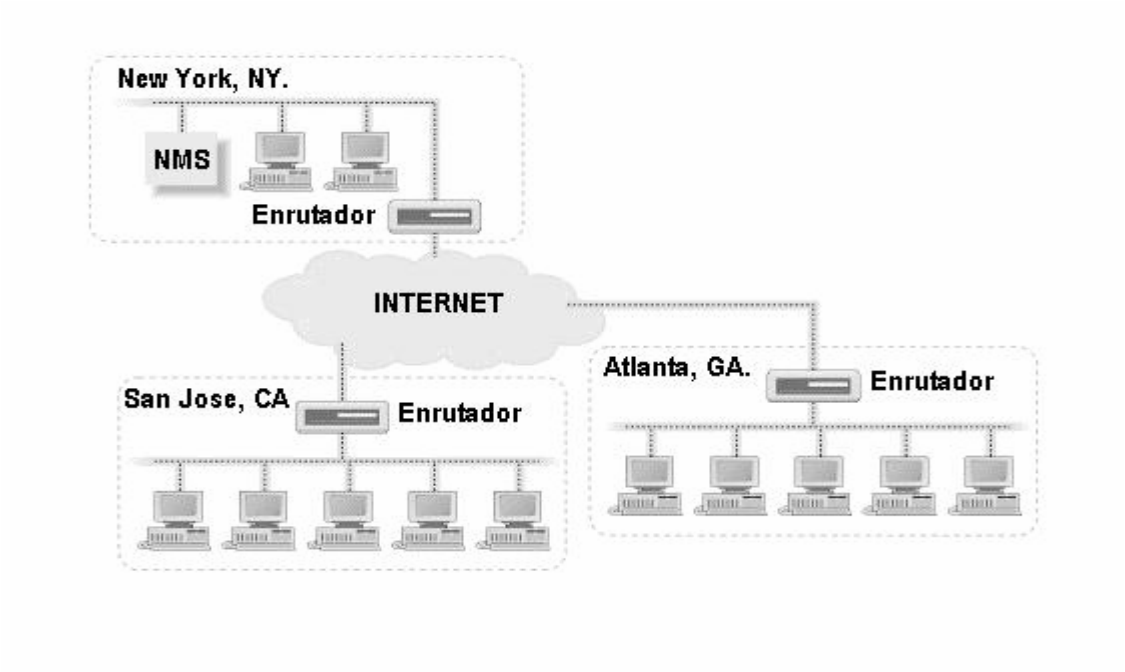


Figura 3: Arquitectura centralizada.

El tráfico generado es otro de los aspectos negativos de esta arquitectura pues el enlace que incluya a la NMS puede verse saturado si la cantidad de nodos crece desesperadamente. [Chen, 2002].

Una solución al problema anterior es usar una arquitectura distribuida (ver Figura 4).

Las ventajas de esta solución hacen que sea la más usada, no solo porque resuelve las limitaciones de la configuración anterior sino que crea una estructura muy robusta, ya que en caso de rotura de uno de los NMS, los restantes pueden asumir sus responsabilidades.

Esta variante tiene al menos una desventaja y es que las NMS pueden necesitar en algunos casos comunicarse entre ellas si solo se controla desde una estación, en ese caso el tráfico

vuelve a ser un problema. La solución más común se relaciona con el establecimiento de canales privados solo para las estaciones de control, estos enlaces no suelen ser de muy alta velocidad si solo se van a usar para el intercambio de paquetes SNMP.

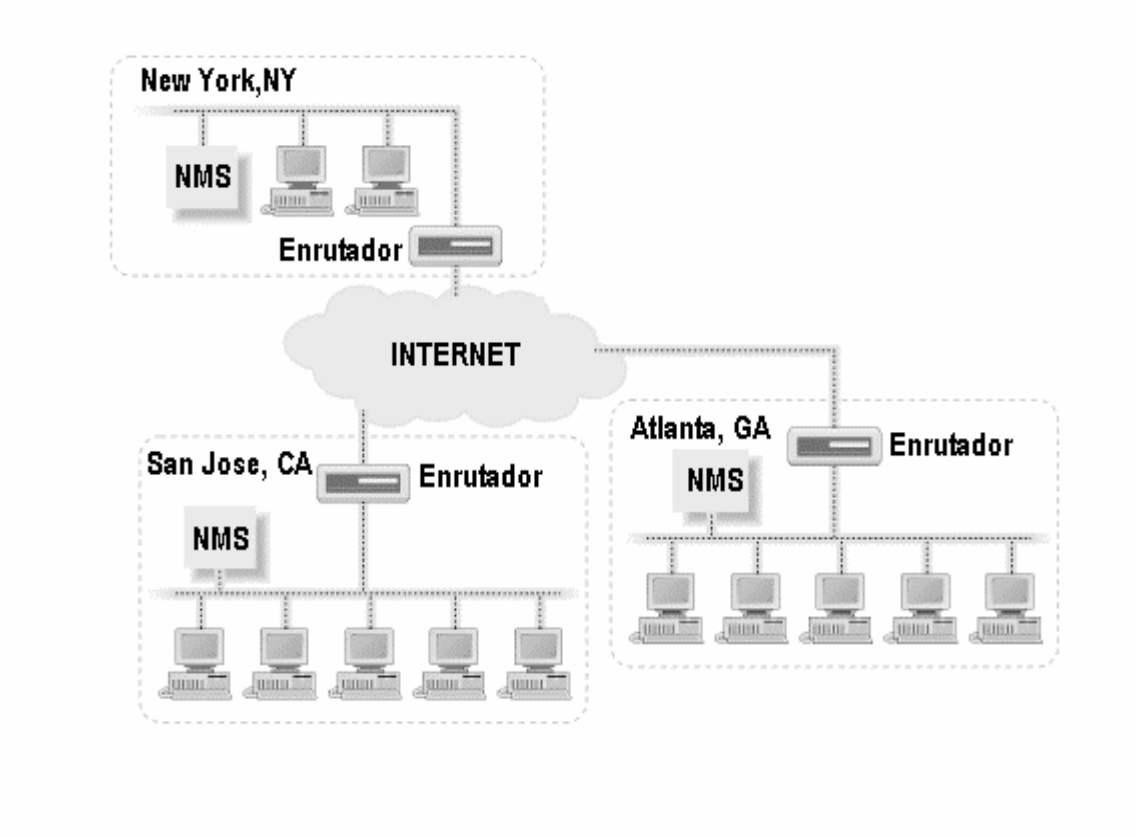


Figura 4: Arquitectura Distribuida.

I.6 Software de Gestión

Otro de los elementos que existen en una cadena de gestión son los programas que soportan SNMP. Estos pueden estar del lado de los agentes o del lado de las estaciones de control. Es importante realizar un proceso de selección muy cuidadoso a la hora de elegir los paquetes que se van a usar, (en caso de no estar satisfecho con los existentes) o la creación de uno adaptado a necesidades específicas.

En el mercado y en la comunidad de software libre de Internet existe una gran variedad de programas que soportan SNMP, construidos sobre diversas plataformas y usando lenguajes de programación de diferentes tipos, desde ANSI-C hasta Visual Basic.Net. Algunos de estos son libres otros no, algunos son gratis otros no, unos solo ocupan cientos de *kilobytes* y otros llegan a *gigabits*. El proceso de selección no es sencillo, pero debe ser realizado con la mayor seriedad posible porque la opción que sea elegida jugará un papel determinante en la estabilidad de la red.

I.6.1 Agentes de SNMP

Como se mostró anteriormente los agentes son los programas encargados de la comunicación desde y hacia los dispositivos de SNMP. En el caso que nos ocupa, los equipos adquiridos para la interconexión de las subredes de las facultades son capaces de soportar agentes SNMP que brinda el mismo propietario de la firma dentro del aparato, el cual es posible de activar y configurar de forma relativamente fácil.

I.6.2 Estaciones de Gestión

Los paquetes que cumplen con las necesidades de un NMS generalmente agrupan varios programas individuales que realizan funciones específicas. Los NMS en la mayoría de los casos permiten la visualización gráfica de las estaciones y de los agentes que pertenecen a la red. También controlan las formas de alarmas y la creación de reportes que permitan un estudio del comportamiento de la red. También es un punto importante a tener en cuenta a la hora de seleccionar un NMS el soporte que brinda a los dispositivos que se tienen en la red, para lograr de ellos un máximo aprovechamiento. [Chen, 2002]. Para el montaje de la red de gestión se utilizaran los que mostramos a continuación.

- Castle Rock SNMPc
  Plataforma: Windows NT/2000

Ventajas: orientado a redes pequeñas y medianas. Contiene todo lo necesario en un NMS. El precio es razonable y existen suficientes *plug-ins* para soportar

Desventajas: la construcción de los mapas de la red puede resultar un poco difícil.

- Nagios

  Plataforma: LINUX

  Ventajas: no está solo orientado a chequeos basados en SNMP, soporta gran cantidad de *plugins* que permiten extender y adaptar su funcionamiento a condiciones muy específicas.

  Desventajas: Resulta un complicado a la hora de configurar.

I.7 Equipamiento para gestionar una Red

El equipamiento es el último punto de la cadena de un sistema de gestión, pero no por eso deja de ser uno de los más importantes. Gracias a la especificación del protocolo SNMP todos los dispositivos que lo soportan pueden intercambiar información entre ellos. Eso permite que se puedan adquirir equipos de varios fabricantes sin temor a incompatibilidades, aunque existe una política muy generalizada de comprar la mayoría de los dispositivos a una misma firma. La tendencia a los sistemas homogéneos se ha creado porque existen muchas opciones extras que cada fabricante se reserva el derecho de activar cuando los demás elementos del sistema de gestión son también de su propiedad.

Allied Telesyn es el único fabricante de equipamiento compatible con SNMP que se abordará en este trabajo porque fue el seleccionado para perfeccionar la estructura de la Red de la UCLV. En el **Anexo III** se brinda información relacionada a esta firma.

I.7.1 Ethernet en la capa 3

Tanto las soluciones de *switches/routers* de nivel 3 de sobremesa como las modulares basadas en los chasis de *Allied Telesyn*, están diseñadas para proporcionar plataformas de conmutación multinivel de alto rendimiento, para conexión en la red principal y para equipos de sobremesa y grupos de trabajo a velocidades que pueden llegar hasta 1 *Gigabit*. Por ejemplo el *switch* Rapier 24i de nivel 3 es capaz de agregar circuitos E1/T1 y E3/DS3 a *Ethernet*, añadiendo la capacidad de control de ancho de banda por puerto para limitar la velocidad.

I.8 Consideraciones finales

En este capítulo se ha abordado la gestión de redes y lo que representa. Se ha visto que la estructura de gestión está formada por un agente, una estación de gestión y el protocolo que hace posible esta comunicación. El protocolo más usado es el SNMP, que ha resistido el paso del tiempo gracias a su facilidad para ser usado haciendo que los complicados detalles de su diseño queden relegados.

La información que los agentes manejan es estándar y está reglamentada en MIBs, aunque cada fabricante se reserva el derecho de extenderla usando sus propios OIDs. Esto permite que una gran variedad de programas de gestión puedan ser utilizados con equipos de distintos fabricantes, aunque una buena recomendación es mantener la uniformidad tanto en software como en hardware dentro de la red.

Desde el punto de vista teórico se dispone de todos lo elementos necesarios para enfrentar la tarea propuesta en este proyecto. En el próximo capítulo se comienza a modelar una solución.

Capítulo II: Evolución de la estructura del *Backbone* UCLV.

I.1 Estado actual de la infraestructura de la red universitaria.

La red de la UCLV, diseñada y planificada en el año 1998, se instalo a principios del año 2000, esta presentaba una topología estrella, e implementaba tecnología *FastEthernet*. Desde un principio ha sido el centro de esta arquitectura un *SWITCH* modular capa3 *LanMaker 5000*, de fabricación israelita.

Las conexiones realizadas en el inicio propiciaron que la estructura de que la red de datos quedara como muestra la figura 5:

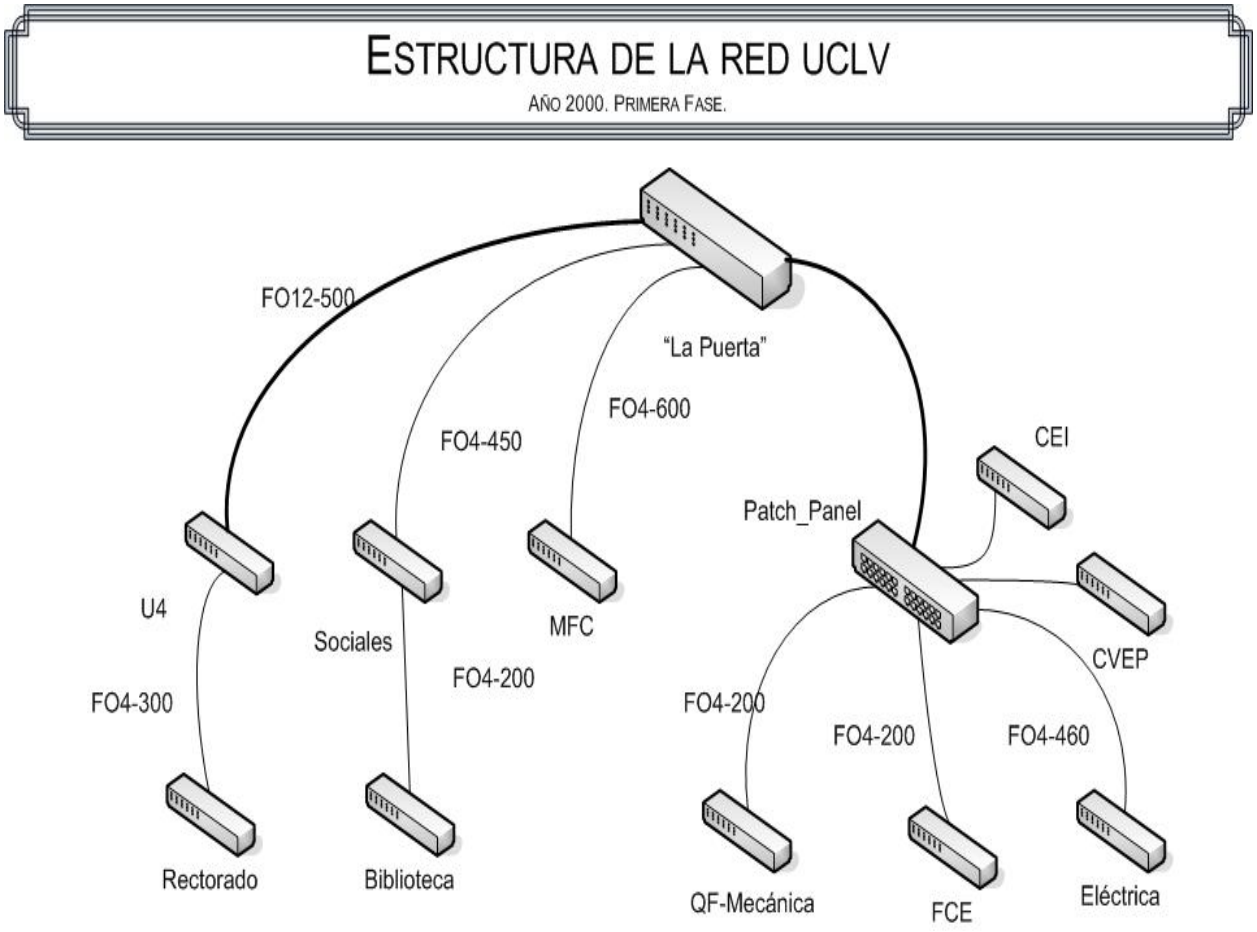


Figura 5: Primera Fase de la Estructura de la Red UCLV.

Se hizo referencia a las distancias y al tipo de fibra por la importancia que presentan estos elementos a la hora de realizar aseveraciones o conclusiones acerca del futuro del equipamiento de la red, que sin dudas es un factor fundamental para el desempeño de la misma.

A medida que estos cambios se tornaban reales en la práctica, se iban acumulando grandes resultados producto del trabajo realizado en la red, la educación del usuario universitario relacionado con el uso de Internet, Correo Electrónico e intercambio de información entre dependencias fue creciendo enormemente. Debido a estos grandes logros se avecinaban nuevos cambios para el año 2002, diseñados y formulados con anterioridad en el año 2000.

La expansión posibilito el acceso de profesores y estudiantes de las facultades de Ciencias Agropecuarias y Construcciones a la Intranet Universitaria. También quedaron conectadas zonas cercanas como el SEDER y el Centro de Bioactivos Químicos.

La estructura queda como se muestra en la figura 6, donde se pueden apreciar la expansión de la misma, se hizo homogéneo el uso de la Fibra Óptica TELDOR multimodo 62.5/125 en los enlaces nuevos.

