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

Reestructuración Tecnológica y Gestión de Red en el *backbone* de la UCLV

Tesis presentada en opción al Título Académico de Master en Telemática

Autor: *Ing. Manuel Oliver Domínguez*
Tutor: *Dr. Francisco Herrera Fernández*

Año 2004

Resumen

Este trabajo trata sobre la Gestión en redes de computadoras y específicamente en la red de la Universidad Central “Marta Abreu” de Las Villas.

Analiza los aspectos teóricos más importantes relacionados con la supervisión y el control en redes de computadoras. Desglosa un canal de gestión típico y explica todos sus componentes. Especifica en cada caso donde encontrar infamación adicional con el fin de profundizar más en temas muy específicos.

Luego del análisis teórico se muestra el caso de la red de la UCLV, viendo los cambios y las modificaciones por las que ha navegado. Se identifican las deficiencias actuales y las necesidades futuras y se plantean un grupo de medidas para solucionar ambos problemas.

Estas soluciones se dividen en dos grupos: los cambios físicos en la red y los cambios lógicos. Los dos grupos están estrechamente relacionados.

Para solucionar los problemas físicos se plantean dos medidas principales: la ampliación del backbone de la UCLV y el mejoramiento de los equipos activos instalados en él.

Por otra parte la elección de los programas encargados de gestionar la información relacionada con el funcionamiento de la red es el eje central de la solución lógica.

Índice

Introducción 1

CAPÍTULO I: Gestión en redes de Computadoras 5

I.1 Introducción al modelo SNMP 5
I.2 Redes Gestionadas *vs* Redes no Gestionadas 6
I.2.1 Los recursos humanos en una red gestionada 7
I.2.2 Características del protocolo SNMP 9
I.2.3 Ventajas y desventajas de SNMP 10
I.2.4 Versiones de SNMP 11
I.3 El protocolo SNMP por dentro 13
I.3.1 Comunidades de SNMP 15
I.3.2 Representación de los datos 16
I.3.3 Extensión de la MIB 20
I.3.4 Operaciones en SNMP 22
I.4 Protocolo RMON (*Remote Monitoring*) 23
I.5 Arquitecturas de NMS 23
I.6 Software de Gestión 26
I.6.1 Agentes de SNMP 26
I.6.2 Estaciones de Gestión 28
I.7 Equipamiento para gestionar una Red 31
I.7.1 Productos Allied Telesyn para redes 31
I.7.2 Ethernet en la capa 3 33
I.8 Sistema Operativo Windows 2000 33
I.8.1 Servicios de Directorios 34
I.9 Sistema operativo Linux 35
I.10 Consideraciones finales 36

CAPITULO II: Cambios en la infraestructura del *backbone* de la Red UCLV 37

II.1 Bosquejo histórico de la Red UCLV 37
II.1.2 *Backbone* de Fibra Óptica 1ra Parte 38
II.1.3 *Backbone* de Fibra Óptica 2da Parte 39
II.2 Deficiencias de la Red UCLV 39
II.3 Proyecto VLIR (*VLAAMSE INTERUNIVERSITAIRE RAAD*) 42
II.4 Mejoras tecnológicas en la Red UCLV 42
II.4.1 *Backbone* de Fibra Óptica 3ra Parte 45
II.4.2 *Backbone* de Fibra Óptica 4ta Parte 48
II.5 Valoración de las mejoras tecnológicas implementadas 48
II.6 Consideraciones finales 52

CAPITULO III: Gestión de red en el *backbone* de la UCLV 53

III.1 Identificación de los elementos a monitorear y controlar 53

III.2 Propuesta de una estructura para lograr una “red más inteligente” 59
III.2.1 Supervisor *Nagios* 60
III.2.2 Programa SNMPc 64
III.3 Desempeño de una “red inteligente” 65
III.4 Respuesta a interrupciones 67
III.5 Consideraciones Finales 68

Conclusiones 69

Recomendaciones 70

Referencias Bibliográficas 71

ANEXOS 73

Introducción

Por todos es conocido la importancia de las computadoras y el papel que estas desempeñan en la vida actual. Si hace 20 años una computadora era algo fuera del alcance de la mayoría de las empresas y personas hoy ocurre todo lo contrario. Las computadoras se han insertado en todos los aspectos de la vida humana, desde que un ser humano nace hasta que muere esta en contacto directa o indirectamente con computadoras. El nivel de dependencia humana hacia las computadoras es algo muchas veces discutido pero nadie lo puede negar.

Los últimos años no solo han visto una evolución y masificación de las computadoras, también han sido testigos de la creación y el desarrollo de las conexiones entre ellas. Hoy en día una computadora aislada de “la red” no se encuentra explotada en su totalidad. Este fenómeno se hace más visible debido a la generalización que han logrado las redes inalámbricas y los dispositivos móviles. Hace unos años los cables de cobre y de fibra óptica monopolizaban el mundo de las redes pero hoy los pequeños dispositivos inalámbricos están descubriendo un mundo nuevo de posibilidades y de aplicaciones.

Con todo este aumento de velocidades, volúmenes de datos y cantidad de estaciones se incrementa también la necesidad de que todo “trabaje bien”. Es evidente que si por un lado se gana mucho con el uso de las computadoras y de las redes de computadoras por el otro se pierde mucho más si estas redes dejan de trabajar o lo hacen con intermitencia. Este es un costo que casi nunca hay que pagar pero que no debemos olvidar que existe.

El mantener una red trabajando “bien” es una labor de personas conocidas como administradores de red y el mantener trabajando las aplicaciones que son las que en realidad “ve” el usuario es responsabilidad de los administradores de sistemas.

Estos dos roles anteriores son a veces confundidos porque pueden estar ubicados en una sola persona siempre y cuando la carga de trabajo no sea muy grande. En el caso de grandes redes con los sistemas es imposible que una sola persona se pueda ocupar de ambos trabajos.

Las vías y los métodos usados para supervisar y controlar el correcto funcionamiento de un red y para aumentar la comodidad y la productividad de los usuarios que la utilizan han sido tema de muchos artículos científicos, libros y de revistas especializadas, es un tema que aun mantiene muchos problemas sin resolver e interrogantes sin respuestas.

En la Universidad Central "Marta Abreu" de Las Villas (UCLV) existe una red de computadoras que ha crecido aceleradamente en los últimos años, actualmente hay alrededor de 1000 computadoras conectadas, 7000 usuarios de tiempo completo y otros 3000 ocasionales. Esto ha aumentado el nivel de exigencia en el trabajo del personal que labora en la red y la rigurosidad en la solución de los problemas relacionados con el funcionamiento de la Intranet. Las fallas son un lujo cada día menos permitido.

Todo este proceso de crecimiento de la Red UCLV ha estado guiado por los administradores de cada una de las áreas, que han creado políticas que responden a sus respectivas necesidades. Lo mismo ocurre con la selección del equipamiento instalado en los nodos que conforman la red. Esto impide que se pueda monitorear y controlar la Red de la UCLV desde un solo punto.

La inexistencia de una estrategia de supervisión y control de los equipos del *backbone* de la Red UCLV y la casi nula gestión de la información relacionada con el funcionamiento de la red constituye hoy día un problema.

Al analizar el problema identificado surgen las interrogantes siguientes:

- ¿Cuáles son las condiciones existentes en las diferentes áreas de la UCLV para la asimilación de nuevos servicios y tecnologías informáticas?
- ¿Qué inversiones son necesarias para mejorar tecnológicamente el *backbone* de la Red UCLV?
- ¿Cómo se pudiera supervisar y controlar mejor la red de computadoras de la UCLV?

- ¿Cómo integrar todos los cambios que se hagan dentro de la estrategia de informatización de la universidad, del MES y del país?

Por lo que el objetivo general de este trabajo es crear una infraestructura que facilite la gestión de redes, la supervisión y el control de los equipos conectados al *backbone* UCLV. Para lo cual se ha propuesto ejecutar las tareas específicas siguientes:

- Analizar las condiciones existentes en el *backbone* de la UCLV.
- Caracterizar el proceso de selección de nuevos equipos.
- Diseñar e implementar una estructura para una gestión eficiente de los equipos del *backbone*.
- Documentar el proceso de ampliación de la Red UCLV.

Este trabajo se ha estructurado en: introducción, tres capítulos que abordan las tareas anteriormente citadas, conclusiones, recomendaciones, referencias bibliográficas, glosario de términos y anexos. A continuación se describen brevemente el contenidos de los capítulos de este informe.

Capítulo 1: Gestión en redes de Computadoras.

Este capítulo aborda el estado del arte de la gestión de redes en el mundo actual. Contiene una descripción del modelo SNMP (*Simple Network Management Protocol*), enumera los elementos de un sistema de gestión así como ejemplos de cada una de las partes involucradas. Muchos de los elementos tratados incluyen referencias bibliográficas que permitirán, en caso deseado una ampliación y profundización en el estudio de estos temas.

Capítulo 2: Cambios en la infraestructura del backbone de la Red UCLV.

En este capítulo, que es un poco más práctico, se describe la Red de la Universidad Central “Marta Abreu” de Las Villas. Incluye la historia del *backbone* de esta red y las modificaciones que a través del tiempo se han realizado. Se analiza la red de la UCLV con el fin de identificar las necesidades existentes lo que posibilita la selección del equipamiento a instalar para dar respuesta al objetivo propuesto. Finalmente se presentan gráficas de mediciones de la velocidad de transmisión antes y después de los cambios realizados.