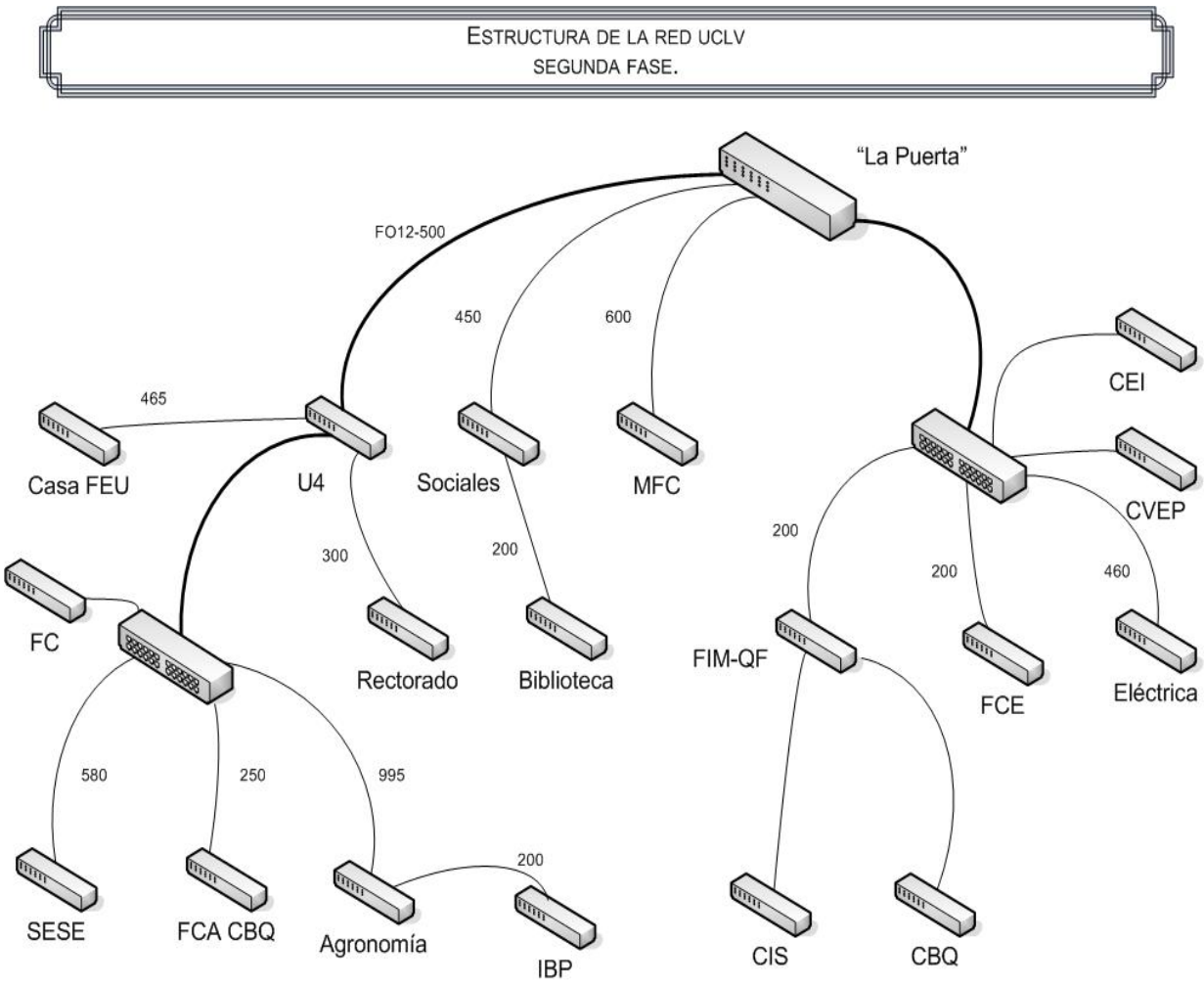


Figura 6: Segunda Fase en la Evolución de la Red UCLV.

II.2 Elementos que afectan la Gestión de la red UCLV.

En estos momentos el *backbone* de la red muestra buenas características funcionales y suple la mayoría de las necesidades que han surgido con el paso del tiempo, pero analizando la estructura más a fondo podemos percatarnos de que existen algunos aspectos que atentan contra el establecimiento de un sistema óptimo de gestión de la red de datos.

Exponemos a continuación los aspectos antes anunciados:

- *Gateways no especializados:* Debido al direccionamiento IP asignado a cada facultad se asigna un *router* que permite el intercambio de paquetes, en la mayoría de los casos estos *routers* son computadoras que no presentan las características suficientes de hardware para que el intercambio de datos sea lo más veloz posible, esto justifica un embotellamiento a la entrada de cada una de las facultades que afecta todo tipo de intercambio de datos, incluyendo los de administración.

- *Aseguramiento eléctrico:* Este es uno de los puntos que más desastres ocasiona cuando no se toma en cuenta. El objetivo es tratar de mejorar el respaldo energético en cada una de las subredes para que el servicio tenga mayor disponibilidad, además no es necesario tomar el riesgo de perder equipos gestionables producto de descargas eléctricas y demás.

- *Uso no generalizado de una plataforma de gestión a nivel global:* No se ha establecido el uso generalizado de una plataforma de supervisión en la cual los administradores de red tengan el control del estado de las estaciones existentes en cada una de las subredes de la UCLV y de sus equipos de comunicación.

- *Falta de enlaces redundantes:* La interconexión existente entre las subredes de las facultades es de forma simple, no existe redundancia en los enlaces y este es uno de los elementos a considerar para tener sistemas de respaldo o para equilibrar el tráfico de entrada y/o salida.

- *Centralización de servicios:* Desde un inicio los servicios que existían en la red de la universidad se manejaban a nivel de facultades, esto resulto ser la solución a muchos de los problemas que existían en aquellos momentos; debido al aumento en la complejidad de los sistemas usados, los costos para elevar la calidad de las estaciones de todos los nodos y la estrategia para evolucionar hacia sistemas abiertos se ha logrado la coexistencia centralizada de los algunos de los servicios de

la Red UCLV. Aunque el trabajo y los logros han sido inmensos hasta el momento se debe de seguir trabajando mucho sobre estas ideas, para lograr un ente completamente estable.

Todo este conjunto de ineficiencias conllevan a la red a acumular problemas que afectan su gestión.

II.4 Implementación de Mejoras y Soluciones.

El aseguramiento del tráfico de información está ligado de forma indisoluble a la calidad de los equipos encargados de la conmutación de paquetes. Esta calidad es también lo que decide las opciones de la red de gestión, las características de los equipos se manejaron de manera minuciosa, para tomar la decisión que mejor relación costo desempeño presenta.

Dentro de las características que se requieren, para tener buen soporte en la red de gestión se encuentran las siguientes:

- Capacidad puertos 10/100 TX.
- Al menos dos expansiones para enlaces por fibra óptica a 100Mbps y a 1Gbps.
- Soporte de SNMP, y Monitoreo Remoto (RMON).
- Filtrado de paquetes.
- Creación de redes virtuales (VLANs).
- Calidad de Servicio (QoS).
- Ruteo de paquetes Ipv4 e Ipv6.
- Soporte de *multicasting*.
- Soporte para RIP (*Routing Internet Protocol*) versión 1 y 2.
- Soporte para OSPF (*Open Shortest Path First*).

Un aspecto que fue tomado en cuenta, a la hora de la selección de los equipos de comunicación, fue la homogeneidad en la firma del fabricante, o sea, que no deben mezclarse equipos de varias firmas en una misma red. El incumplimiento de esta sentencia por supuesto que no implica que la red no funcione, o que lo haga mal. El uso de equipos de varios fabricantes conlleva, en la generalidad de los casos, a que los equipos usados no sean aprovechados al 100% de sus posibilidades. La decisión final fue la compra de productos de la firma *Allied Telesyn.*

Es importante considerar las especificaciones de las estaciones para la implementación y mantenimiento de los servicios en el nodo central, estas computadoras son de alto rendimiento, en la actualidad existen seis de ellas, dos que desempeñan el papel de los servidores de correo de toda la universidad, dos que son las que se encargan de Internet y flujo de correo internacional junto con resolución de nombres entre otras cosas, una con servicios de multimedia, y otra con el sistema de bases de datos y servicios Web a nivel universitario. Hasta el momento ninguno de estos equipos ha fallado y se comportan de acorde a lo planificado.

Chasis	Con fuente de 400 watts. 3 *fans* adicionales.
MotherBoard	ASUS P4P800 Deluxe
Procesador	P4C 3.0 GHz
Memoria	1Gb (256x4) DDR400 Infineon
Discos duros	2 SATA 120 GB 1 IDE ATA 133 40 GB 2 IDE ATA 133 80 GB

Uno de los elementos claves en la mejora de la red UCLV ha sido la selección de conmutadores (switch) gestionables de la firma Allied Telesyn con las siguientes características:

- *SWITCH* modular AT-9816GB: 16 *slots* que soportan enlaces de 1 GB, LX, SX o TX.
- *Switch* AT-8324-XL: 24 puertos 10/100 TX. Dos *slots* disponibles para enlaces *gigabit* sobre fibra óptica o sobre cobre.

- *Switch* AT-8024-GB: similar al anterior pero con menos especificaciones y un poco más lento, que satisface a las necesidades reales de las dependencias indicadas.

Para las subredes de las facultades se seleccionó el AT-8324-XL, este presenta 24 puertos de cobre, ideal para ser el centro en la subred de una dependencia donde solo se tienen pares trenzados para la comunicación entre las máquinas. Entre las posibilidades que brinda podemos citar la construcción de redes virtuales (VLAN) agrupando puertos de manera variable, esto es aplicable para el caso en que se quiera separar subredes por razones de seguridad o ruteo IP.

Entre otras posibilidades que brinda el equipo están:

- Implementación de calidad de servicio (QoS).
- Ruteo desde y hacia todos los puertos disponibles, incluso entre las mismas VLANs creadas en el equipo.
- Puerto en espejo para el muestreo de paquetes, usado generalmente con fines de seguridad informática.
- Filtrado de paquetes. Bajo la acción de un mismo software que viene incorporado en el sistema operativo, *Ipfilter*.
- Implementación de un agente SNMP.
- Soporte para protocolo RMON.
- Servidor HTTP, lo cual lo hace totalmente operable mediante WEB, incluyendo la configuración y monitoreo.
- Agente DHCP. Este agente funciona como servidor, puesto que es conocido como agente de confianza (*agent relay*), y es capaz de asignar direcciones a partir de parámetros que le concede el servidor DHCP de la Red.
- Clientes para servidores de RADIUS, en el caso que se disponga de tarjetas de expansión para MODEM (los cuales son soportados también por el equipo), la autenticación de los usuarios puede ser hecha a través de solicitudes a servidores de este tipo.

Otro de los elementos más importantes es el reporte de actividades y eventos del equipo a un servidor de *Syslog*, el cual registra toda la información contenida dentro de los paquetes enviados y es capaz de construir resúmenes para el entendimiento del comportamiento de ciertos equipos y ordenadores, esta es una herramienta muy útil para el caso en que se quiera saber "vida y obra" del *Switch* en un momento dado. El servidor de *Syslog* en estos momentos se encuentra soportado sobre el servidor de correo externo, montado con Linux Red Hat 9.0 y demás software de código abierto.

II.6 Etapa Final de la Estructura de la Red.

La figura 7 muestra la estructura de la Red UCLV luego de aplicadas las modificaciones en las diferentes dependencias universitarias. Nótese en esta figura como se muestran los enlaces que presentan dificultades para alcanzar el *gigabit* y que se encuentran en fase de pruebas.

La configuración de la red con velocidades de transmisión altas permite que la red de gestión sea un poco más flexible a la hora de seleccionar los datos a muestrear ya que la información de supervisión puede en la mayoría de los casos no ser una carga para el trafico de la red, por lo menos en los nodos donde más circulación de paquetes existe. Esta es otra de las ventajas que ofrece el *backbone gigabit* para la red de gestión.

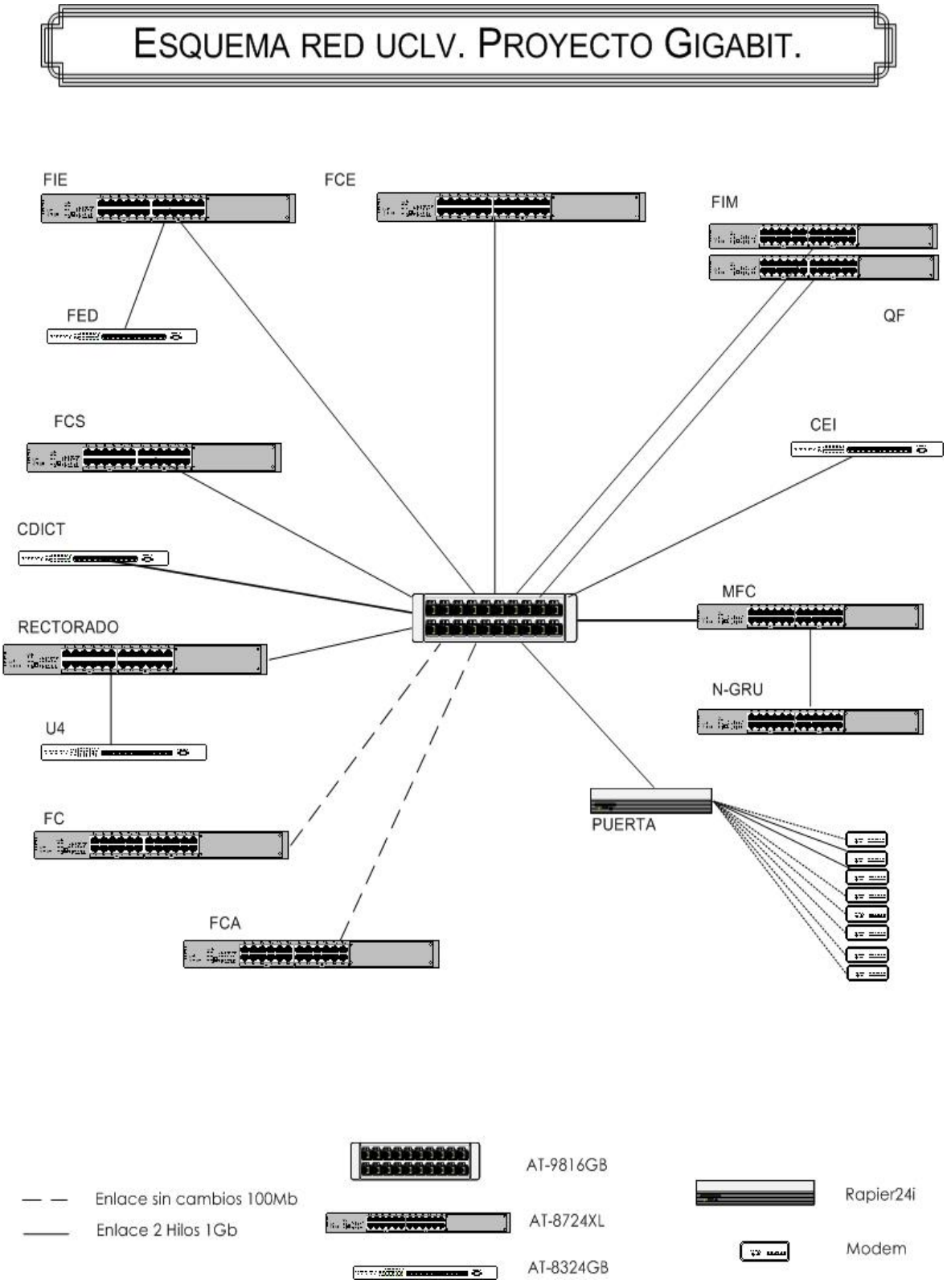


Figura 7: Esquema de la Red UCLV según el proyecto para la expansión a *Gigabit.*

II.7 Consideraciones finales.

Después de esta caracterización se puede apreciar que el *backbone* ofrece las siguientes posibilidades para la gestión de la intranet UCLV:

- Esta dotado actualmente de equipamiento gestionable con las condiciones óptimas para la red de gestión, desde el punto de vista de *Hardware* y de *Software*.

- Las condiciones para el logro de altas velocidades están creadas en la mayoría de los enlaces, lo que implica un ancho de banda aun mayor, una facilidad muy positiva para el intercambio de información de administración.

- Los servicios se pueden gestionar con mucha más flexibilidad si se implementan sobre una red rápida y uniforme como la Intranet UCLV.

Después de conocer la red en la que se desarrolla el sistema de administración podemos sentar las bases para la construcción de la estrategia de gestión, el objetivo central de este trabajo.

Capítulo III Estrategia de Gestión para la Intranet UCLV

III.1 Aspectos necesarios para la creación de la Estrategia.

Durante el capítulo anterior se mostraron cuales son las características de la red en cuanto a tecnologías de hardware y disposición de los servicios, además de las deficiencias que se presentaron en la red que atentaban contra la gestión de la misma.

Para desarrollar la estrategia de gestión de la red UCLV se toman en consideración los siguientes elementos:

- Configuración de los conmutadores acorde a los servicios que se pretenden brindar, para lo cual existe un módulo especifico de software, para cada servicio, dentro del sistema del *switch*.

- Establecimiento de una plataforma de gestión a nivel global, y la proposición de la programación de nuevos módulos para el desarrollo de aplicaciones para la Universidad Central; el programa de supervisión "*Nagios*" es el candidato para jugar este rol.

- Evaluación de resultados que demuestren el aprovechamiento del *backbone* y la posibilidad del intercambio de información administrativa. Las pruebas de tráfico realizadas a los enlaces de fibra interfacultades muestran resultados concluyentes al respecto.

Durante el desarrollo del capítulo se describe cada uno de los aspectos necesarios para la creación de la estrategia de gestión.

III.2 Sistema de Almacenamiento.

Los equipos conmutadores presentan un sistema operativo propietario de *Allied Telesyn*, lo que significa que una vez en nuestras manos, debe existir cierta familiarización con el sistema para poder conversar el mismo idioma, este se auxilia de 32 *megabytes* de memoria RAM, esta es la memoria en la cual se cargan todos los datos necesarios para el inicio y disponibilidad del complejo , como este tipo de almacenamiento es volátil hay que guardar toda la información una vez que se altera para salvar los cambios, puesto que una vez que se reinicie el hardware toda la información contenida en esta RAM se pierde, para esta situación existe un medio de almacenamiento no volátil llamado NVS (*Non Volatile Storage*), y por último la memoria flash, en la cual está contenido todo el software usado por el *switch*, junto a las versiones nuevas o parches usados en la actualización del sistema operativo, además se almacena la información de hardware del equipo obtenida desde su fabricación. [*Allied Telesyn*, 2004].

III.3 Configuración de los Conmutadores. Fichero de Inicio.

La información de cómo están configurados los módulos que activan o desactivan los servicios prestados por el *switch* se encuentra grabada en un fichero en la región de almacenamiento NVS, durante el inicio del sistema esta información es copiada a la memoria RAM desde donde se accede constantemente, en caso de existir cambios en la configuración del mismo fichero se deben de actualizar en la región de NVS. [*Allied Telesyn*, 2004].

A continuación son descritas muchas de las partes del fichero mencionado anteriormente, el cual lleva por nombre: *"uclvras.cfg"* en un equipo de la misma familia de los *switches* del *backbone*, este se encuentra trabajando actualmente en el nodo central de "La Puerta". Para profundizar sobre el fichero de configuración ver Anexo IV.

"uclvras.cfg"

```
# SYSTEM configuration

set system name="sw.uclv.edu.cu"
set system location="FIE"
set system contact="Grupo de Redes UCLV"
#
```

En esta parte se muestra la identificación del *switch* como objeto de la red, nótese las directivas para asignarle un nombre, localización, y un contacto utilizado en nuestra caso para definir la entidad a la que pertenece.

III.3.1 Servicio de RAS.

Aquí se identifican los usuarios creados localmente en el sistema, en el caso que nos ocupa son usuarios del servicio RAS, brindado actualmente en el nodo central y que está presto a modificaciones en cuanto a la autenticación de estos mismos usuarios con los directorios activos de Windows.

```
# USER configuration
add user=abelgv
pass=573cdb4e330a5463b8a52893b38a9a0ff677e97ea33e7a4d38a528f3b38a9a0c
lo=no
set user=abelgv desc="Abel Goya Valdivia" netmask=255.255.255.255
add user=abreu
pass=571c9b1b36144b4d98a528d3b38a9a0ff677e97ea33e7a4d38a528f3b38a9a0c
lo=no
set user=abreu desc="Jose Abreu" netmask=255.255.255.255
add user=agarcia
pass=371c8849535b0f2a9dcb4192b38a9a09f677e97ea33e7a4d38a528f3b38a9a0c
lo=no
set user=agarcia desc="Agustin Garcia Rdguez" netmask=255.255.255.255
add user=aldo
pass=b71c8d110d0c4a7d9ba52883b38a9a0ff677e97ea33e7a4d38a528f3b38a9a0c
lo=no
set user=aldo desc="Aldo Oliva Gonzalez" netmask=255.255.255.255
```

Las líneas de código describen acciones como la adición del usuario y de su clave, la cual se muestra encriptada como resultado de una función MD5 aplicada sobre la palabra original; en las líneas se pueden ver los privilegios que tiene el usuario para autenticarse en el sistema localmente, lo cual se llama *"logon locally"*, los usuarios antes mencionados no tienen ese tipo de posibilidad lo cual implica un elemento más para identificarlos como

usuarios de acceso remoto, también aparece la descripción completa de la persona que se identifica con el nombre adicionado.

La configuración de los puertos asíncronos, a continuación, para la atención de MODEM, conectados a tarjetas en bahías de expansión multiuso soportadas por el equipo mismo, es un proceso necesario para que estos puertos reconozcan y trabajen con el hardware conectado.

```
# ASYN configuration

set asyn=1 speed=115200 cd=connect ip=172.20.1.241
set asyn=2 speed=115200 cd=connect ip=172.20.1.242
set asyn=3 speed=115200 cd=connect ip=172.20.1.243
set asyn=4 speed=115200 cd=connect ip=172.20.1.244
set asyn=5 speed=115200 cd=connect ip=172.20.1.245
set asyn=6 speed=115200 cd=connect ip=172.20.1.246
#
```

En la configuración de los puertos asíncronos se especifica la velocidad máxima a la cual se pueden conectar los MODEM y los números IP que se le asignan a cada uno de estos puertos.

```
# ACC configuration

add acc call="RAS-1" dir=answer encap=ppp auth=chap asyn=1
set acc call="RAS-1" ppptemplate=1
set acc call="RAS-1" rscript=nvs:reset.mds
add acc call="RAS-2" dir=answer encap=ppp auth=chap asyn=2
set acc call="RAS-2" ppptemplate=1
set acc call="RAS-2" rscript=nvs:reset.mds
add acc call="RAS-3" dir=answer encap=ppp auth=chap asyn=3
set acc call="RAS-3" ppptemplate=1
set acc call="RAS-3" rscript=nvs:reset.mds
add acc call="RAS-4" dir=answer encap=ppp auth=chap asyn=4
set acc call="RAS-4" ppptemplate=1
set acc call="RAS-4" rscript=nvs:reset.mds
add acc call="RAS-5" dir=answer encap=ppp auth=chap asyn=5
set acc call="RAS-5" ppptemplate=1
set acc call="RAS-5" rscript=nvs:reset.mds
add acc call="RAS-6" dir=answer encap=ppp auth=chap asyn=6
set acc call="RAS-6" ppptemplate=1
set acc call="RAS-6" rscript=nvs:reset.mds
#
```

En el sistema se designan *ACC (Aynchronous Call Control*) para activar las interfaces de comunicación y referirse al comportamiento de las mismas, se les puede asignar un grupo

de características tales como el nombre, el rol que van a desempeñar en la comunicación con el MODEM (el cual puede ser “de respuesta” o “de llamada”), el tipo de encapsulado usado en la transmisión, la autenticación usada para identificar los usuarios, y un *script* que se usa para poder reiniciar la interfase (aclarando el nombre y la ubicación del mismo en memoria NVS).

```
# INTERFACE configuration

set int=ppp0 mtu=1500
set int=ppp2 mtu=1500
set int=ppp2 mtu=1500
#
```

En la configuración de las interfaces, uno de los elementos para estandarizar la transmisión es el tamaño máximo permitido por la red para los paquetes llamado Máxima Unidad de Transferencia, en redes *Ethernet* se limita este número a 1500; este es un elemento importante a tener en cuenta cuando se usa TCP/IP.

III.3.2 Servicio de Autenticación de Usuarios de Acceso Remoto.

```
# RADIUS configuration
```

En el momento en que se extrajo esta información el *switch* manejaba alrededor de 201 usuarios locales de RAS, que son atendidos por seis MODEM conectados a seis interfaces o tarjetas de expansión soportadas en el equipo. Se definió montar un servidor de RADIUS (*Remote Authentication Dial In User Service*), para la autenticación de los usuarios remotos que se conectan por línea telefónica, en uno de los ordenadores dedicados del nodo central para que los identifique de forma automática según sus credenciales en el directorio activo de Windows, y no de manera local en el sistema como se encuentra en estos momentos, donde suple las necesidades existentes en el momento pero no es del todo centralizado como para cumplir con los objetivos de la intranet universitaria.

Este módulo especifica la dirección IP del servidor de RADIUS asignado y la palabra secreta que se intercambia en las transmisiones cliente-servidor.

III.3.3 Estructuración de Redes Virtuales (VLAN).

Aquí se crean distintas redes virtuales, cada una de ellas con un identificador y un nombre, con el objetivo de reunir comunidades de intereses, esto facilita la comunicación entre usuarios del mismo tipo: científicos, estudiantes, profesores, secretarios, o cualquiera que pueda ser creado con estos fines.

```
# VLAN general configuration

create vlan="INTERNET" vid=5
create vlan="INTRANET" vid=10
create vlan="INTRANET-1" vid=11
create vlan="INTRANET-2" vid=12
create vlan="INTRANET-3" vid=13
create vlan="INTRANET-4" vid=14
#
```

En las líneas siguientes se designan cuales son los puertos que le pertenecen a cada VLAN. Verifíquese que se especifican más de 24 puertos, el 25 y el 26 son los que se han conectado en bahías de expansión multiuso delanteras, un puerto de fibra a 1GBps y un puerto para UTP a 1GBps, estos forman parte de la última VLAN.

```
# VLAN port configuration

add vlan="INTERNET" port=1-6
add vlan="INTRANET" port=7-10
add vlan="INTRANET-1" port=11-14
add vlan="INTRANET-2" port=15-18
add vlan="INTRANET-3" port=19-22
add vlan="INTRANET-4" port=23-26
#
```

III.3.4 Servicio de Ruteo.

La tabla de rutas fijas que contiene el sistema es usada para “encaminar” paquetes por el método de tablas de ruta estáticas. Este *switch* es, actualmente, uno de los *gateways* por defecto de casi todas las subredes en la universidad. Nótese que en este módulo se activa un IP para el *switch*, esta es la forma mediante la cual se identifica al equipo dentro de la red y permite que el *switch* sea identificado por cualquiera de sus puertos, elemento este indispensable para el uso de sus servicios.

```
# IP configuration

enable ip
add ip int=vlan10 ip=172.20.1.240 mask=255.255.255.0
add ip rou=172.20.2.0 mask=255.255.255.0 int=vlan10 next=172.20.1.39
add ip rou=172.20.3.0 mask=255.255.255.0 int=vlan10 next=172.20.1.44
add ip rou=172.20.4.0 mask=255.255.255.0 int=vlan10 next=172.20.1.44
add ip rou=172.20.5.0 mask=255.255.255.0 int=vlan10 next=172.20.1.44
add ip rou=172.20.6.0 mask=255.255.255.0 int=vlan10 next=172.20.1.36
add ip rou=172.20.7.0 mask=255.255.255.0 int=vlan10 next=172.20.1.43
add ip rou=172.20.8.0 mask=255.255.255.0 int=vlan10 next=172.20.1.56
add ip rou=172.20.9.0 mask=255.255.255.0 int=vlan10 next=172.20.1.38
add ip rou=172.20.10.0 mask=255.255.255.0 int=vlan10 next=172.20.1.35
add ip rou=172.20.11.0 mask=255.255.255.0 int=vlan10 next=172.20.1.35
add ip rou=172.20.12.0 mask=255.255.255.0 int=vlan10 next=172.20.1.41
add ip rou=172.20.13.0 mask=255.255.255.0 int=vlan10 next=172.20.1.38
add ip rou=172.20.14.0 mask=255.255.255.0 int=vlan10 next=172.20.1.47
add ip rou=172.20.15.0 mask=255.255.255.0 int=vlan10 next=172.20.1.37
add ip rou=172.20.16.0 mask=255.255.255.0 int=vlan10 next=172.20.1.42
add ip rou=172.20.17.0 mask=255.255.255.0 int=vlan10 next=172.20.1.55
add ip rou=172.20.18.0 mask=255.255.255.0 int=vlan10 next=172.20.1.56
add ip rou=172.20.19.0 mask=255.255.255.0 int=vlan10 next=172.20.1.39
add ip rou=172.20.20.0 mask=255.255.255.0 int=vlan10 next=172.20.1.41
add ip rou=172.20.21.0 mask=255.255.255.0 int=vlan10 next=172.20.1.56
add ip rou=172.20.22.0 mask=255.255.255.0 int=vlan10 next=172.20.1.100
add ip rou=172.20.23.0 mask=255.255.255.0 int=vlan10 next=172.20.1.57
add ip rou=172.20.24.0 mask=255.255.255.0 int=vlan10 next=172.20.1.63
add ip rou=172.20.25.0 mask=255.255.255.0 int=vlan10 next=172.20.1.35
add ip rip int=vlan10 ipaddr=172.20.1.9 send=rip2 receive=rip2
add ip dns prim=172.20.1.53
#
```

En el siguiente módulo se puede activar el uso de IPv6 y tener en cuenta algunos elementos de configuración del protocolo. En la UCLV todavía no se implementa este servicio, se usa la versión cuatro de protocolo de Internet.

```
# IPv6 configuration
```

A continuación se muestra el modulo que referencia otro de los protocolos importantes de ruteo:

```
# OSPF configuration
```

La información que puede estar contenida aquí es un elemento importante a considerar por el hecho de que en la red de la universidad se ha definido la instalación de enlaces redundantes, lo cual quiere decir que para alcanzar un determinado destino puede haber más de una vía. Se puede efectuar un balance de carga entre los enlaces según las métricas

o utilización que tengan estos enlaces en determinado momento, este protocolo de ruteo *OSPF* (*Open Shortest Path First*) obtiene el camino más "pequeño" entre un origen y un destino. Las métricas usadas en la selección del camino más apropiado indican la prioridad de una ruta para ser elegida antes que otra con métrica mayor. [Shaikh, 2002].

III.3.5 Agente SNMP.

Configuración y habilitación del protocolo SNMP y de las comunidades utilizadas en la transmisión de la información de gestión. El agente SNMP, usado en la estrategia de gestión de la UCLV, se habilita y configura en esta sección.

```
# SNMP configuration

enable snmp
create snmp community=public0 open=on
#
```

III.3.6 Servicio de Filtrado de Paquetes.

La configuración de un cortafuegos, llamado "*Paladin*", se puede adicionar en esta sección del fichero.

```
# FIREWALL configuration
```

Nótese que este *firewall* solo esta presente en los *switch* de nodos grandes (AT-9816GB), y en el *Rapier* de la puerta, en los que le corresponden a las facultades (AT-8324-XL) se usa un *IPfilter*, un software que usa reglas de filtrado de paquetes pero no tiene las mismas prestaciones que este *firewall*.

III.3.7 Servicio de Asignación de Direcciones.

```
# BOOTP configuration
```

El protocolo de asignación de recursos durante el inicio, designado y construido para máquinas que no tienen medios de almacenamiento como pudieran ser un disco duro o un

floppy, puede ser configurado en esta sección, la vía de enlace con servidores que almacenan imágenes necesarias para el inicio de estas maquinas, direcciones IP y máscaras de subred.

```
# DHCP configuration
```

Encontramos la configuración del módulo de un cliente de DHCP, el cual posibilita asignar números IP a las interfaces del mismo equipo en dependencia de los parámetros descritos por un servidor de DHCP en la red, especificado en este módulo, junto a muchos factores más.

III.3.8 Servicio de Sincronización de Relojes.

La implementación de *NTP (Net Time Protocol)* en el *switch* esta basada en las RFC-958, RFC-1305 y RFC-1510. Son soportadas dos tipos de operaciones llamadas “Cliente” y “Servidor”, en la mayoría de los casos el equipo trabaja en modo cliente, en el cual encuesta un servidor primario asignado cada cierto tiempo determinado por el administrador, esta encuesta es posible debido a la construcción de pares llamados “Cliente-Servidor”.

```
# NTP configuration
```

Se pueden especificar servidores de tiempo primarios aceptados en la mayoría de los casos como ejes para la sincronización de relojes de los ordenadores en la red, lo cual implica al *switch* como servidor de tiempo secundario, estos son elementos primordiales para la comunicación entre servidores, computadores personales y demás componentes activos a lo largo de la red UCLV.