Capítulo 3: Gestión de red en el backbone de la UCLV.

Este tercer y último capítulo aborda la parte de *software* para la gestión de redes, los programas usados para monitorear la red y los parámetros a encuestar. Se enumeran las variables consideradas más importantes para el trabajo de la red y los eventos que de ocurrir pudieran comprometer la estabilidad de los sistemas. Finalmente se explican las plataformas elegidas para implementar la supervisión y el control de la Red UCLV.

En este informe de tesis se han utilizado un conjunto de términos en idioma inglés, sin traducirlos debido al amplio uso que tienen en el ámbito donde se desarrolla este trabajo. Al final del cuerpo del trabajo se anexa un glosario de términos que contiene una descripción más detallada de estos.

CAPÍTULO I: Gestión en redes de Computadoras

En las complejas redes de *routers*, *switches* y servidores 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]

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*). En él se agrupan las áreas consideradas claves en la administración de redes. Estas áreas son: *Fault Management, Accounting Management, Configuration and Name Management, Performance Management, Security Management.* Este modelo tiene una gran importancia académica, 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. En [Stallings, 1998] se dedica el epígrafe 1.1 a este tema.

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. El SNMP 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*) fue desarrollado para controlar *routers*, SNMP puede ser usado para gestionar sistemas basados en UNIX o en Windows, impresoras, *rack* de MODEMs o fuentes de respaldo por solo citar algunos ejemplos. La lista no se limita solo a dispositivos físicos, también pueden ser supervisados servidores de Web, de archivos o de bases de datos.

Otro aspecto de la gestión de red 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. [Stallings,1998]

I.2 Redes Gestionadas *vs* Redes no Gestionadas

Antes de continuar es justo cuestionarse la necesidad de gestionar una red de computadoras, para ello analicemos el ejemplo siguiente:

Si se asume que se dispone de una red local (LAN – *Local Area Network*) de 100 estaciones, entre las que se encuentran algunos servidores WEB, de FTP, de impresión y de bases de datos que contienen la información clave que usan los usuarios de la red para realizar su trabajo y que todas estas estaciones están conectadas a través de varios *switches* que a su vez están enlazados a Internet a través de un

enlace de 2 MB por una interfaz WAN (*Wide Area Network*) de un *router*. ¿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 pues el administrador estaría disponible para solucionarlo; pero si ocurriera un viernes por la tarde, o un domingo la situación sería completamente distinta.

Si además de esto consideramos que red pertenece a una empresa que da servicio a usuarios en Internet puede predecirse que las pérdidas pudieran ser enormes y esto es un gran problema. Un 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 corresponde a los usuarios detectarla y luego se busca a la persona encargada de corregirla. En una red gestionada SNMP se encarga de monitorear los elementos especificados y en caso de detectar cualquier anomalía en su funcionamiento avisa a la persona responsable de solucionarlo. [Held, 1996]

La situación pudiera ser incluso mejor, SNMP puede darse cuenta de que se avecina un problema y alertar sobre eso antes de que en realidad ocurra. 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 Los recursos humanos en una red gestionada

Otro aspecto importante a considerar es desde el punto de vista del reconocimiento social. La administración de redes es casi siempre vista desde el punto de vista técnico, pero tiene una parte más filosófica. En muchas ocasiones es mejor ser “el que arregla las cosas”. Casi nunca se nota a un administrador de redes donde todo trabaja bien, donde nunca existan problemas. Sin embargo todos reconocen “al que arregla rápido las cosas” y “al que soluciona rápido los problemas”, y esta discriminación llega hasta el punto de que el “administrador salvador” puede tener un salario mucho mayor que el “administrador que no se nota”. Douglas Mauro en [Mauro, 2001. p3] también plantea

este problema “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.”

Hay otros aspectos en los que se debe pensar a la hora de crear un sistema de gestión de red, Gilbert Held plantea que 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. [Held,1996]

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 por Douglas Mauro han pasado la “prueba del tiempo” y han demostrado ser la solución perfecta para muchas de las redes existentes, pero eso no debe significar 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]

I.2.2 Características del protocolo SNMP

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*), y hoy día es también aplicable a otras redes que no están basadas en TCP/IP como IPX/SPX.

Existe una gran cantidad de libros y de materiales que describen SNMP. 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.[Mauro, 2001]

El protocolo SNMP está definido sobre un modelo cliente/servidor. El programa cliente, también conocido como *network manager* (administrador de red) o NMS (*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 *MIB object identifiers* (identificadores de objetos de una MIB) 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.[Held, 1996]

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

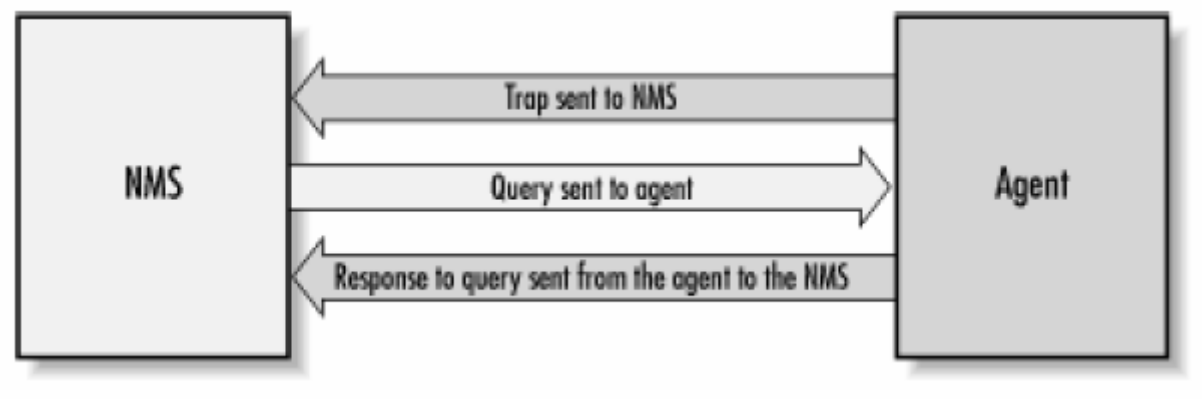

Figura 1 Relación entre un NMS y un Agente

Dada la complejidad de las MIBs , del ASN.1 y de otros elementos que aún no se han mencionado se dedica un epígrafe más adelante para lograr una mejor comprensión.

I.2.3 Ventajas y desventajas de SNMP

SNMP tiene muchas ventajas, pero la principal es su popularidad. 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. [Held, 1996]

Pero como toda obra humana SNMP no es perfecto, tiene algunas debilidades y defectos. Muy al contrario de lo que su nombre dice (*"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. [Mauro, 2001]

La forma en que las variables de SNMP son identificadas (cadenas de *bytes*, donde cada *byte* se corresponde a un nodo en la MIB) es otra forma de gastar espacio en los paquetes de datos.

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

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

La IETF [IETF] es la responsable de la definición de los estándares que gobiernan el tráfico en Internet incluyendo SNMP como ya se explicó anteriormente. 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. [Stallings, 1998]

Actualmente existen tres versiones de SNMP, las cuales se explican brevemente a continuación:

- 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,Cap 4]

- SNMP Versión 2 (SNMPv2): esta es técnicamente referenciada como SNMPv2c, está declarada en la RFC 1905, la RFC 1906 y la RFC 1907. [Stallings,1998,Cap11]

- SNMP Versión 3 (SNMPv3): será la próxima versión del protocolo. Es actualmente un estándar propuesto y está definido en las RFC 1905, 1906, 1907, 2571, 2572, 2573, 2574 y la RFC 2575. Adiciona soporte al uso de métodos mucho más seguros para la autentificación y la comunicación entre las entidades involucradas.[Stallings,1998,Cap 14]

Aunque generalmente se ve como algo muy lejano, la necesidad 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. 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/.

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.

I.3 El protocolo SNMP por dentro

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 sobre TCP (*Transmisión Control Protocol*) 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 el 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 por 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.