III.3.9 Servicio de Mensajes de Control de Errores.

Como es de esperar este equipo de comunicación brinda la posibilidad de realizar chequeos y control de errores mediante el Protocolo de Mensajes de Control de Internet (ICMP). El conmutador implementa todas las opciones no obsoletas del protocolo, se le puede cambiar todo el *set* de parámetros a estos mensajes ICMP, con el objetivo de realizar

distintas pruebas que dependen en la mayoría de los casos de las particularidades de la máquina o sección de subred cuestionada. En este módulo se pueden configurar los parámetros deseados para la ejecución de un *ping* a un destino determinado

```
# PING configuration
```

III.3.10 Conexión desde Equipos Remotos.

```
# TELNET configuration
```

El módulo donde se describe el protocolo de conexión TELNET puede ser configurado para determinadas propiedades ajustables dentro del protocolo, como son niveles de privilegio y demás.

III.3.11 Servicio de Registro de Eventos e Historiales.

Durante el tiempo de trabajo de estos dispositivos se originan ciertos eventos y registros que trazan su comportamiento a medida que se van efectuando acciones en el mismo.

```
# LOG module configuration
cre log out=1 dest=syslog server=172.20.1.33 secure=no mess=20
add log out=1 filt=1 all
#
```

Estos reportes pueden ser analizados, filtrados, priorizados y procesados por el equipo, los resultados, según la manipulación deseada por el administrador, se pueden almacenar en memoria RAM o NVS, enviar a un puerto asíncrono determinado en el cual se coloca un dispositivo capaz de recibirlos y almacenarlos o se pueden enviar hacia un servidor que tiene la responsabilidad de recolectarlos para establecer bitácoras de eventos y así poder analizarlas en casos necesarios por cuestiones de seguridad u otros aspectos. Estos servidores son generalmente llamados servidores "*Syslog*", mencionados en el capítulo anterior, y son capaces de construir ciertos resúmenes de cómo se ha comportado el *switch*, durante cierto tiempo establecido por el administrador del sistema. [*Allied Telesyn*, 2004]

III.3.12 Servicio de Correo.

Como parte del sistema de protección y comunicación del *switch*, se implementa un subsistema de correos propietario.

```
# MAIL configuration
```

El conmutador ejecuta un cliente SMTP que permite realizar conexiones hacia un servidor de correo y enviar mensajes SMTP, es de destacar que solamente se implementa la transmisión de mensajes del *switch* hacia un servidor SMTP, y en ningún caso la recepción de estos mensajes.

III.3.13 Servicio Web.

Se ha construido el soporte, en el equipo, para un cliente y un servidor HTTP, los cuales son compatibles con los navegadores que cumplen con HTTP 1.1, el servidor permite al *switch* publicar páginas HTML fuera de la memoria *flash* hacia un explorador Web. El estado del servicio de HTTP se puede estar supervisando en cualquier momento, se puede depurar o limpiar el servidor en caso de presentarse obstáculos al iniciar y se puede configurar la página que se muestra, basta realizar pruebas para determinar todas las posibilidades alcanzables.

```
# HTTP configuration
```

En el **Anexo V** se muestra una imagen de la página de inicio, las posibilidades para realizar la configuración y monitoreo del sistema se pueden observar en los **Anexos VI** y **VII**.

Como se ha podido ver hasta el momento los servicios implementados en el trabajo han sido varios, se destaca que las aplicaciones estudiadas en el *switch* son, en general, las más importantes.

Solo queda mencionar que la información existente al respecto esta estructurada en forma de manuales que el propio fabricante incluye dentro de la compra, estos manuales son exhaustivos y muy abarcadores, y tratan todo lo relacionado con las aplicaciones antes mencionadas.

III.4 Software de Gestión.

A continuación se describe el software de gestión, seleccionado por estudios anteriores al nuestro, cuestión esta por la cual solo citamos el programa y no su proceso de selección ya que no fue objetivo inicial de nuestro trabajo, en este epígrafe analizamos algunos de los aspectos que se pueden cubrir con esta propuesta para la gestión de la red UCLV.

III.4.1 Supervisor *Nagios*. Uso de Software Libre.

El *nagios* es un supervisor de servicios y estaciones de trabajo diseñado para informar de los problemas en la red antes de que lo hagan los usuarios. Fue creado para plataformas Linux pero se ejecuta bastante bien sobre ambientes UNIX. La idea básica es disponer de un *daemon* que supervise los servicios especificados y que avise en caso de que algo no este bien. Es capaz de monitorear servicios de red tales como SMTP, POP3, HTTP, NNTP, PING y recursos locales de una *PC* como carga del procesador y uso del disco duro.

El proceso monitor usa comandos previamente escritos y que pueden ser extendidos mediante el uso de *plugins.* Los avisos pueden ser enviados por diversas vías, por ejemplo correo, SMS o un sistema de mensajería instantánea como ICQ, *Yahoo Messenger* o *Jabber*. El estado actual y pasado puede ser encuestado a través de cualquier navegador de WEB.

La Figura 8 muestra un ejemplo que contiene el estado de los servidores de la UCLV.

El punto débil de este programa es lo tedioso de su configuración y aunque existen aplicaciones hechas por terceros que facilitan esta tarea su uso no está libre de errores por lo que muchas veces resulta conveniente hacer todo el proceso de configuración manualmente.

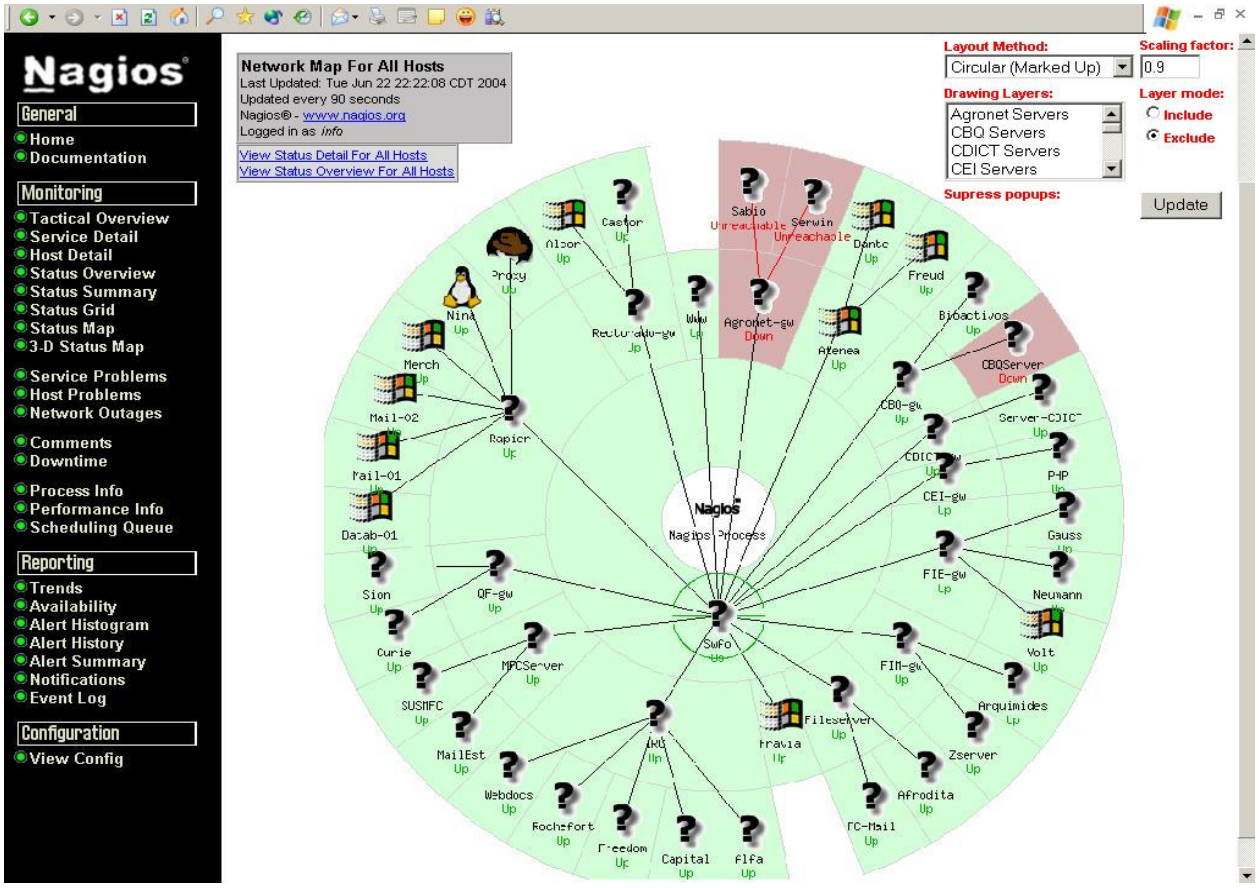


Figura 8: Mapa de estado del Nagios

III.4.2 Sistema de Ficheros de *Nagios.*

Los ficheros de configuración del *nagios* se relacionan en la tabla a continuación.

nagios.cfg	Es el fichero principal, en el se encuentran las referencias a los demás ficheros. Incluye la ubicación de los ficheros *logs* y los descriptores del *daemon nagios*.

services.cfg	Contiene la declaración de los servicios que se desean monitorear a nivel de estaciones. Y los datos que regulan este monitoreo.
hosts.cfg	Incluye las direcciones IP, responsables, descripción de las estaciones a las que se les va a monitorear algún servicio. También es el que brinda la información de la estructura física de la red.
hostgroups.cfg	Permite agrupar estaciones que compartan características diferentes como las personas responsables o los servicios a monitorear.
contacts.cfg	Es aquí donde se definen los nombres y los datos básicos de los responsables que existen en la red.
contactgroups.cfg	Al igual que *hostsgroups.cfg* este fichero permite agrupar los contactos.
cgi.cfg	Orientado a regular el acceso al *nagios* desde un navegador Web. Aspectos como la autentificación y las acciones posibles, sobre el proceso de chequeo, son configuradas aquí.
commands.cfg	Contiene la definición de los comandos a ejecutar, estos comandos son los que informan el estado de los servicios.
checkcommands.cfg	Cada estación puede tener un primer chequeo para decidir si se prueban o no los servicios que están definidos para ella. Los comandos para este primer contacto se definen aquí.
serviceextinfo.cfg	En este fichero se definen aspectos más bien visuales de los servicios creados. Por ejemplo el icono con el que aparecerá ese servicio en los resúmenes mostrados por Web.
hostsextinfo.cfg	Lo mismo que el caso anterior pero orientado a las estaciones.
dependencies.cfg	Ocurre en ocasiones que no vale la pena chequear un servicio en una estación porque un fallo en otro lado de la red lo impide. Esto no significa que el servicio no este trabajando de forma adecuada por lo que la imposibilidad de conocer su estado no debe ser tratada como un fallo en su comportamiento. El fichero *dependencies.cfg* se crea para permitir relaciones de este tipo entre los servidores.

La documentación de la estructura de los objetos presentes en cada uno de los ficheros relacionados puede ser encontrada en el propio sitio Web creado por el *nagios* o en el sitio oficial del producto. [NAGIOS, 2004].

III.4.3 Configuración de los Ficheros de Sistema.

Para lograr una mejor visualización de los ficheros tratados se muestra un pequeño ejemplo de los más importantes.

hosts.cfg

```
define host{
        host_name               merch
        alias                   MERCH
        address                 172.20.1.5
        parents                 sw-fo
        check_command           check-host-alive
        max_check_attempts      10
        notification_interval   120
        notification_period     24x7
        notification_options    d,u,r
        }
```

hostgroups.cfg

```
define hostgroup{
        hostgroup_name  uclv-servers
        alias           UCLV Servers
        contact_groups  uclv-admins
        members         fravia,merch,mail-01,mail-02,Datab-01
        }
```

contacts.cfg

```
define contact{
        contact_name                    root
        alias                           root
        service_notification_period     24x7
        host_notification_period        24x7
        service_notification_options    w,u,c,r
        host_notification_options       d,u,r
        service_notification_commands   notify-by-email
        host_notification_commands      host-notify-by-email
        email                           root@nagios.uclv.edu.cu
        }
```

contactgroups.cfg

```
define contactgroup{
        contactgroup_name       uclv-admins
```

```
        alias                   UCLV Administrators
        members                 rtorres,manuel,root
        }
```

service.cfg

```
define service{
        hostgroup_name                  uclv-servers
        service_description             PING
        is_volatile                     0
        check_period                    24x7
        max_check_attempts              3
        normal_check_interval           5
        retry_check_interval            1
        contact_groups                  uclv-admins
        notification_interval           120
        notification_period             24x7
        notification_options            c,r
        check_command                   check_ping!100.0,20%!500.0,60%
        }
```

command.cfg

```
command[check_ping]=/usr/local/nagios/libexec/check_ping -H $HOSTADDRESS$
-w 10:20% -c 60:100%
```

El *nagios* incluye una gran variedad de comandos, desde simples chequeos de *ping* hasta cantidad de espacio libre dentro de un *filesystem* específico. Pero quizás la posibilidad más útil que tenga sea la instalación de agentes en otras estaciones. Estos agentes están disponibles para Linux, Windows y hasta MS-DOS. Ellos simplemente recolectan la información y esperan ser encuestados por la estación principal. La sencillez de este proceso garantiza su éxito. Es la misma idea de SNMP y causalmente tiene el mismo punto débil: la seguridad. Para resolver ese problema *nagios* implementa dos métodos, el primero consiste en solo permitir conexión desde ciertas direcciones IP y el segundo es la codificación del tráfico que viaja. El primero es el más usado por su sencillez pero no es totalmente seguro. El segundo es más seguro pero implica más complejidad en su implementación.

Como regla general debe evitarse la ejecución de comandos en estaciones activas, solo debe existir la posibilidad de solicitar información de muestreo. En caso de que la información sea crítica debe encontrarse otra vía más segura para su transmisión.

En el caso de la Red UCLV la comunicación entre el *nagios* y las estaciones que tienen agentes corriendo se asegura utilizando *firewalls.*

III.5 Comportamiento de los Enlaces. Pruebas de Tráfico.

Hasta el momento se ha visto como es el comportamiento de los *switches* y cuales son las posibilidades que nos brindan una vez que optamos por su uso. Se ha abordado además el software establecido como plataforma de gestión a nivel de Intranet y su configuración. Durante el desarrollo del epígrafe se describen las pruebas que se realizaron para analizar los cambios en el estado del enlace, antes y después de implementar el uso de estos equipos.

Dentro de las inversiones que se realizaron en la UCLV se adquirieron módulos para los enlaces a 1Gbps entre las subredes de las facultades, en las primeras compras se adquirieron seis módulos de este tipo, dos de ellos para enlaces LX , otros dos para SX y los restantes para lograr la conexión por pares de cobre.

Las pruebas se realizaron en facultades que tuvieran una tierra física aceptable, y en casos diferentes con respecto a la normas de atenuación por distancia, el caso fuera de la norma fue la Facultad de Eléctrica, el otro fue la de Sociales.

Las experiencias se analizaron según un medidor de tráfico llamado *Chariot* de la firma *NetIQ*, una empresa de gran prestigio a nivel mundial en Gestión de Redes de computadoras. Este software incluye pruebas de ancho de banda, de respuesta de paquetes en tiempos determinados, entre otras, las cuales se pueden configurar minuciosamente mediante *scripts* incluidos en el programa.

III.5.1 Enlace Facultad de Eléctrica y Nodo Central.

Los resultados obtenidos en las gráficas a continuación corresponden al enlace entre FIE y Nodo Central. Estas pruebas se realizaron entre dos estaciones a 100Mbps en cada extremo del enlace. Nótese que las velocidades no exceden los 77Mbps y la latencia de los paquetes alcanza el valor de 0.14ms.

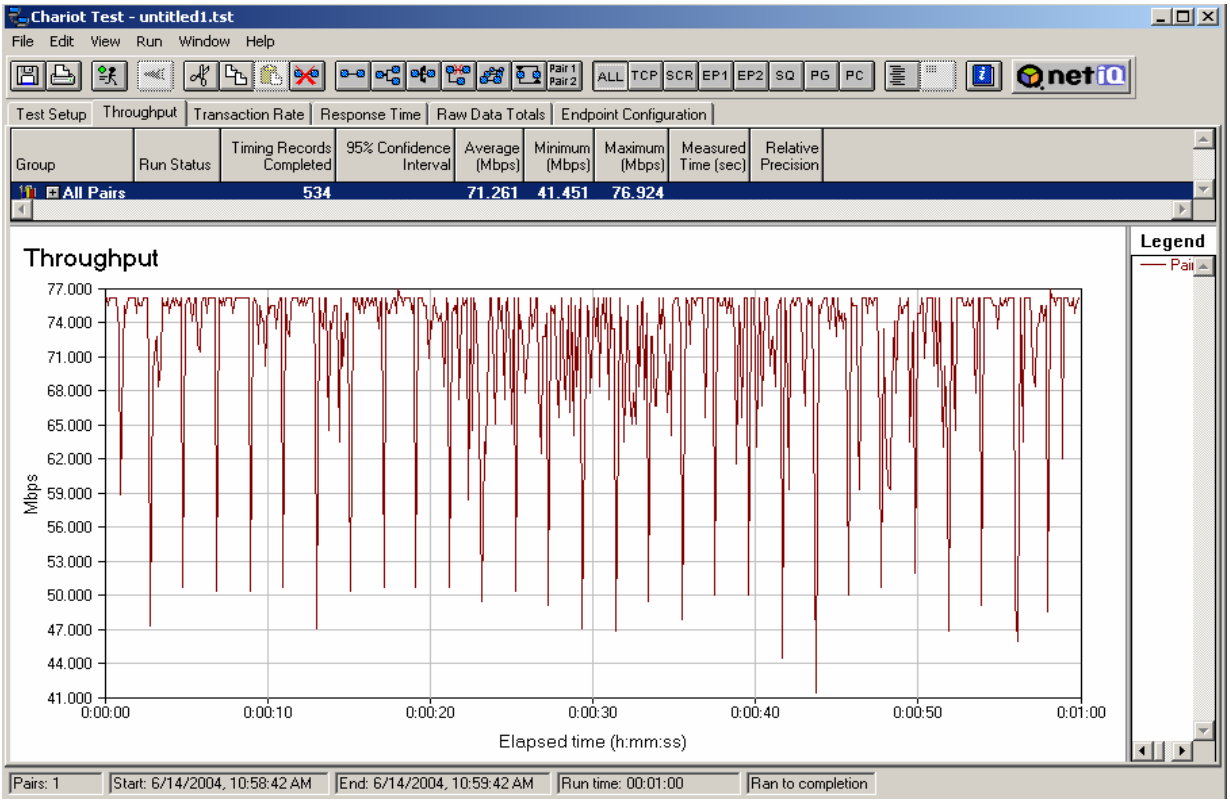


Figura 9: Gráfica de Ancho de Banda de transmisión. Enlace a 100Mbps.

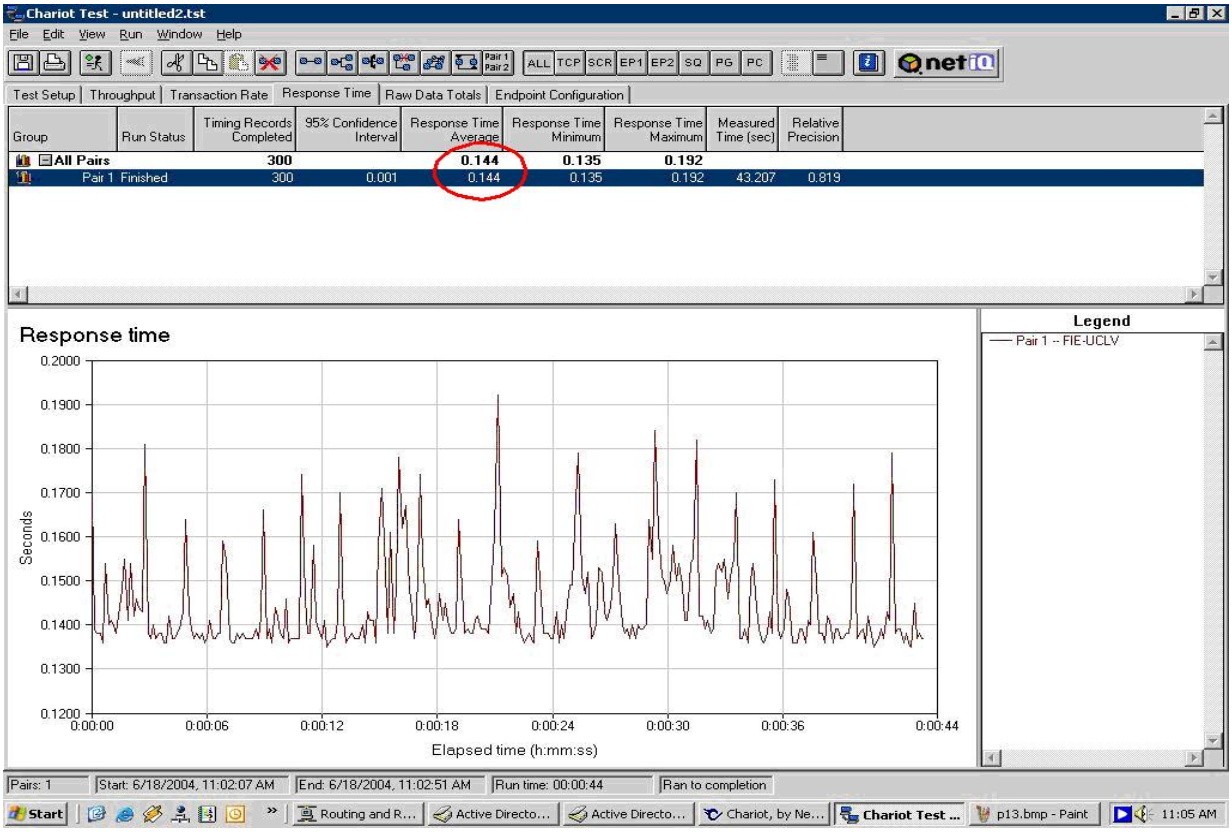


Figura 10: Gráfica de Latencia de Paquetes. Enlace a 100Mbps.

Aquí se ha probado el mismo enlace pero con la conexión mediante módulos *gigabit*. Reiteramos la atención en los límites de velocidad y latencia de los paquetes.

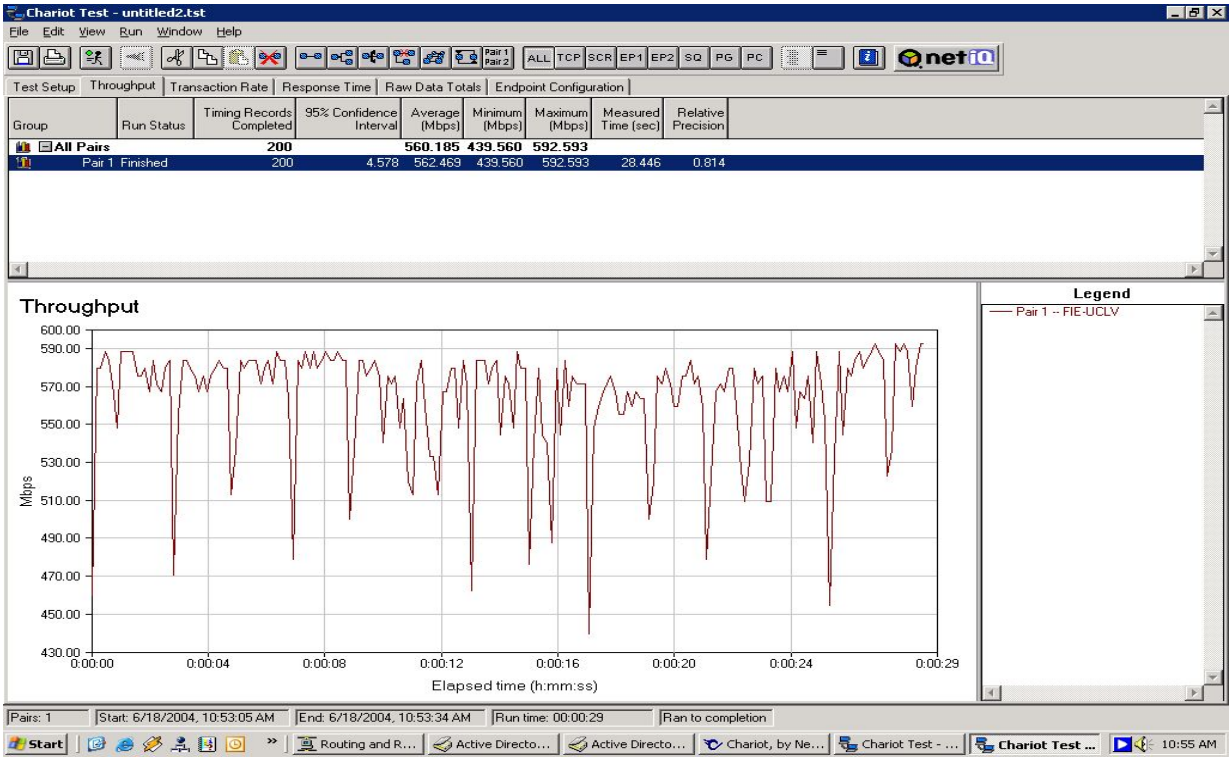


Figura 11: Gráfica de Ancho de Banda. Enlace a 1Gbps usando los módulos de conexión.

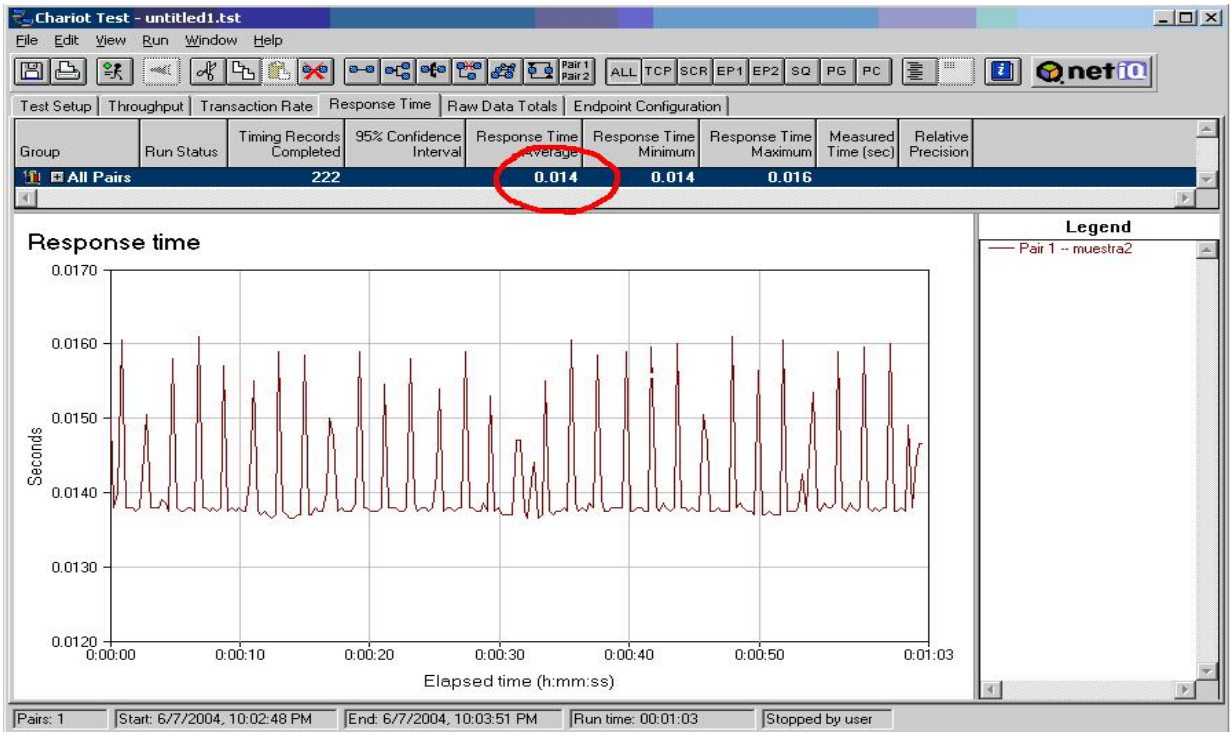


Figura 12: Gráfica de Latencia de Paquetes. Enlace a 1Gbps usando los Módulos de Conexión.

III.5.2 Enlace Facultad de Sociales y Nodo Central.

A continuación las mismas pruebas en un enlace dentro de la norma:

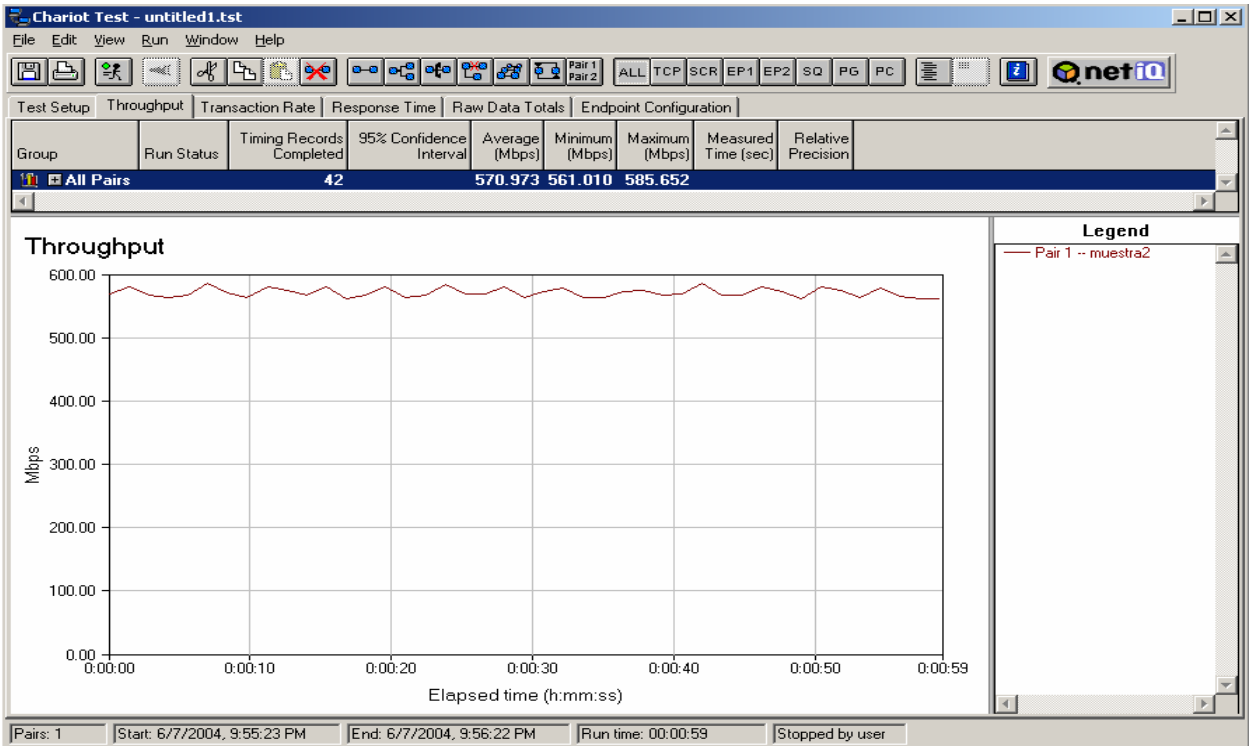


Figura 13: Gráfica de Ancho de Banda. Enlace a 1Gbps, enlace Fac. Sociales.

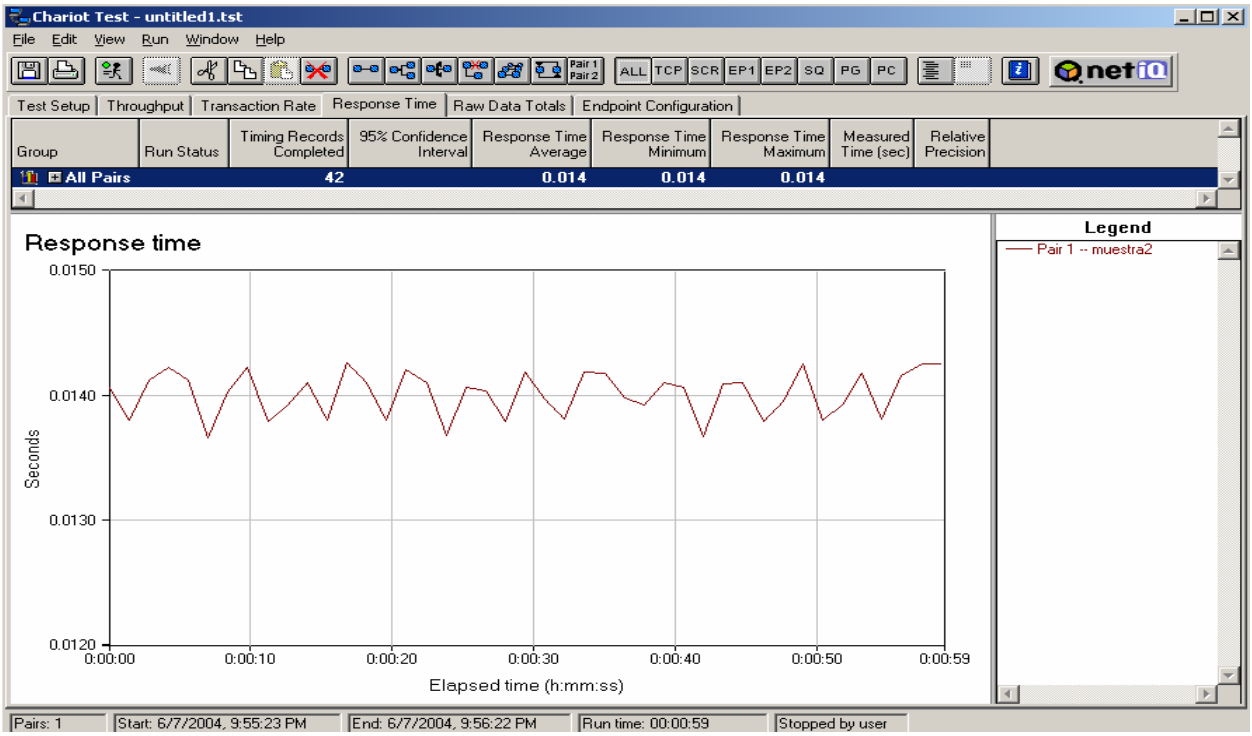


Figura 14: Gráfica de Latencia de Paquetes. Enlace a 1Gbps, enlace Fac. Sociales.