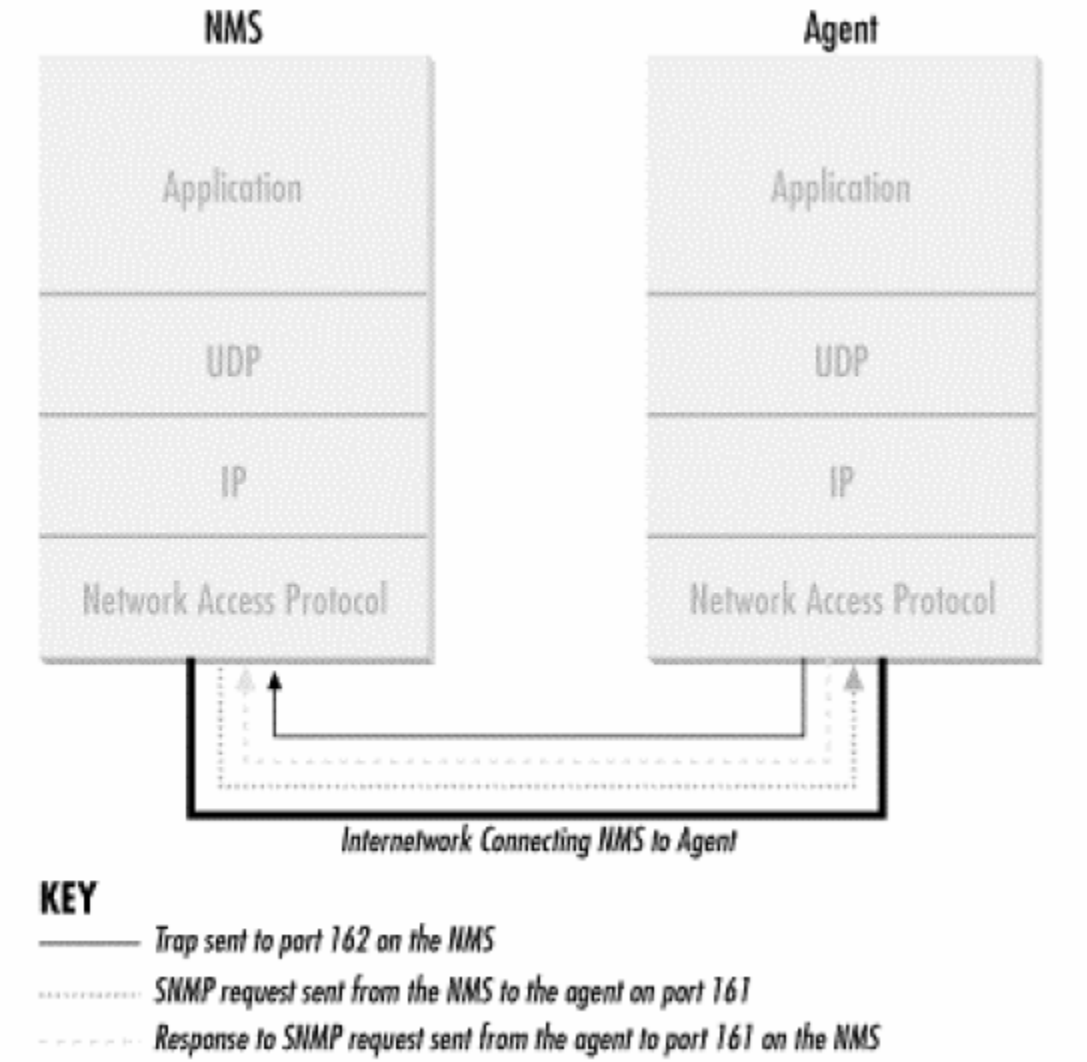

Figura 2 TCP/IP y SNMP

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, o sea el *switch* del ejemplo.

Todo este proceso y las funcionalidades de las tres capas inferiores que se muestran en la Figura 2 estan 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 riego 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 en contra cuando no se toman 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.

I.3.2 Representación de los datos

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.

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 la RFC 2578 se declara una mejora aplicable a SNMPv2. [Held, 1996]

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

- *name*: 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 la Figura 3 se detallan algunos niveles de este árbol.[Mauro, 2001]

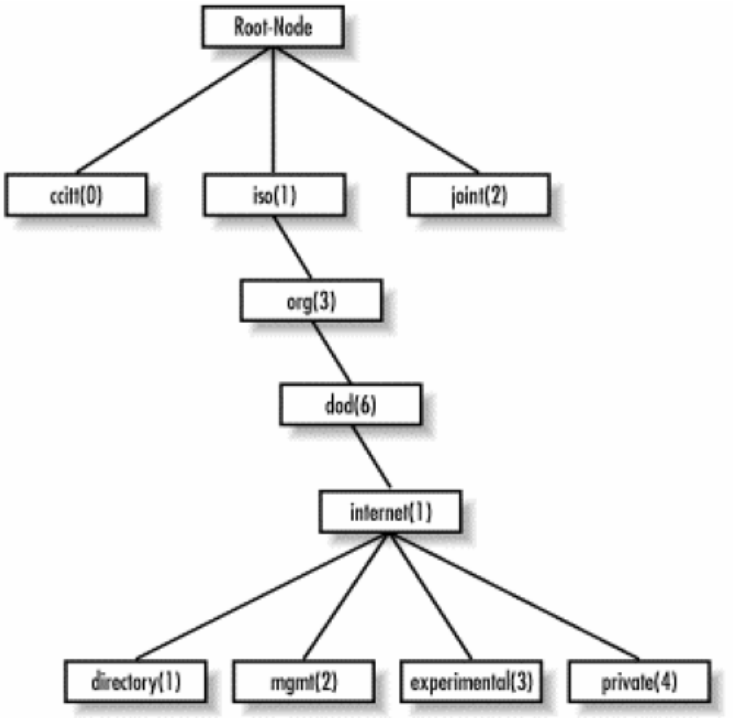

Figura 3 Árbol de Objetos SMI.

La parte superior del árbol de objetos es llamada *root* o raíz, 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 [Mauro,2001].

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 la Figura 4.

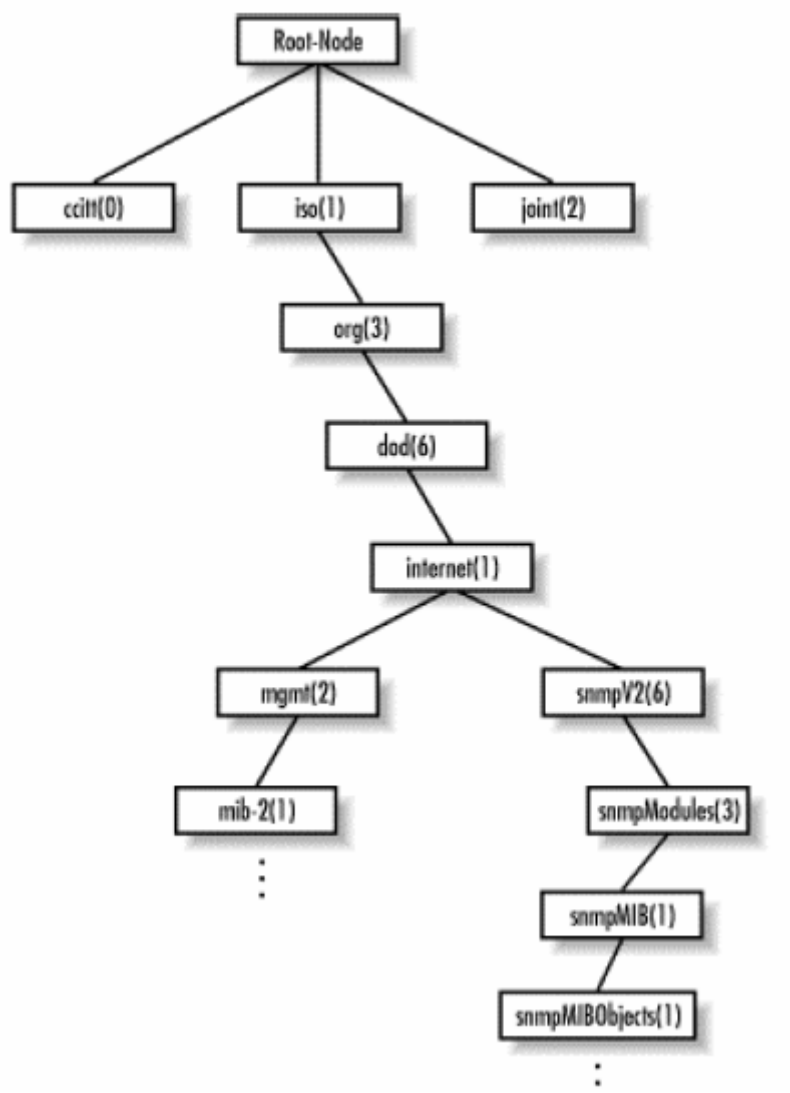

Figura 4 Nueva rama para SNMPv2

Los nuevos tipos de datos son: INTEGER32, COUNTER32, GAUGE32, UNSIGNED32, COUNTER64 y BITS. Una descripción de todos estos tipos de datos puede ser consultada en [RFC-1442].

La definición de los objetos también cambió ligeramente si se compara con SMIv1. 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.

I.3.3 Extensión de la MIB

Con el paso del tiempo los objetos definidos en la MIB estándar resultaron insuficientes para cubrir las necesidades de gestión. Es por ello que se define una extensión: la MIB-II.

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 explicada 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.[Held, 1996]

La extensión que se logra con la inclusión de la MIB-II en la MIB original aumenta la cantidad de ramas del árbol de la Figura 4 y resulta en una estructura semejante a la Figura 5.

Las ramas que se adicionan son:

- *system* (1.3.6.1.2.1.1) define un listado de objetos que están relacionado en la operación del sistema, por ejemplo el tiempo que el dispositivo lleva operando, el nombre de la persona encargada y el nombre del dispositivo.
- *interfaces* (1.3.6.1.2.1.2) mantiene el estado de cada una de las interfaces de las que dispone el agente.
- *at* (1.3.6.1.2.1.3) este grupo solo se brinda para mantener la compatibilidad con versiones anteriores.

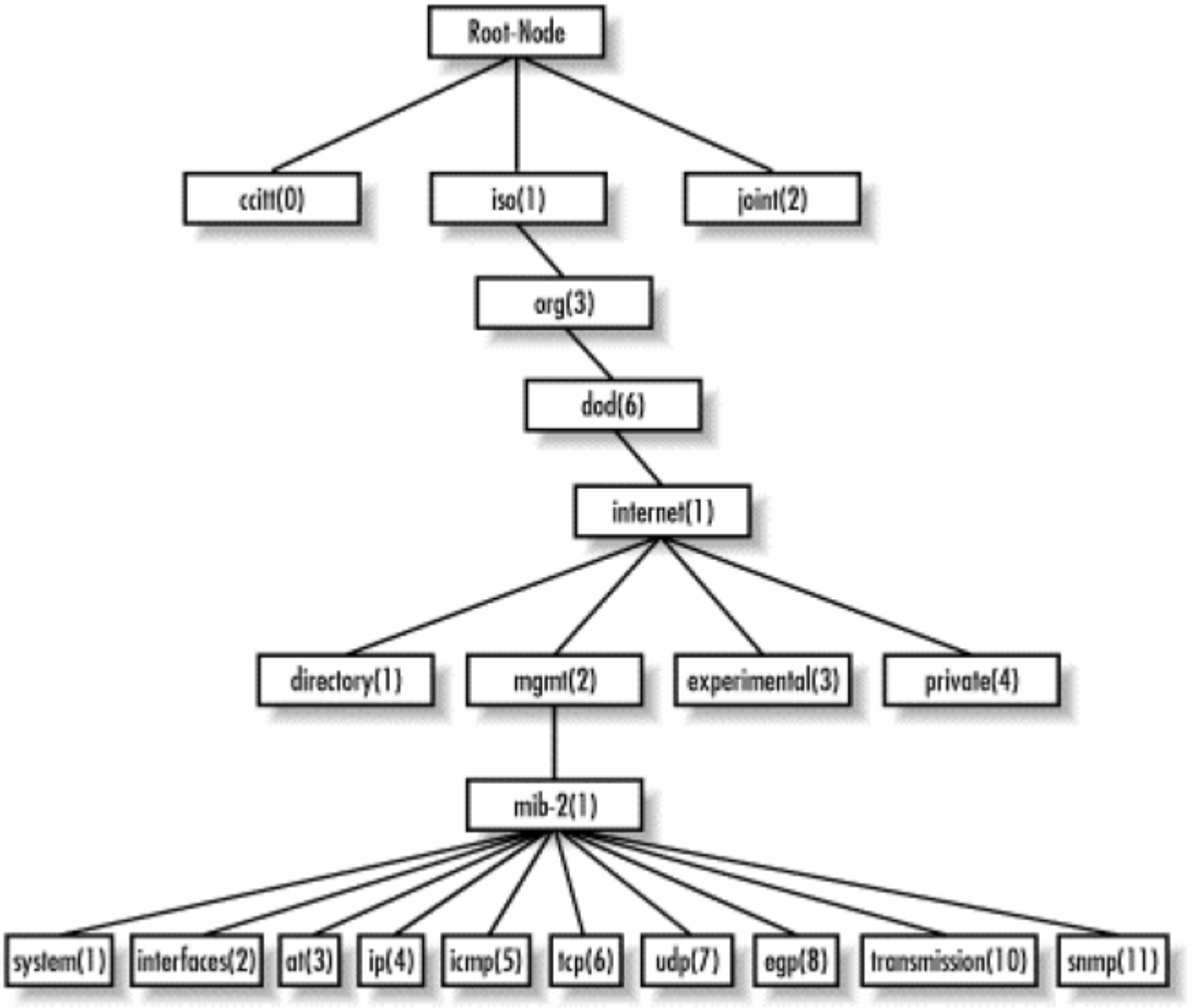

Figura 5 Rama MIB-II

- *ip* (1.3.6.1.2.1.4) mantiene la información de los aspectos relacionados con IP, incluidos el ruteo.
- *icmp* (1.3.6.1.2.1.5) contiene datos relativos al protocolo ICMP (*Internet Control Message Protocol*).
- *tcp* (1.3.6.1.2.1.6) rastrea entre otras cosas el estado de las conexiones TCP, o sea *CLOSED*, *LISTEN*, *SYN_SENT*, etc.
- *udp* (1.3.6.1.2.1.7) mantiene datos pero de conexiones UDP.
- egp (1.3.6.1.2.1.8) mantiene información relacionada con el protocolo EGP (*Exterior Gateway Protocol*) incluidas las tablas de vecinos.

- *transmission* (1.3.6.1.2.1.10) no hay objetos definidos en este grupo pero otras MIBs usan esta rama.
- *snmp* (1.3.6.1.2.1.11) mediciones relacionadas con el rendimiento de este protocolo.

I.3.4 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 RMON (*Remote Monitoring*)

Aunque RMON no es el tema fundamental de este proyecto, es conveniente aclarar algunas nociones básicas relacionadas con su definición y funcionamiento dada existencia de más de una MIB orientada solo a cubrir este protocolo.

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.[Stllings, 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.

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. 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.5 Arquitecturas de NMS

Hasta este momento se han abordado las generalidades del SNMP como protocolo para supervisar y controlar una red, pero no se ha tratado nada respecto a 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 1 Mb de datos, 1.4 Gb por día. Un disco de 40 Gb se podría llenar en un mes.

Quizás el ejemplo anterior es un poco exagerado, el intervalo de 1 minuto es 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, pero no por esto deben ser tomada 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, y ¿cómo se puede esperar una red estable si la estación de control es inestable?

La selección de la estación también dependerá de la arquitectura que se elija, en la Figura 6 se muestra un ambiente de gestión centralizado, donde solo una NMS se encarga de encuestar a todas las estaciones de la red.

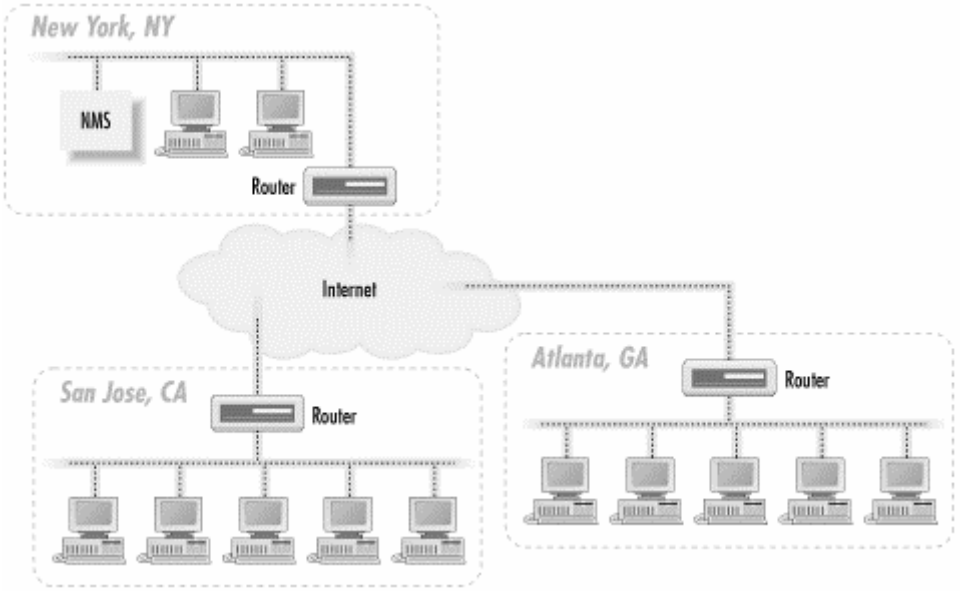

Figura 6 Arquitectura centralizada

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. 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 demasiado.[Mauro, 2001]

Una solución al problema anterior es usar una arquitectura distribuida (ver Figura 7).

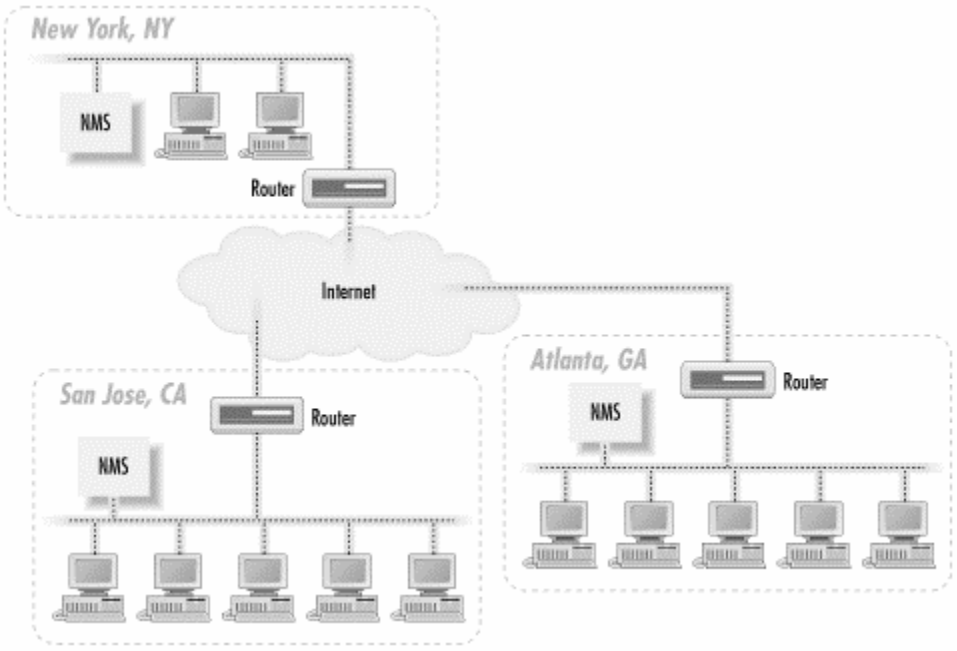

Figura 7 Arquitectura Distribuida

Las ventajas de este método hacen que sea el más usado, 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 es la ofrecida por [001], y consiste en el establecimiento de canales privados solo para las estaciones de control, estos enlaces no deben ser de muy alta velocidad si solo se van a usar para paquetes SNMP.