Nótese que los resultados alcanzados en los ejemplos, para los cuales el enlace se conecta a un *gigabit* por segundo, solo alcanzan velocidades cerca de los 600Mbps, aun cuando se prueba en el enlace dentro y fuera de la norma.

Es de destacar que las pruebas realizadas se montaron sobre enlaces punto a punto como se muestra la figura 15, donde todos los equipos, tanto los *switch* como las estaciones, soportan *Gigabit Ethernet.*

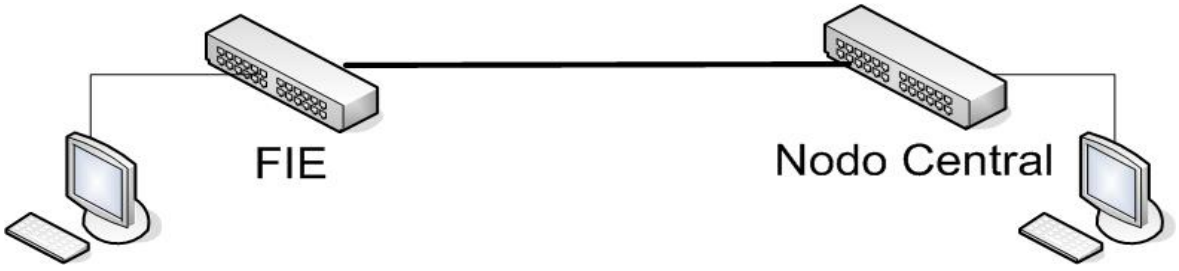


Figura 15: Enlace efectuado para las pruebas de tráfico.

El enlace no se puede saturar debido a que no se efectúan conexiones multipunto, este tipo de prueba no se pudo realizar por la falta de equipamiento (módulos de fibra). Es necesario aclarar que el resto del equipamiento para la conexión a un *gigabit* se encuentra en trámites

de compra, una vez instalado completamente se realizan las pruebas nuevamente para comprobar los resultados y compararlos con los obtenidos en este trabajo.

No obstante, las velocidades alcanzadas fueron exitosamente elevadas, un promedio de 560Mbps, casi siete veces las existentes en el *backbone* de fibra que esta funcionando actualmente, además, el enlace esta siendo probado con todo el tráfico entrante y saliente de la Facultad de Eléctrica sin reportes de error en la transmisión de los paquetes, estos datos se verifican mediante las herramientas de administración y monitoreo del *switch*, el cual dice el estado de cada una de sus interfases.

Después de haber obtenido los resultados anteriormente expuestos, se efectuaron las mismas pruebas para un enlace punto a punto entre dos máquinas con tarjetas *Gigabit Ethernet*, mediante un cable *crossover*, obviamente verificamos una vez más que el enlace no es saturable mediante conexiones simples. Obtuvimos resultados similares en cuanto a la velocidad del enlace, véase figuras 16 y 17, solo se evidencia una latencia de paquetes menor debido a la distancia de la conexión.

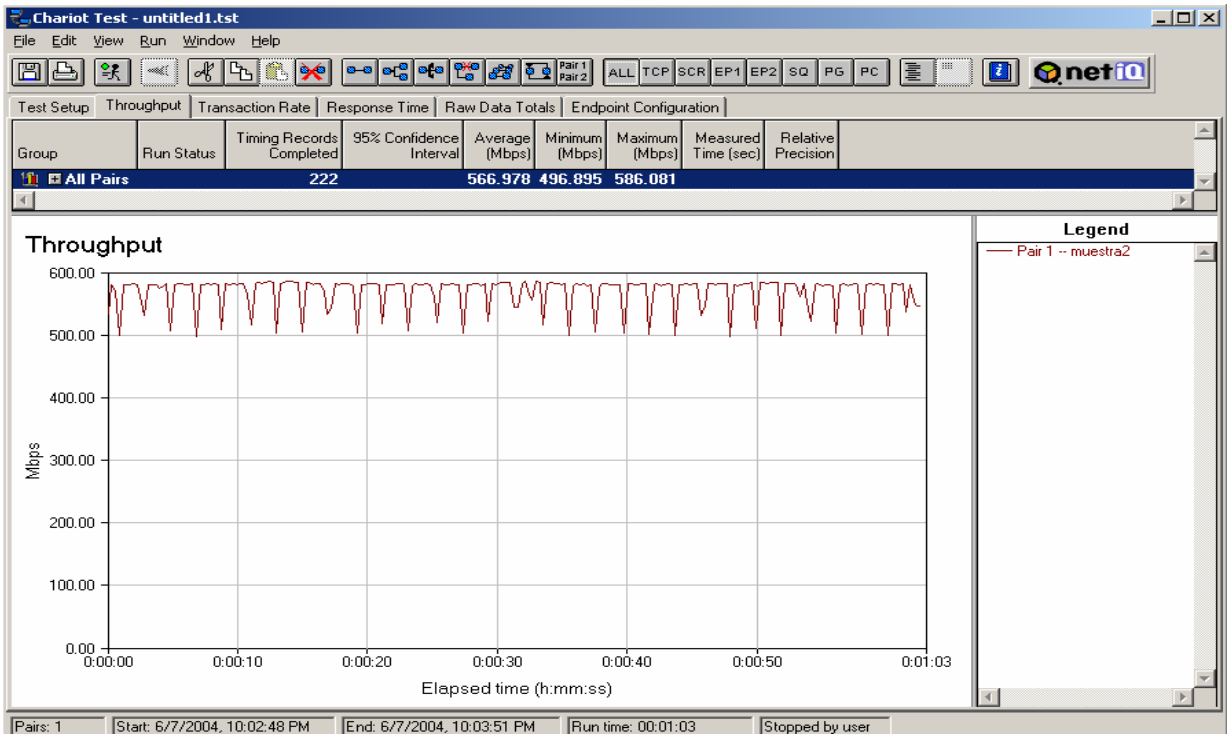


Figura 16: Gráfica de Ancho de Banda. Enlace a 1Gbps usando un Crossover.

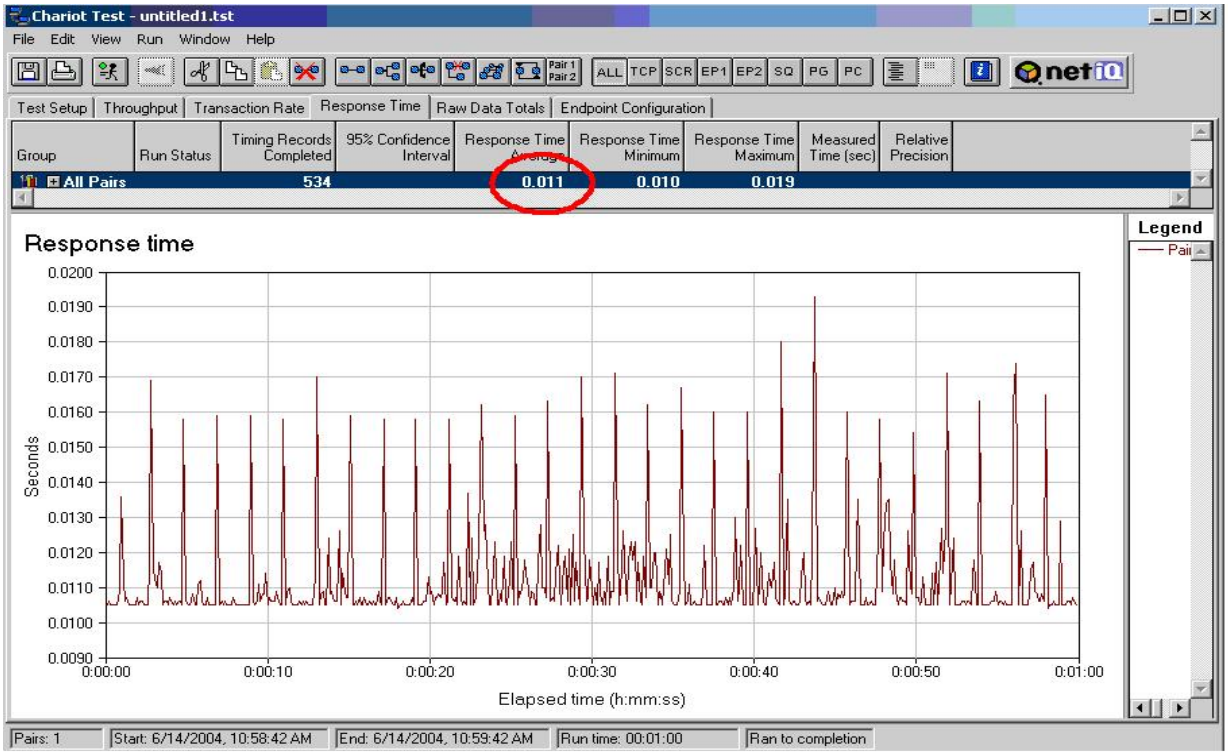


Figura 17: Gráfica de Latencia de Paquetes. Enlace a 1Gbps usando un Crossover.

III.4 Consideraciones Finales.

En este capítulo se han identificado y desglosado las partes más importantes de un sistema de gestión para una intranet, y en específico para la intranet de la Universidad Central

Por tanto se trata la implementación y configuración de los servicios a prestar en los equipos conmutadores, y la solución de gestión valorada mediante el uso del software de supervisión previsto, el cual ha sido seleccionado en un estudio anterior al presente, también se inspeccionan aspectos que cubren la configuración de este software.

Se muestran los resultados de las pruebas de tráfico realizadas en el *backbone*, donde se puede observar el cambio en las características de los enlaces interfacultades.

Conclusiones.

Según el trabajo realizado, y basado en los resultados obtenidos durante esta etapa de estudio se puede arribar a las siguientes conclusiones:

- La administración de redes y el uso de protocolos que auxilian la gestión y supervisión de equipos y servicios existentes en una red de computadoras es un mundo que sufre grandes cambios progresivos en los días de hoy. En la UCLV el estudio continuo de estas tendencias es una necesidad para mantener actualizados tanto a las tecnologías que se usan como a las personas que tienen que ver con ellas.

- El análisis y caracterización de la estructura actual de la Red UCLV permitió conocer con profundidad la red en la cual se desarrolla el sistema de gestión, además de encontrar varias deficiencias que obstaculizan el desempeño óptimo de este.

- Una Estrategia de Gestión debe estar regida, primeramente, por el reconocimiento de la red en cuestión y de los servicios que en ella habitan, la implementación de un equipamiento que brinde un buen soporte para estos servicios y su administración, y una plataforma de gestión que generalmente es desempeñada por un software, en el cual se puede reunir toda la información necesaria para la supervisión de la red.

- Como elemento clave para la estrategia de gestión, se mostró la configuración de los *switch* gestionables y sus capacidades, algunas de estas son: servicio de RAS, servicio de autenticación de usuarios de acceso remoto, estructuración de redes virtuales (VLAN), ruteo, SNMP, filtrado de paquetes, asignación de

direcciones, sincronización de relojes, mensajes de control de errores, conexión desde equipos remotos, registro de eventos e historiales, correo electrónico y el servicio Web.

- El establecimiento del programa supervisor *Nagios* mostró sus amplias posibilidades como plataforma de gestión a nivel de intranet. Durante su etapa de montaje y prueba se ha demostrado que su uso le ha otorgado más robustez y estabilidad a los servicios de la Intranet.

- Las pruebas de tráfico realizadas en los enlaces hacia las Facultades de Sociales y Eléctrica obtienen resultados positivos que demuestran el perfeccionamiento del ancho de banda sobre el cual se brinda un buen soporte para el montaje de nuevos servicios y aplicaciones en la Intranet Universitaria.

Recomendaciones

Con el propósito de obtener resultados cada vez más positivos dentro del desempeño de la Intranet Uclv y de su perfeccionamiento se proponen las siguientes recomendaciones:

- Orientar el estudio del protocolo SNMP dentro de todos los integrantes del grupo de administradores de la Universidad, con el objetivo de lograr una mejor comprensión de las condiciones creadas con la instalación del nuevo equipamiento.

- Colaborar y trabajar con la programación de módulos que impliquen la ampliación de *Nagios* con redes compuestas por dispositivos SNMP, y con otros elementos que puedan facilitar una implementación menos tediosa y exhaustiva del software.

Referencias Bibliográficas.

AlliedTelesyn – Empresa Allied Telesyn (2004) [En línea] Accesible en http://www.alliedtelesyn.com (Consultado 2003).

Black, Uyless D. (1993). *Computer Networks*. 2da Edición, 436 páginas. Pearson Education POD, EUA.

Breitgand David, Raz Danny, Shavitt Yuval. (2002). *SNMP Getprev: An efficient way to browse Large MIB Tables*. IEEE Journal on Selected Areas in Communications. (4): 656 – 667.

Chen Tomas M., Liu Stephen S. (2002). *A Model and Evaluation of Distributed Network Management Approaches*. IEEE Journal on Selected Areas in Communications. 20(4): 850 – 857.

Feit, Dr. (1993). *A Guide to Network Management.* 674 páginas. McGraw-Hill Professional, EUA.

IANA – Internet Assigned Numbers Authority (2004) [En línea] Accesible en http://www.iana.org (Consultado 2004).

IETF- Internet Engineering Task Force, The. (2004) [En línea] Accesible en http://www.ietf.org (Consultado 2004).

Kazem Sohraby, Zhensheng Zhang, Xiaowen Chu, Bo Li. (2003) *Resource management in an integrated optical network* IEEE Journal on Selected Areas in Communications. (7). 1052-1062.

Keisuke Ishibashi, Mika Ishizuka, Masaki Aida, Shin-ichi Kuribayashi (2004) *Capacity Dimensioning of VPN Access Links for Elastic Traffic in the Hose Model.* Vol.E87-B (1) 132.

Kim Myung Sup, Choi Mi-Jeong, Hong James W. (2003). *Highly Available and Efficient Management System using SNMP and Web*. IEEE/IFIP Network Operations and Management Symposium. (1): 619 – 632.

Lópes Rui Pedro, Oliveira José Luis. (2001) *SNMP for MASIF Platforms*. IFIP/IEEE International Symposium of Integrated Network Management. (1): 313 – 316.

NAGIOS (2004) [En línea] Accesible en http://www.nagios.org (Consultado 2004)

Mauro, Douglas. (2001). *Essential SNMP*. 300 páginas. O'Reilly & Associates, EUA.

McCloghrie, Keith. (1995). *How to manage your network using SNMP*. 549 páginas. Prentice Hall, EUA.

Rose, Marshall T. (1992). *The Simple Book*. 542 páginas. Pearson Higher Education, EUA.

Rose, Marshall T. (1996). *The Simple Book*. 2da Edición, 336 páginas. Prentice Hall, EUA.

Rui Pedro Lopes, José Luís Oliveira. (2003) *Delegation of expressions for distributed SNMP information processing* IM 2003 - 9th IFIP/IEEE International Symposium on Integrated Network Management, no. 1, pp. 395-408.

Shaikh Aman, Goyal Mukul, Greenberg Albert, Rajan Raju, Ramakrishnan K. K. (2002) *An OSPF topology server : Design and evaluation*. IEEE Journal on Selected Areas in Communications. (4): 746 – 755.

Sohraby Kazem. (2003) *Resource management in an integrated optical network.* IEEE Journal on Selected Areas in Communications. (7): 1052-1062.