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, o (en caso de no estar satisfecho con los existentes) 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. A continuación se muestra un resumen de los principales agentes existentes en la actualidad y una breve descripción de cada uno de ellos.

- HP Extensible SNMP Agent
  Plataforma: Solaris, HP-UX
  Ventajas: Incluye el programa *snmptrap* y un agente orientado principalmente a sistemas HP (*Hewlett-Packard*). El agente es extensible usando un subgrupo de instrucciones de ASN.1
  Desventajas: El costo es por dispositivo. Está compuesto por varios *daemons* a los que hay que controlar por separado.
  Más información: http://www.openview.hp.com

- Sun Microsystems
  Plataforma: Solaris

Ventajas: está disponible libre para las últimas versiones de Solaris. El agente es extensible.

Desventajas: Solo soporta MIB-II

Más información: http://www.sun.com

- Concord SystemEDGE

  Plataforma: Windows NT, la mayoría de las versiones de UNIX

  Ventajas: brinda una información muy detallada del sistema, CPU, espacio en disco y aplicaciones instaladas. Está integrado con el servicio SNMP de Windows NT. El agente es muy fácil de extender.

  Desventajas: Es muy caro, a menos que se compre en grandes cantidades.

  Más información: http://www.empire.com

- Microsoft

  Plataforma: 9x/NT/2000

  Ventajas: está integrado en el *kernel* del sistema operativo.

  Desventajas: Solo soporta los requerimientos mínimos. Hay que instalar el *Service Pack* luego de instalar el servicio.

  Más información: http://www.microsoft.com

- Net-SNMP (formalmente proyecto UCD-SNMP)

  Plataforma: Windows, la mayoría de las versiones de UNIX.

  Ventajas: Libre y muy robusto. Muy fácil de extender a través de *scripts*. Incluye un *daemon* para soportar *traps*.

  Desventajas: Documentación muy escasa, lo que hace que sea un opción poco elegida por administradores sin conocimientos avanzados.

  Más información: http://net-snmp.sourceforge.net

- SNMP Research

  Plataforma: UNIX, Windows NT

  Ventajas: dispone de excelentes herramientas para la construcción de un agente.

Desventajas: no está integrado como un servicio, es más bien una herramienta de desarrollo, se necesita de mucho trabajo para lograr que sea útil en otra área.
Más información: http://www.int.snmp.com

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. Con este espectro tan abarcador es difícil encontrar el NMS adecuado porque algunos desarrollan excesivamente una faceta dejando casi sin atender otra. 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. [Twonsend, 1995]

Entre las NMS mas populares se encuentran:

- HP OpenView NNM
  Plataforma: Solaris, HP-UX, Windows NT/2000
  Ventajas: muy bueno para soluciones en redes medianas y grandes. Aunque puede ser chocante a primera vista es muy fácil de administrar a través de interfaces gráficas y páginas WEB. Se pueden obtener licencias para un número infinito de nodos a un precio muy bueno.
  Desventajas: no existen muchos *plug-ins* de otros fabricantes disponibles.
  Más información: http://www.openview.hp.com

- HP OpenView ITO
  Plataforma: Solaris, HP-UX, Windows NT/2000
  Ventajas: orientada a empresas muy grandes, esta orientada a perfiles de usuarios, los mapas, eventos y resúmenes pueden ser mostrados o no en dependencia del usuario. Existe una gran cantidad de *plug-ins* disponibles.

Desventajas: extremadamente caro. No es fácil de lograr explotar este producto sin un entrenamiento adecuado.

Más información: http://www.openview.hp.com

- Tivoli NetView

  Plataforma: OS/390, Solaris, AIX, Digital UNIX, Windows NT/2000

  Ventajas: una solución realmente distribuida, tiene la capacidad de detectar muchos problemas que pueden afectar el trabajo de los usuarios antes de que ocurran.

  Desventajas: es un sistema que requiere de grandes inversiones y recursos antes de ser aplicado.

  Más información: http://www.tivoli.com/products/index/netview/

- 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.

  Más información: http://www.castlerock.com

- BMC

  Plataforma: UNIX, Windows NT/2000

  Ventajas: dispone de bases de datos con la solución de muchos de los problemas que ocurren en las redes.

  Desventajas: las bases de datos son propietarias, el costo es alto. No se usa SNMP como lenguaje nativo.

  Más información: http://www.bmc.com

- Computer Associates Unicenter TNG Framework

  Plataforma: UNIX, Windows NT/2000

  Ventajas: puede ayudar a administrar la red completa, todo lo existente en un sistema tradicional de gestión es almacenado en un servidor Oracle de bases de datos.

Desventajas: es otro sistema muy difícil de instalar y configurar, puede tomar gran cantidad de tiempo.

Más información: http://www.cai.com

- Veritas NerveCenter

  Plataforma: Solaris, HP-UX, Windows NT/2000

  Ventajas: usa modelos de comportamiento (máquinas de estado finitas) para modelar situaciones reales. NerveCenter está diseñado para ser usado como una estación de encuesta independiente o para apoyarse en los mapas gráficos del OpenView.

  Desventajas: es mas difícil de configurar y de mantener que el OpenView.

  Más información: http://www.veritas.com

- OpenRiver

  Plataforma: Solaris.

  Ventajas: esta compañía dice que sus sistemas no necesitan intervención humana, dispone de capacidad para descubrir dispositivos capa 2 y 3 y tiene un precio muy bueno.

  Desventajas: no esta disponible para muchos sistemas operativos.

  Más información: http://www.riversoft.com

- GxSNMP

  Plataforma: aquellas que soporten ANSI C

  Ventajas: es un programa libre, dispone de varias herramientas para la creación de mapas y está integrado con SQL.

  Desventajas: no soporta creación de mapas por descubrimiento de agentes. Es un proyecto relativamente joven.

  Más información: http://www.gxsnmp.org

- OpenNMS

  Plataforma: cualquier que soporte JAVA

  Ventajas: es un intento para brindar a los usuarios un producto abierto. Está escrito en JAVA y se distribuye con licencia GPL.

Desventajas: Es un proyecto relativamente joven.

Más información: http://www.opennms.org

- 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 poco tedioso de configurar.

  Más información: http://www.nagios.org

I.7 Equipamiento para gestionar una Red

El equipamiento es el último punto de la cadena de un sistema de gestión. 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 empresa. Esto se hace 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.

Dada la extensa lista de fabricantes que existe actualmente que producen equipamiento compatible con SNMP y la abundante información disponible solo se abordará uno de ellos. Un listado más detallado de fabricantes puede ser encontrado en [Mauro, 2001].

I.7.1 Productos Allied Telesyn para redes

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. De ese tema se tratará en el próximo capítulo. En este epígrafe solo se brindará información de la posición en el mercado de esta empresa y de algunos de sus productos fundamentales.

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 simples 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 marca *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 [AlliedTelesyn].

I.7.2 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 Sistema Operativo Windows 2000

Aunque el objetivo principal de este trabajo está relacionado con la supervisión y el control de redes de computadoras es importante tener clara la idea de que una red no es importante por el equipamiento que tenga instalado, sea este gestionable o no. Es evidente que una buena infraestructura ayuda a mantener la estabilidad que se necesita en toda red pero las redes de computadoras “valen” por los servicios que ejecutan. Si estos son útiles y trabajan a tiempo completo la red cumplirá con su objetivo en caso contrario solo se tiene una tela de araña de cables y cajas muy cara.

Windows 2000 y Windows 2003 son los últimos sistemas operativos para servidores de Microsoft, empresa líder en este campo a nivel mundial. Las ventajas que este sistema operativo brinda a nivel de usuarios difícilmente se pueden lograr con otros sistemas operativos para redes (*Network Operating System,* NOS).

Un componente clave en la estructura de Windows 2000 es el manejo de usuarios cuando se usa como servidor de dominio. El *Active Directory* (AD) o Directorio Activo es el encargado de este trabajo.

I.8.1 Servicios de Directorios

Active Directory aparece en Windows 2000 pero la idea no es nueva, desde hace tiempo los servicios de directorios se han usado como vía para organizar la información de usuarios y para facilitar las búsquedas. *Netware* de Novell fue uno de los primeros productos que dio a los servicios de directorios un papel protagónico dentro del sistema operativo. Sin embargo corresponde a Microsoft el mérito de lograr un nivel de integración nunca antes visto en el mundo de las redes, permitiendo la administración casi completa de todos los elementos que se integran en una red a través del AD y de sus políticas.

Las ventajas de AD pueden ser resumidas así:

- Integración con DNS: el DNS es un punto fundamental en el funcionamiento de AD. A través del DNS se conocen los servidores que se encuentran en la red y los roles de cada uno.

- Extensible: los administradores pueden agregar nuevas clases y propiedades al esquema que existe, permitiendo así la adición de atributos propios a la red donde está implementándose este servicio.

- Administración basada en políticas: las políticas de grupos son el medio más sencillo y rápido de aplicar un cambio a un conjunto de usuarios o de computadoras. Por ejemplo tareas como ejecutar una aplicación cada vez que se enciende una estación o cuando un usuario se conecta a la red, pueden ser planificadas desde el servidor de dominio.

- Escalabilidad, se pueden adicionar dominios a medida que aumente la complejidad y el tamaño de la red.

- Replicación de la Información, todos los datos necesarios para el correcto funcionamiento de la red, incluyendo la información relativa a los usuarios se replica entre los servidores de dominios asegurando así que no existan serios problemas si uno de los servidores necesita ser apagado.

- Uso de estándares, con el uso de LDAP (*Lightweight Directory Access Protocols*) y de la version 5 del conocido mecanismo de autentificación *Kerberos*, *Microsoft* garantizó que AD no fuera incompatible con otros sistemas de directorios y de autentificación que existen en el mercado.

Un documento que puede ayudar a explicar mejor todos estos puntos y a ejemplificarlos puede ser encontrado en el sitio Web de Windows 2000 [AD]

I.9 Sistema operativo Linux

El sistema operativo Linux se inició como el proyecto universitario de un individuo, Linus Torvalds (http://www.cs.Helsinki.FI/linux/). En principio surgió como una idea para desarrollar un Sistema Operativo basado en MINIX[1].

Actualmente, Linux es el fruto del trabajo de miles de voluntarios de todo el mundo, que han contribuido a mejorar y añadir nuevas características al sistema. Paralelamente a esto se originó un movimiento enfocado a crear un sistema operativo «libre» (sin restricciones de uso y licencias): el proyecto GNU (http://www.gnu.org). Este proyecto ha permitido el desarrollo de miles de aplicaciones y utilidades. El sistema Linux fue incluido en dicho proyecto y, por tanto, actualmente se habla del sistema «GNU/Linux» al referirnos al sistema completo (sistema y aplicaciones que lo acompañan).

La colaboración de un número cada vez mayor de programadores, aficionados y expertos en UNIX, fue fundamental para llevar a cabo el rápido desarrollo que ha experimentado Linux. Y desde todo el mundo han surgido los aportes que, constantemente, han ido y van mejorando y ampliando las prestaciones de su *kernel* (núcleo).

[1] MINIX fué un Sistema Operativo desarrollado por Andrew Tanembaum con el objetivo de formar a sus alumnos en los detalles de su construcción. Es una versión reducida de UNIX.

Linus Torvalds terminó lo que llamó versión 1.0 en el primer tercio de 1992. Hasta entonces había desarrollado varias versiones iniciales a las que fue aportando la funcionalidad básica.
Hoy día Linux se conoce como un *clon* de UNIX[2] que varios millones de personas utilizan en todo el mundo, movimiento al que, cada vez, mayor número de grandes compañías se están uniendo, aportando soluciones tanto comerciales como bajo licencia GPL (Sun Microsystems, IBM, etc.).

I.10 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.

[2] Existe un grupo de personas que piensan lo contrario e incluso argumentan que: Linux Is Not UniX.

CAPITULO II: Cambios en la infraestructura del *backbone* de la Red UCLV

La Universidad Central "Marta Abreu" de Las Villas es un centro de estudios universitarios cerca de 6000 estudiantes en cursos diurnos y un claustro de casi 1000 profesores. Con más de un kilómetro cuadrado de área y alrededor de 1000 computadoras enlazadas, la Red de la UCLV es una de las más grandes y complejas del país. En los últimos años ha ido en aumento la utilización y el nivel de exigencia de la Red.

Teniendo en cuenta las tendencias actuales en el ámbito de las redes de computadoras, el incremento en el uso de servicios informáticos, el papel de la UCLV dentro de la estrategia de informatización del MES se hace necesario la reestructuración y la ampliación del backbone de la Red UCLV.

II.1 Bosquejo histórico de la Red UCLV

Desde 1995 en la UCLV existían redes de computadoras, estas agrupaban conjuntos de hasta 12 máquinas pero estaban aisladas entre ellas. La tecnología usada en aquel momento estaba basada en cable coaxial y la velocidad de transmisión era de 10 Mb/s. La situación cambió un poco con el pasar de los años y en 1998 ya se disponía de redes a nivel de facultades y de centros de investigación, ejemplo de esto es la red de la Facultad de Ingeniería Eléctrica que con un *backbone* de 10 Mb/s sobre cable CAT 5 enlazaba a siete pequeñas redes que en su mayoría estaban sobre cable coaxial.

Ya en esta época estaba clara la necesidad de instalar una red a nivel de universidad que agrupara y permitiera la interacción de todas las áreas de la UCLV. Los primeros pasos en este camino comprendieron un enlace por par de cobre perteneciente al sistema telefónico de la UCLV, que estaban en desuso, entre el grupo de investigación MERCHISE y la Facultad de Matemática Física y Computación. Otro enlace similar fue establecido con la Biblioteca Central. Las velocidades de

transmisión de estas líneas eran de 19200 bps y se usaron principalmente para el intercambio de correo electrónico. Poco después se creo otra conexión de este tipo con el local que se conoce como “la puerta” y que desde esa época se convirtió en el centro de la red universitaria por su conexión con el proveedor de correo electrónico

II.1.2 *Backbone* de Fibra Óptica 1ra Parte

La Red UCLV diseñada y proyectada en 1998, se terminó de instalar en mayo del 2000, es una red con topología estrella que usa tecnología *Fast Ethernet* y que descansa sobre un *switch* modular capa 3 *LanMaker* 5000 de la empresa israelita *LanOptics*. Este equipo es la base sobre la cual descansa el intercambio de paquetes en la UCLV.

Las conexiones existentes en la primera etapa de la red universitaria se muestran en la Figura 8, se incluyen además las distancias entre los nodos y la cantidad de hilos de fibra existentes.

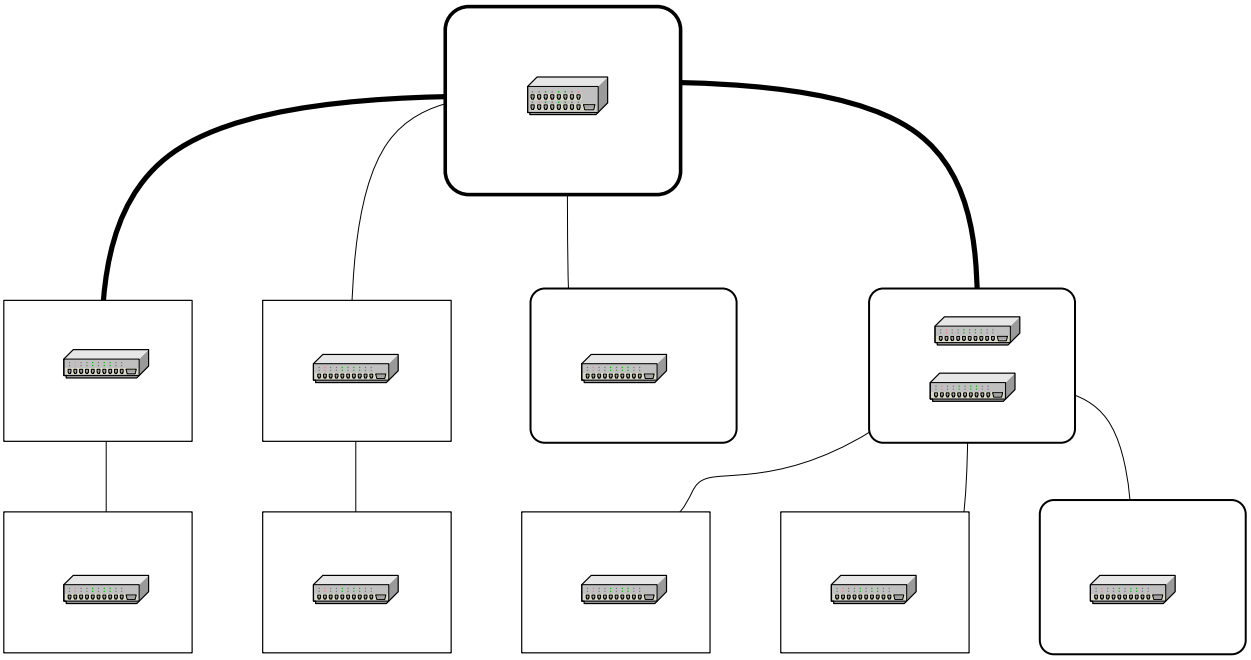

Figura 8 Fase 1 *Backbone* UCLV

Todos los tramos son de fibra óptica multimodo de tipo 62.5/125, el fabricante de estos cables es TELDOR y una especificación técnica de este cable puede ser encontrada en el Anexo 1.