SNMPC (2002) [En línea] Accesible en http://www.castlerock.com (Consultado 2004).

Stallings, William. (1998). *SNMP, SNMPv2, SNMPv3 and RMON 1 and 2*. 3ra Edición, 640 páginas. Addison-Weslay Pub Co, EUA.

Stallings, William. (2002). *Network Security Essentials*. 2da Edición, 432 páginas. Prentice Hall, EUA.

Stallings, William. (2003). *Data and Computer Communications*. 7ma Edición, 864 páginas. Prentice Hall, EUA.

Suzuki Yasuhiro, Harada Hideaki. (2003). *A Management Design for a LAN-Like Optical Access Network*. Network Management/Operation. E86-B(1): 428.

Tannenbaum, Andrew S. (2002). *Computer Networks*. 4ta Edición, 912 páginas. Prentice Hall PTR, EUA.

Thottan Marina K, Swanson George K, Cantone Michael. (2003) *SEQUIN: An SNMP Network Monitoring System.* Bell Labs Technical Journal. 8 (1): 95 – 111.

Westerinen Andrea, Bumpus Winston. (2003) *The Continuing Evolution of Distributed System Management*. IEICE Transactions on Communications. E86-D(11): 2256 – 2261.

Zeltserman David. (1999). *A Practical Guide to SNMPv3 and Network Management*. Prentice Hall. USA.

Anexos.

Anexo I: Estandarización de versiones y RFCs.

La IETF [IETF] es la responsable de la definición de los estándares que gobiernan el tráfico en Internet, incluyendo SNMP. La IETF publica RFCs (*Request For Comments*), los cuales son especificaciones para muchos protocolos que existen en el reino IP. Las RFC son documentos que deben ser primeramente una propuesta para estándar, luego un *drafts* y solo cuando se aprueben adquieren el nivel de estándar. Aunque en realidad existen muchos menos estándares aprobados de los que realmente se piensa este método ha demostrado ser muy efectivo para encaminar y asegurar el desarrollo de la comunidad IP. Existen otras dos definiciones en el camino de un estándar: histórico y experimental. Estas categorías definen un documento que ha sido remplazado por una definición más nueva y uno que aún no está listo para ser declarado estándar pero que está en fase de pruebas.

En ocasiones resulta un poco difícil encontrar lo que se busca dado el elevado número de RFCs que existen, para facilitar esta tarea en [Mauro, 2001] se aconseja usar un servicio de la Universidad de Ohio disponible en:
http://www.cis.ohio-state.edu/cs/services/rfc/index.html

El sitio http://www.ietf.org/ es el lugar donde oficialmente se encuentran todas las RFCs existentes. Todo centro que posea redes de computadoras debe disponer de un lugar donde esté disponible una copia de estos documentos para garantizar su alcance a la comunidad científica. En la Universidad Central "Marta Abreu" de Las Villas este lugar es ftp://neumann.uclv.edu.cu/doc/rfc-all/.

Anexo II: Representación de Datos.

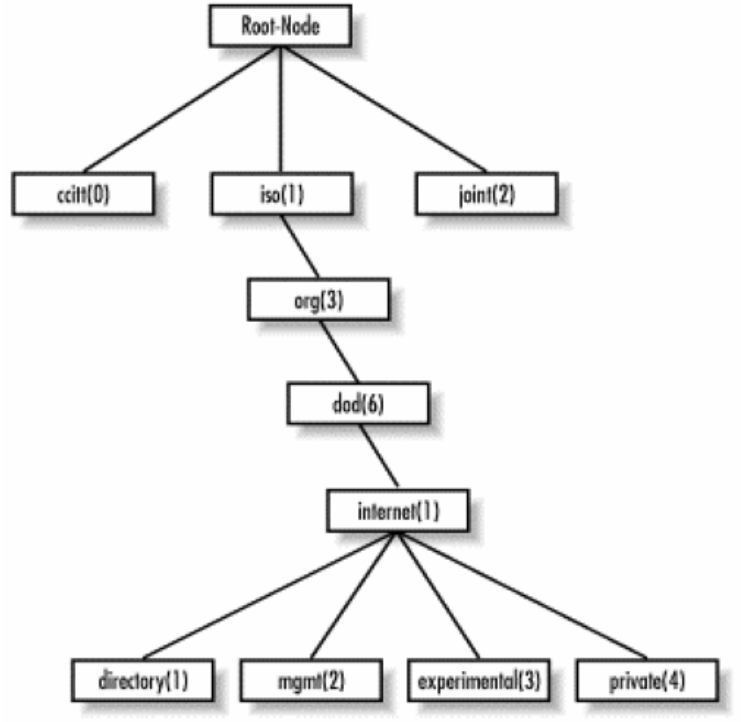
El primer paso es comprender cómo son representados los datos en el contexto de SNMP. SMIv1 (*Structure Management Information version 1*) define exactamente eso. En [RFC-1155] se explica y se especifica cómo son nombrados y de qué tipo son los objetos

gestionados (*managed objects*) más comunes, o sea los considerados estándares, y en [RFC-2578] se declara una mejora aplicable a SNMPv2. [Breitgand, 2002].

La definición de los objetos gestionados puede ser clasificada en tres partes:

- Nombre: El nombre o el *object identifier* (OID) que representa a un objeto especifico. Se puede mostrar en dos formas: numérico o en una cadena de caracteres entendible por humanos. En cualquiera de los casos es algo muy largo y difícil de memorizar. En las aplicaciones SNMP se dedica gran parte del trabajo a ayudar a los administradores a navegar a través de estos OID.
- Tipo y sintaxis: El tipo de datos de un OID es definido usando ASN.1, esta es la forma de especificar cómo los datos serán representados y transmitidos entre el *manager* y el agente. Lo bueno acerca de ASN.1 es que no depende de la arquitectura de la máquina, facilitando así la comunicación entre por ejemplo una estación Windows y un SPARC con UNIX de Sun.
- Codificación: Una instancia de un OID esta codificada en una cadena de octetos usando BER (*Basic Encoding Rules*). BER define cómo los objetos son codificados y decodificados para que puedan ser transmitidos sobre el medio de transporte.

Los OID están organizados en una jerarquía en forma de árbol de tres ramas iniciales. Esta estructura es la base del esquema de nombres de SNMP. El identificador de un objeto está compuesto por una serie de enteros separados por puntos que se obtienen de la ruta desde el inicio del árbol hasta el objeto en cuestión. En el esquema 1 se detallan algunos niveles de este árbol. [Mauro, 2001]



Esquema 1: Árbol de Objetos SMI.

La parte superior del árbol de objetos es llamada raíz o *root*, cualquier nodo con hijos se conoce como *subtree* y cualquier nodo sin hijos es llamado hoja o *leaf.*

Cuando se habla por ejemplo del nodo *mgmt* se puede referenciar de dos formas: la primera es la que se usa en el protocolo y es la secuencia de los números separados por puntos, esto es 1.3.6.1.2. La segunda forma es más usada por las personas y consiste en unir los nombres de los nodos, por ejemplo:
iso.org.dod.internet.mgmt.

La rama *directory* no está en uso actualmente. La rama *mgmt* define un grupo de objetos estándares para la gestión en redes IP, la rama *experimental* por su parte se reserva para objetos de pruebas y de investigaciones. La rama *private* está repartida entre los fabricantes de equipos que soportan SNMP de forma que todos dispongan de un área donde poner objetos específicos de sus equipos.

La definición de estas ramas en ASN.1 sería así:

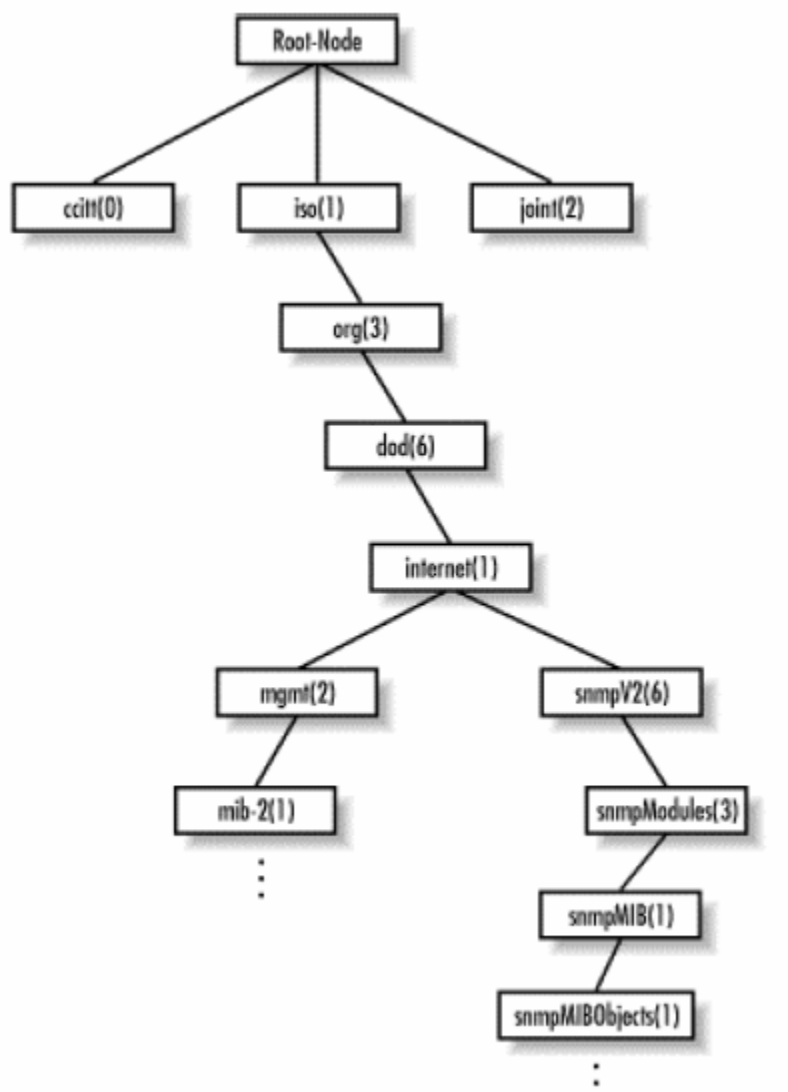
```
internet        OBJECT IDENTIFIER ::= { iso org(3) dod(6) 1 }
directory       OBJECT IDENTIFIER ::= { internet 1 }
mgmt            OBJECT IDENTIFIER ::= { internet 2 }
experimental    OBJECT IDENTIFIER ::= { internet 3 }
private         OBJECT IDENTIFIER ::= { internet 4 }
```

Dentro de la rama *private* es la IANA (*Internet Assigned Numbers Authority*) [IANA] la organización con la responsabilidad de asignar los identificadores a cada persona, empresa o institución que los solicite. Un listado de los números asignados actualmente puede ser encontrado en: ftp://ftp.isi.edu/in-notes/iana/assignmentes/enterprise-numbers/. Como ejemplo puede citarse a Cisco la cual responde al OID 1.3.6.1.4.1.9

Esta definición es bastante fácil de entender, pero no sucede así con las restantes instrucciones de ASN.1. Los tipos de datos de SMIv1 existentes son: INTEGER, OCTECT STRING, COUNTER, OBJECT IDENTIFIER, NULL, SEQUENCE, SEQUENCE OF, IPADDRESS, NETWORKADDRESS, GAUGE, TIMETICKS y OPAQUE. Una explicación más detallada de cada uno de estos puede ser encontrada en [Breitgand, 2002].

La segunda versión de SMI o sea SMIv2 extiende el árbol de objetos agregando una rama llamada *snmpv2* a la rama de Internet, y nuevos tipos de datos tal como se muestra en el esquema 2.

Los nuevos tipos de datos son: INTEGER32, COUNTER32, GAUGE32, UNSIGNED32, COUNTER64 y BITS. Una descripción, completamente detallada, de los tipos de datos que acá se presentan puede ser consultada en [RFC-1442].



Esquema 1: Nueva rama para SNMPv2.

La definición de los objetos, en esta segunda versión de SMI, también cambió ligeramente si se compara con su versión anterior. Aparecen los campos siguientes: UNITSPARTS, MAX-ACCESS, STATUS, AUGMENTS. Los cuales se usan para controlar cómo son accedidos los objetos, para obtener mejores descripciones y para aumentar una tabla adicionando columnas.

Anexo III: *Allied Telesyn*.

Allied Telesis International, cuya sede central se encuentra en Chiasso (Suiza), viene desarrollando su actividad como empresa innovadora en el diseño y la fabricación de soluciones *Ethernet* de alta calidad y bajo costo desde 1987. Fundada sobre una premisa existente de necesidad de productos para redes sencillas pero fiables y compatibles con los estándares, el Grupo *Allied Telesis* salva eficazmente la distancia que separa una amplia gama de productos *Ethernet* para redes. En enero de 1999, la compañía introdujo una iniciativa nueva y muy dinámica para buscar la expansión apoyándose en su principal campo de competencia (*Ethernet*), con el fin de establecer una presencia de liderazgo en el mercado de proveedores de servicios de red. Actualmente, esta iniciativa conocida con el nombre de "*Ethernet & IP All the Way*" está dando lugar a la creación de un amplio espectro de productos que constituyen la línea completa de soluciones de acceso, agregación y transporte principal.

La filosofía de *Allied Telesis* y la firma *Allied Telesyn* siguen siendo las mismas para desarrollar la más avanzada infraestructura de banda ancha, igual que ha ocurrido a lo largo de la historia de la compañía como líder de soluciones *Ethernet*, es decir, proporcionar tecnología sencilla pero potente que pueda utilizar el mundo, a un precio asequible. La iniciativa *Ethernet & IP All the Way* está basada en el conjunto de protocolos más popular, el protocolo estándar utilizado por Internet y todos los servidores y ordenadores que acceden a la World Wide Web. El estado del IP como estándar de Internet demuestra la posibilidad de transportarlo a través de una red global y heterogénea de sistemas y medios diferentes, no muy distinta de la infraestructura de cable de fibra óptica en expansión que existe en todo el mundo. Como líder mundial en la conversión de medios, *Allied Telesyn* goza de una envidiable posición para ayudar a los diseñadores de redes globales de banda ancha y alta velocidad a conseguir que Ethernet se transporte a través de una enorme variedad de trazados de cableado distintos. El Grupo *Allied Telesis* utiliza diversas tecnologías para suministrar los productos que necesitan los proveedores de servicios para ofrecer sus servicios de banda ancha flexibles y fiables a través de redes de área metropolitana, regional, extensa y local; estas tecnologías incluyen conmutación de

banda ancha, transporte a larga distancia por fibra óptica, línea digital de abonado (*Digital Subscriber Line*, DSL), multiplexión por división de la longitud de onda (*Wavelength Division Multiplexing*, WDM), servicios para operadores de telecomunicaciones (E1/T1, E3/DS3) y comunicación inalámbrica.

Con objeto de asegurar la rápida ejecución de *Ethernet & IP All the Way*, *Allied Telesis* sigue invirtiendo en adquisiciones, asociaciones y desarrollos orgánicos, creando una organización para satisfacer la demanda de tecnología de sus clientes de todo el mundo [*Allied Telesyn*, 2004].

Anexo IV: Fichero de configuración.