II.1.3 *Backbone* de Fibra Óptica 2da Parte

Debido al éxito en el trabajo de la red, del creciente uso de los recursos compartidos y de facilidades como correo electrónico e Internet, en el año 2002 se instaló y comenzó a funcionar la segunda expansión de la Red UCLV. Este trabajo ya estaba diseñado desde el año 2000 pero por limitaciones económicas no había sido posible su realización.

La expansión posibilitó el acceso de los estudiantes y profesores de las facultades de Ciencias Agropecuarias y de Construcciones a la Intranet universitaria. También zonas como el SEDER, y el Centro de Bioactivos Químicos (CBQ) quedaron conectadas.

En la Figura 9 se pueden constatar las nuevas adiciones. Entre las características técnicas fundamentales que se mantienen esta el uso de fibra óptica TELDOR multimodo 62.5/125 en los nuevos enlaces.

II.2 Deficiencias de la Red UCLV

Aunque el *backbone* que existe en la UCLV funciona y satisface las necesidades actuales no está libre de deficiencias. Desde su diseño y principalmente por limitaciones económicas quedaron algunos puntos débiles en la estructura de la Red UCLV. Con el paso del tiempo y la aparición de nuevos estándares y de nuevas necesidades estas antiguas debilidades se han convertido en problemas reales que impiden el óptimo aprovechamiento de los recursos existentes.

En el momento actual se deben solucionar todas estas limitaciones si se aspira a avanzar un poco más. Algunas de ellas no tienen una solución viable (económicamente hablando) pero su efecto puede ser atenuado con medidas en otras áreas.

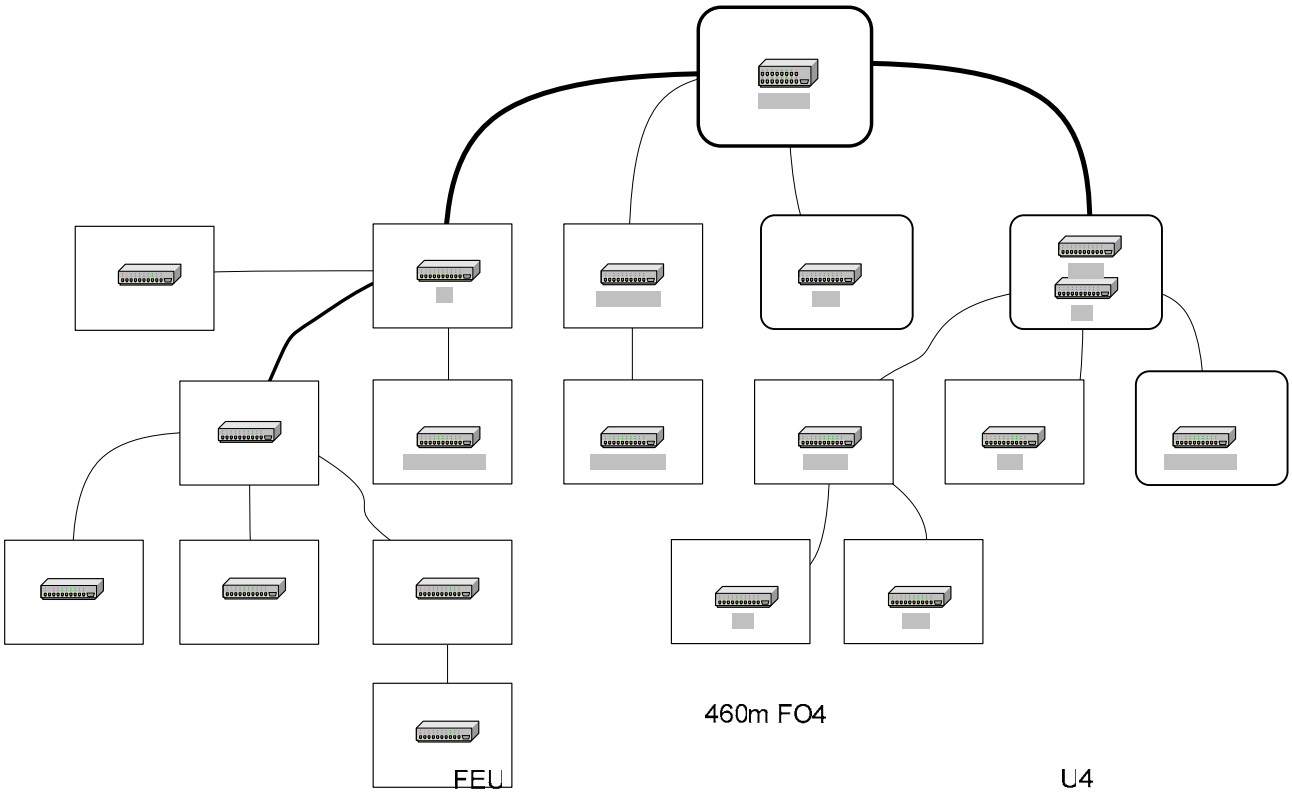

Figura 9 Fase 2 *Backbone* UCLV

De un análisis global del *backbone* UCLV se han identificado los aspectos deficientes que a continuación se detallan:

- Fibra Óptica 62.5/125: Este tipo de fibra está dejando de ser usada. Está siendo sustituida por la Fibra Óptica multimodo 50/125. La cual permite una mejor calidad en la transmisión posibilitando distancias más largas entre el transmisor y el receptor.
- Uso de *patch cords*: En lo centros de cableado como son el CEI (Centro de Estudios Informáticos) y el Edificio U4 se usan *patch cords* para unir dos líneas de fibra óptica para formar un enlace. Por ejemplo en el CEI se une la línea CEI-FIE (Facultad de Ingeniería Eléctrica) con CEI-GRU (Grupo de Redes Universitario). Esto agrega una pérdida adicional al enlace. La solución correcta hubiera sido la fusión de esos hilos de fibras o el establecimiento de un canal directo.

- Escasez de equipos gestionables: Durante las dos etapas de la Red UCLV explicadas anteriormente solo se adquirieron dos equipos gestionables. Uno para el nodo central y otro para la Facultad de Construcciones (FC). El segundo con más prestaciones pues se compró dos años después. Quedó en manos de los responsables de los nodos la elección del equipamiento que se encargaría de soportar las redes locales de cada área.

- *Gateways* no especializados: El direccionamiento IP de la Red UCLV permite a cada área disponer de 256 números IP para sus estaciones de trabajo. Cada área necesita además de un *router* que haga función de *gateway* entre la red local y las demás redes de la UCLV. Estas estaciones, en la mayoría de los nodos, no cumplen con los requisitos mínimos de velocidad, estabilidad y flexibilidad necesarios en los momentos actuales.

- Inexistencia de una plataforma de control: La escasez total de una plataforma de gestión en el *backbone* UCLV y en las redes de cada una de las áreas es otra de las limitaciones actuales. Este punto es en parte consecuencia de los dos anteriores y su solución está ligada a la repuesta que se de a los problemas anteriores. Disponer de un mecanismo para supervisar y controlar la mayoría de las estaciones de la Red UCLV permitiría al grupo de administradores solucionar los problemas que ocurren en un tiempo mucho menor.

- Descentralización de servicios: La descentralización de los servicios fue durante mucho tiempo la solución encontrada a los problemas anteriormente relacionados. Esto posibilitó que cada área continuara funcionando aún cuando el nodo principal dejara de hacerlo. El aumento en la complejidad de los sistemas usados, los costos para elevar la calidad de las estaciones de todos esos nodos y la estrategia para pasar a sistemas abiertos han hecho que sea necesario centralizar los servicios brindados en la Red UCLV. Esto es posible también por la estabilidad lograda en la conectividad de las áreas.

- Aseguramiento y estabilidad en el servicio eléctrico: Esta no es una deficiencia directa del diseño de la red pero sin lugar a dudas es la más visible en el funcionamiento diario. Para lograr que la red trabaje lo mejor posible hay que encontrar una solución total o al menos parcial en

este campo. Las pérdidas en equipamiento anuales en la UCLV por deficiencias en las redes eléctricas, ya sea aterramiento o estabilidad en el voltaje, superan los 30 puertos físicos por año.

Todas estas deficiencias limitan las potencialidades de la Red UCLV, e impiden que sean creados nuevos servicios. La solución a estos problemas está indisolublemente ligada a la disponibilidad de financiamiento en moneda libremente convertible.

II.3 Proyecto VLIR (*VLAAMSE INTERUNIVERSITAIRE RAAD*)

En el año 2003 la UCLV fue aceptada como participante en un proyecto conjunto con el consejo de universidades flamencas. Este proyecto se divide en ocho sub-proyectos de los cuales el primero está orientado a mejorar la infraestructura y a facilitar el proceso de informatización de la UCLV. Este programa tiene una duración de cinco años y es prorrogable a otros cinco dependiendo de los resultados alcanzados.

El sub-proyecto *Information and Communication Technology Infrastructure and E-Administration* es el encargado de encaminar las mejoras tecnológicas en el *backbone* de la Red UCLV, además de potenciar la creación y el desarrollo de aplicaciones para ser usadas por usuarios administrativos. Para ello se dispone de un presupuesto de alrededor de 300 000 euros. Este proyecto puede analizarse más detalladamente consultando el Anexo 2 y para una versión mas completa se anexa un fichero en el CD que acompaña este proyecto.

El financiamiento garantizado durante todo un quinquenio por el proyecto VLIR es la vía expedita que posibilita la implementación de nuevos cambios en la Red UCLV.