Fichero de configuración del *switch Allied Telesyn* que radica en la puerta de la uclv. Nótese que se ha hecho referencia solo a unos pocos usuarios locales, ya que colocar la cantidad real haría muy extenso el anexo.

```
#
# SYSTEM configuration
#
set system name="sw.uclv.edu.cu"
set system location="FIE"
set system contact="Grupo de Redes UCLV"
#
# SERVICE configuration
#
# LOAD configuration
#
# USER configuration
#
add user=abelgv
pass=573cdb4e330a5463b8a52893b38a9a0ff677e97ea33e7a4d38a528f3b38a9a0c
lo=no
set user=abelgv desc="Abel Goya Valdivia" netmask=255.255.255.255
add user=abreu
pass=571c9b1b36144b4d98a528d3b38a9a0ff677e97ea33e7a4d38a528f3b38a9a0c
lo=no
set user=abreu desc="Jose Abreu" netmask=255.255.255.255
add user=acebo
pass=8c1c9a1b310e4a7e98a52893b38a9a0ff677e97ea33e7a4d38a528f3b38a9a0c
lo=no
set user=acebo desc="Jose Luis Acebo Puentes" netmask=255.255.255.255
```

```
add user=agarcia
pass=371c8849535b0f2a9dcb4192b38a9a09f677e97ea33e7a4d38a528f3b38a9a0c
lo=no
set user=agarcia desc="Agustin Garcia Rdguez" netmask=255.255.255.255
add user=aldo
pass=b71c8d110d0c4a7d9ba52883b38a9a0ff677e97ea33e7a4d38a528f3b38a9a0c
lo=no
set user=aldo desc="Aldo Oliva Gonzalez" netmask=255.255.255.255
add user=aleidaa
pass=b71c8c17175f3b61b48b06c3b38a9a0ff677e97ea33e7a4d38a528f3b38a9a0c
lo=no
set user=aleidaa desc="Aleida Alfonso Mestre" netmask=255.255.255.255
add user=alfredog
pass=261c8d0c5c4e1b3f89c847c3b38a9a0ff677e97ea33e7a4d38a528f3b38a9a0c
lo=no
set user=alfredog desc="Alfredo Gonzales Morlaes" netmask=255.255.255.255
#
# TTY configuration
#
# ASYN configuration
#
set asyn=1 speed=115200 cd=connect ip=172.20.1.241
set asyn=2 speed=115200 cd=connect ip=172.20.1.242
set asyn=3 speed=115200 cd=connect ip=172.20.1.243
set asyn=4 speed=115200 cd=connect ip=172.20.1.244
set asyn=5 speed=115200 cd=connect ip=172.20.1.245
set asyn=6 speed=115200 cd=connect ip=172.20.1.246
#
# ETH configuration
#
# BRI configuration
#
# PRI configuration
#
# SWITCH (pre-VLAN) configuration
#
# LAPD configuration
#
# Q931 configuration
#
# PPP templates configuration
#
create ppp template=1
set ppp template=1 idle=100 comp=on
#
# ISDN CC configuration
#
# TDM configuration
#
# SYN configuration
#
# ACC configuration
#
add acc call="RAS-1" dir=answer encap=ppp auth=chap asyn=1
set acc call="RAS-1" ppptemplate=1
set acc call="RAS-1" rscript=nvs:reset.mds
add acc call="RAS-2" dir=answer encap=ppp auth=chap asyn=2
```

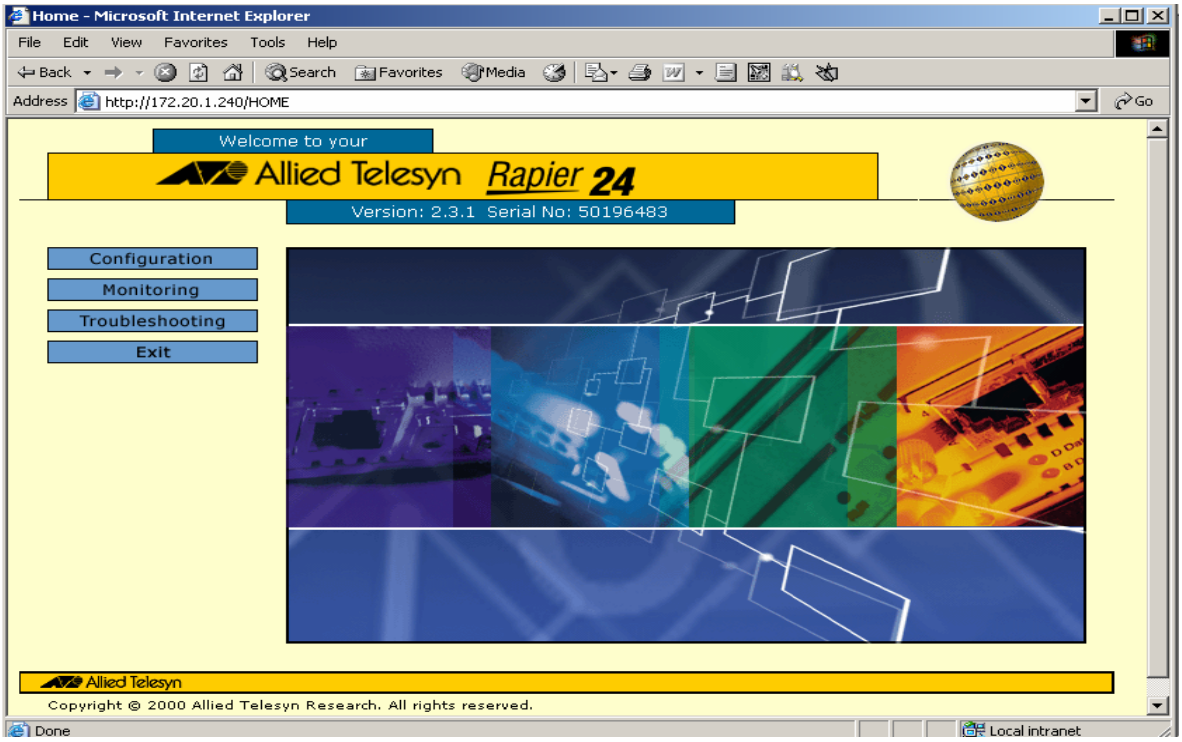
```
set acc call="RAS-2" ppptemplate=1
set acc call="RAS-2" rscript=nvs:reset.mds
add acc call="RAS-3" dir=answer encap=ppp auth=chap asyn=3
set acc call="RAS-3" ppptemplate=1
set acc call="RAS-3" rscript=nvs:reset.mds
add acc call="RAS-4" dir=answer encap=ppp auth=chap asyn=4
set acc call="RAS-4" ppptemplate=1
set acc call="RAS-4" rscript=nvs:reset.mds
add acc call="RAS-5" dir=answer encap=ppp auth=chap asyn=5
set acc call="RAS-5" ppptemplate=1
set acc call="RAS-5" rscript=nvs:reset.mds
add acc call="RAS-6" dir=answer encap=ppp auth=chap asyn=6
set acc call="RAS-6" ppptemplate=1
set acc call="RAS-6" rscript=nvs:reset.mds
#
# X.25 LAPB configuration
#
# X25T configuration
#
# FRAME RELAY configuration
#
# MIOX configuration
#
# L2TP configuration
#
# SA configuration
#
# GRE configuration
#
# VLAN general configuration
#
create vlan="INTERNET" vid=5
create vlan="INTRANET" vid=10
create vlan="INTRANET-1" vid=11
create vlan="INTRANET-2" vid=12
create vlan="INTRANET-3" vid=13
create vlan="INTRANET-4" vid=14
#
# STP general configuration
#
# VLAN port configuration
#
add vlan="INTERNET" port=1-6
add vlan="INTRANET" port=7-10
add vlan="INTRANET-1" port=11-14
add vlan="INTRANET-2" port=15-18
add vlan="INTRANET-3" port=19-22
add vlan="INTRANET-4" port=23-26
#
# VLANRELAY configuration
#


#
# STP port configuration
#
# SWITCH (post-VLAN) configuration
```

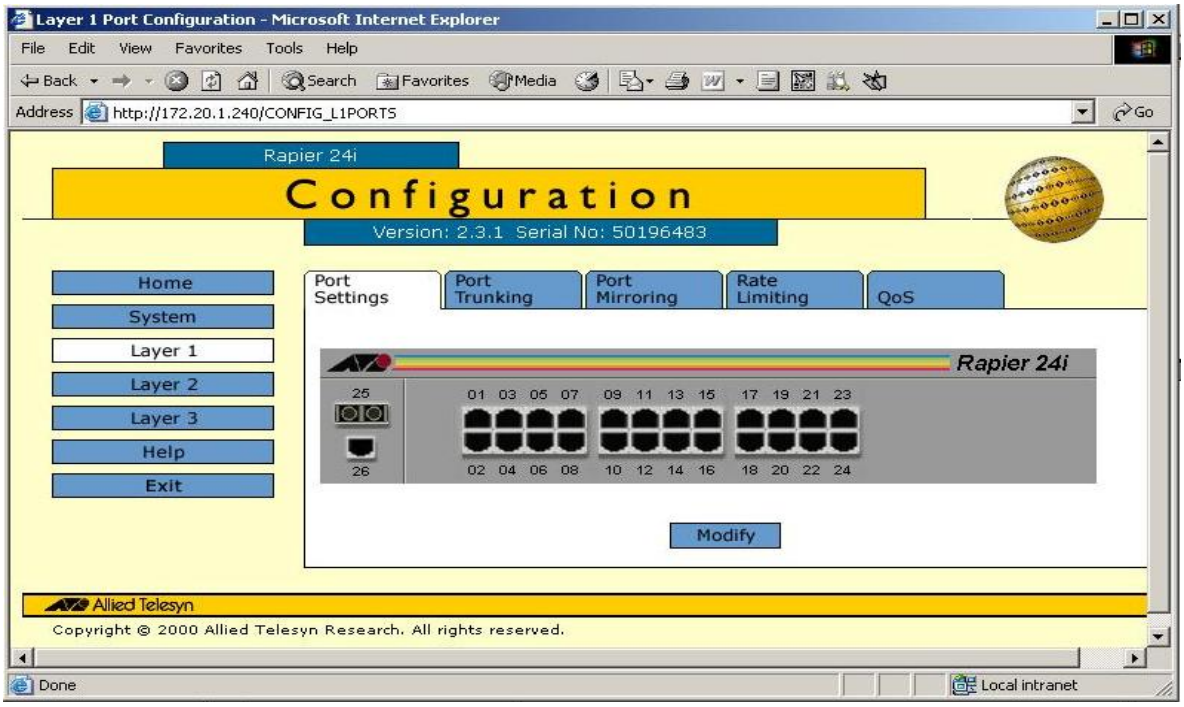
```
#
# PPP configuration
#
# IP configuration
#
enable ip
add ip int=vlan10 ip=172.20.1.240 mask=255.255.255.0
add ip rou=0.0.0.0 mask=0.0.0.0 int=vlan10 next=172.20.1.33
add ip rou=172.20.2.0 mask=255.255.255.0 int=vlan10 next=172.20.1.39
add ip rou=172.20.3.0 mask=255.255.255.0 int=vlan10 next=172.20.1.44
add ip rou=172.20.4.0 mask=255.255.255.0 int=vlan10 next=172.20.1.44
add ip rou=172.20.5.0 mask=255.255.255.0 int=vlan10 next=172.20.1.44
add ip rou=172.20.6.0 mask=255.255.255.0 int=vlan10 next=172.20.1.36
add ip rou=172.20.7.0 mask=255.255.255.0 int=vlan10 next=172.20.1.43
add ip rou=172.20.8.0 mask=255.255.255.0 int=vlan10 next=172.20.1.56
add ip rou=172.20.9.0 mask=255.255.255.0 int=vlan10 next=172.20.1.38
add ip rou=172.20.10.0 mask=255.255.255.0 int=vlan10 next=172.20.1.35
add ip rou=172.20.11.0 mask=255.255.255.0 int=vlan10 next=172.20.1.35
add ip rou=172.20.12.0 mask=255.255.255.0 int=vlan10 next=172.20.1.41
add ip rou=172.20.13.0 mask=255.255.255.0 int=vlan10 next=172.20.1.38
add ip rou=172.20.14.0 mask=255.255.255.0 int=vlan10 next=172.20.1.47
add ip rou=172.20.15.0 mask=255.255.255.0 int=vlan10 next=172.20.1.37
add ip rou=172.20.16.0 mask=255.255.255.0 int=vlan10 next=172.20.1.42
add ip rou=172.20.17.0 mask=255.255.255.0 int=vlan10 next=172.20.1.55
add ip rou=172.20.18.0 mask=255.255.255.0 int=vlan10 next=172.20.1.56
add ip rou=172.20.19.0 mask=255.255.255.0 int=vlan10 next=172.20.1.39
add ip rou=172.20.20.0 mask=255.255.255.0 int=vlan10 next=172.20.1.41
add ip rou=172.20.21.0 mask=255.255.255.0 int=vlan10 next=172.20.1.56
add ip rou=172.20.22.0 mask=255.255.255.0 int=vlan10 next=172.20.1.100
add ip rou=172.20.23.0 mask=255.255.255.0 int=vlan10 next=172.20.1.57
add ip rou=172.20.24.0 mask=255.255.255.0 int=vlan10 next=172.20.1.63
add ip rou=172.20.25.0 mask=255.255.255.0 int=vlan10 next=172.20.1.35
add ip rip int=vlan10 ipaddr=172.20.1.9 send=rip2 receive=rip2
add ip dns prim=172.20.1.5
#
# IPv6 configuration
#
#PIM configuration
#
# X.25C configuration
#
# OSPF configuration
#
# SNMP configuration
#
enable snmp
create snmp community=public0 open=on
#
# INTERFACE configuration
#
set int=ppp0 mtu=1500
set int=ppp1 mtu=1500
set int=ppp2 mtu=1500
#
# FIREWALL configuration
#
# RADIUS configuration
```

```
#
# TELNET configuration
#
# LPD configuration
#
# STREAM configuration
#
# STT configuration
#
# BOOTP configuration
#
# NTP configuration
#
# PING configuration
#
# DHCP configuration
#
# IPX configuration
#
# APPLETALK configuration
#
# ENCO configuration
#
# Secure Shell configuration
#
# LOG module configuration
#
cre log out=1 dest=syslog server=172.20.1.33 secure=no mess=20
add log out=1 filt=1 all
#
# RSVP module configuration
#
# MAIL configuration
#
# TPAD configuration
#
# IPSEC configuration
#
# ISAKMP Configurations
#
# PKI configuration
#
# HTTP configuration
#
# VRRP configuration
#
# GUI configuration
#
# GARP configuration
#
# CLASSIFIER general configuration
#
# BGP configuration
#
# TRIGGER Configuration
#
```

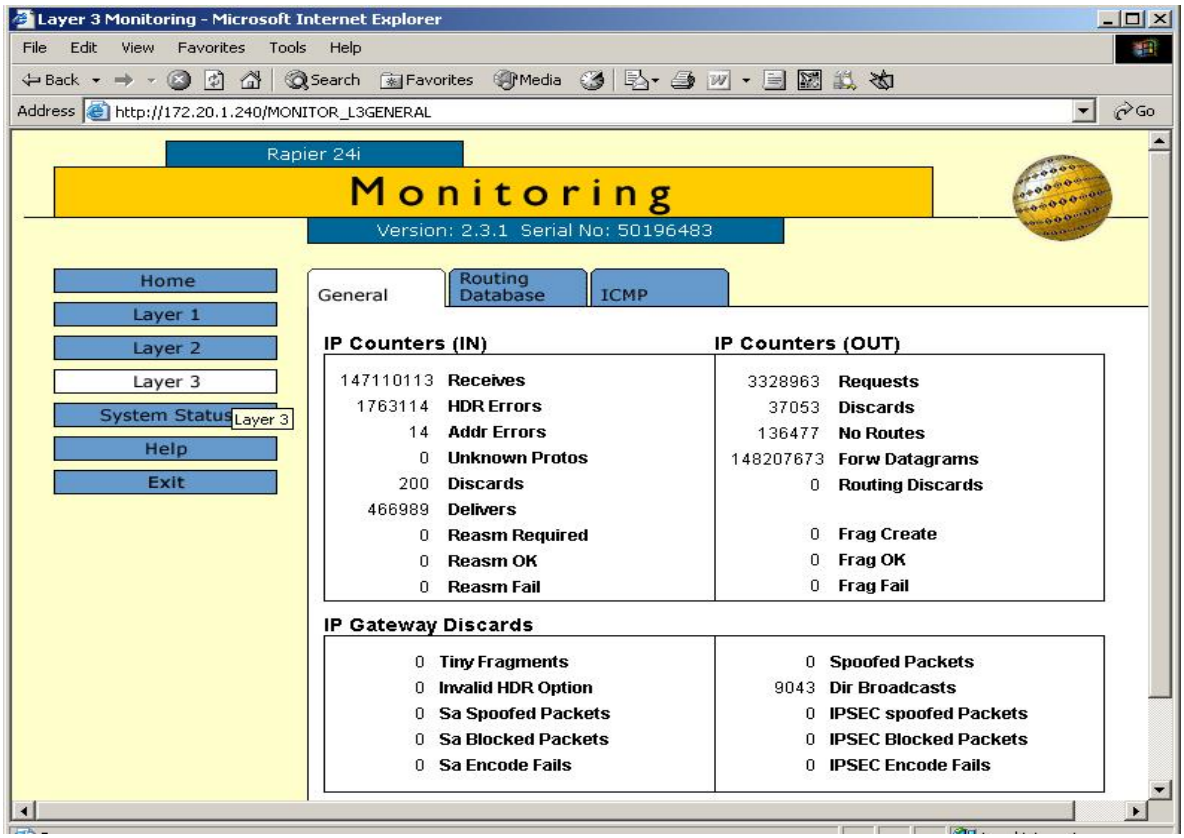
Anexo V: Página de Presentación del Servicio Web.



Anexo VI: Interfaz de Configuración del Sistema.



Anexo VII: Interfaz de Monitoreo del Sistema.



Jose Luis Acebo Puentes
Villa Clara/Cuba
2004.07.01 15:46:05 -
04'00'