II.4 Mejoras tecnológicas en la Red UCLV

Con la existencia de financiamiento para resolver los problemas existentes en la Red UCLV y crear de nuevos servicios desaparece la limitante principal que existía hasta este momento. Queda por establecer el cuerpo que tendrá la solución brindada.

A partir de las deficiencias detectadas y un análisis del problema se decide, dada las características de este, formularlo en dos partes. Una primera parte asociada con los cambios en equipos y una segunda con las modificaciones en el área de los servicios. En este capítulo se aborda lo correspondiente a la primera parte.

Los cambios en equipos pueden subdividirse en dos secciones: equipos para asegurar el tráfico de información y servidores para soportar los servicios existentes.

El aseguramiento del tráfico de información está ligado de forma indisoluble a la calidad de los equipos encargados de la conmutación de paquetes. La calidad de estos equipos es también lo que decidirá las opciones de la red de gestión que será tratada en el próximo capítulo.

Otro aspecto que debe ser tomado en cuenta es que no deben mezclarse equipos de varios fabricantes 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.

Dada las características *backbone* de la Red UCLV y de las modificaciones a realizar se establecen requerimientos que deben cumplir los equipos a instalar. Estos son:

- Capacidad para 24 puertos 10/100 TX.
- Al menos dos expansiones para enlaces por fibra óptica a 100 Mbps y a 1 Gbps.
- Soporte de SNMP, RMON.
- Filtrado de paquetes.
- Creación de redes virtuales (VLANs).
- Calidad de Servicio (QoS).
- Ruteo de paquetes IPv4 y IPv6.
- Soporte de *multicasting*.
- Soporte de RIP (*Routing Internet Protocol*) versión 1 y 2.
- Soporte de OSPF(*Open Shortest Path First*).

Con la especificación de requisitos del equipamiento se procedió a solicitar opiniones a empresas comercializadoras sobre los productos que se comercializan en el país. Los resultados principales de esta indagación fueron los siguientes:

- La línea *Planet* dejaría de ser comercializada.
- Solo se comercializan algunos equipos de AOpen y de 3COM. Resulta muy difícil adquirir equipos como los necesarios pues se salen de la línea "típica" comercializada en el país.
- Las soluciones de *Cisco*, *Allied Telesyn* y de *Extreme Systems* están disponibles.

Por otra parte de un estudio de los equipos existentes en la UCLV se llegó a las valoraciones siguientes:

- Existencia de equipos de *Cisco*, *3COM*, *AOpen*, *Allied Telesyn* y *Planet*. Este último es el predominante.
- Los equipos *Planet* son los más baratos y fáciles de adquirir pero a su vez son los de mayor índice de rotura.

Llegado a este punto se hace necesario un análisis final, el económico. El costo de los equipos marca Cisco es demasiado elevado para el presupuesto existente, lo mismo ocurre con los *switches* fabricados por *Extreme Networks*. Por consiguiente la solución final estará soportada con equipamiento *Allied Telesyn*.

La otra parte del problema, o sea la selección de servidores para soportar los servicios, no es el propósito fundamental de este trabajo por lo que solo se informa la configuración elegida y una breve descripción técnica. Las estaciones usadas como servidores tienen la configuración siguiente:

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

II.4.1 *Backbone* de Fibra Óptica 3ra Parte

La solución propuesta junto con otras modificaciones en la red UCLV puede ser vista como la 3ra actualización o expansión del *backbone* de la Red UCLV. Quizás esta expansión no sea de una magnitud tan grande en cuando a distancias de los enlaces creados si se le compara con sus predecesoras, pero sin duda alguna representa el principal cambio que se ha experimentado hasta el momento en cuando a calidad del equipamiento.

Para la asignación de equipamiento se dividieron las áreas de la UCLV en tres grupos:

- Nodos de elevado tráfico.
- Nodos de tráfico normal.
- Nodos de poco tráfico.

Los nodos de la primera categoría comprenden los centros cableados donde convergen otros nodos. En este caso solo se encuentran el actual GRU y el CEI. En la segunda categoría clasifican la mayoría de los nodos de la Red UCLV, las facultades y algunos edificios administrativos. Y la tercera categoría está destinada a aquellas áreas que no representan una gran carga para el *backbone* de la red, pues solo disponen de pocas computadoras y estas generalmente son manejadas por usuarios “no peligrosos”.

Los *switches* seleccionados para las áreas antes mencionadas son:

- *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 un poco más lento.

Una descripción técnica más detallada de estos equipos puede ser encontrada en los Anexos 3 y 4. La distribución de los equipos por áreas se muestra en la Figura 10.

Además del cambio de los *switches* en las áreas mostradas se propone la creación de enlaces que permitan la conexión de nuevos nodos a la Intranet UCLV. Las áreas a conectar son la Planta de Producción del CBQ, la Facultad de Educación a Distancia y el Centro de Desarrollo de Software.

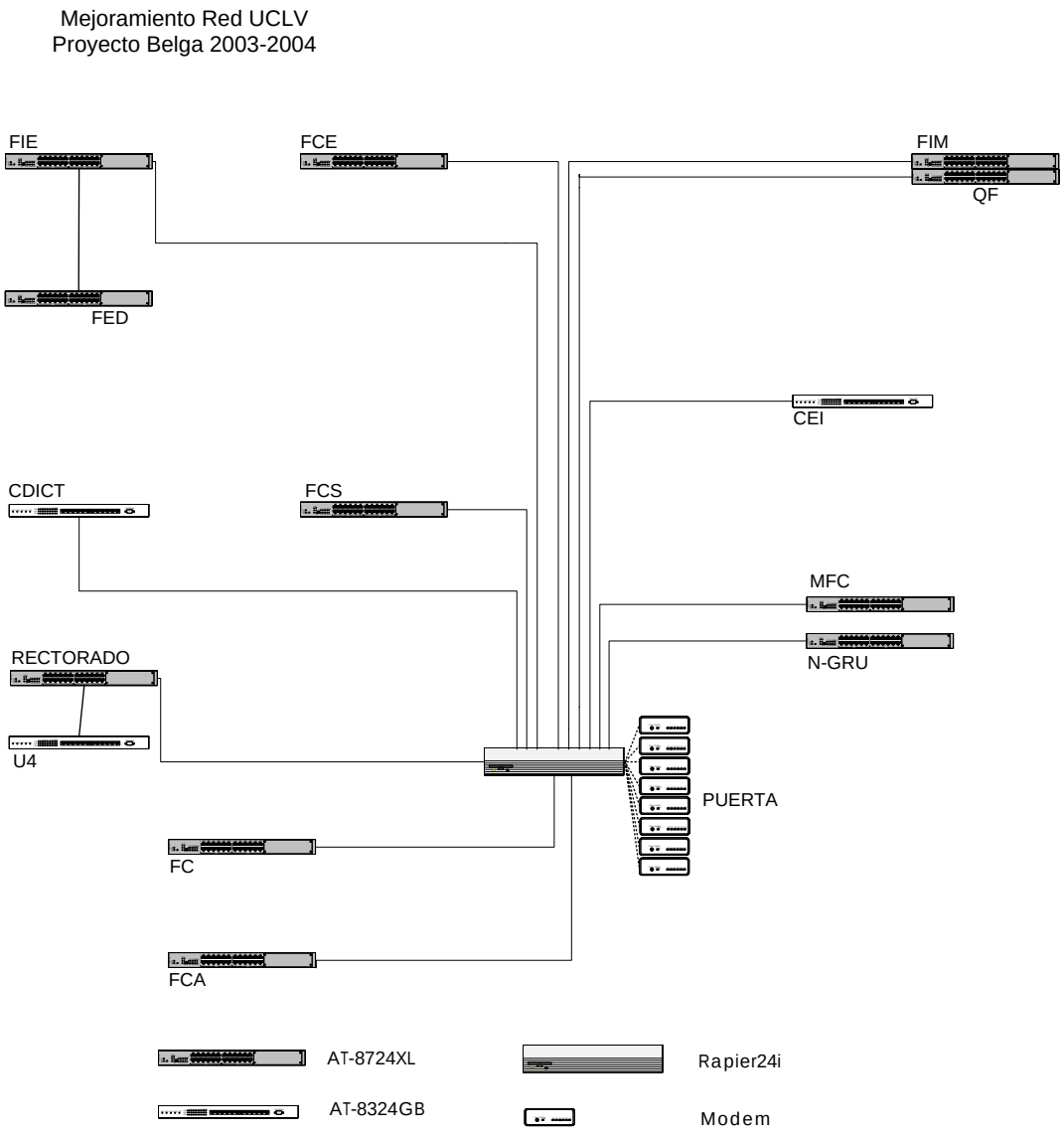

Figura 10 Distribución de los nuevos equipos.

Para la conexión de estas áreas se usan los pares de fibra óptica que quedaron disponibles luego de la segunda expansión de la Red UCLV. En la Figura 11 se muestra los enlaces actuales y los futuros. Estos últimos en color rojo.

Es conveniente reafirmar que se mantiene una de las debilidades señaladas en II.2, el uso de *Patch Cords*. Aunque la cantidad de segmentos disminuyó bruscamente, es imposible, por la implicación económica que esto representa, la eliminación total de estos puntos de pérdidas.

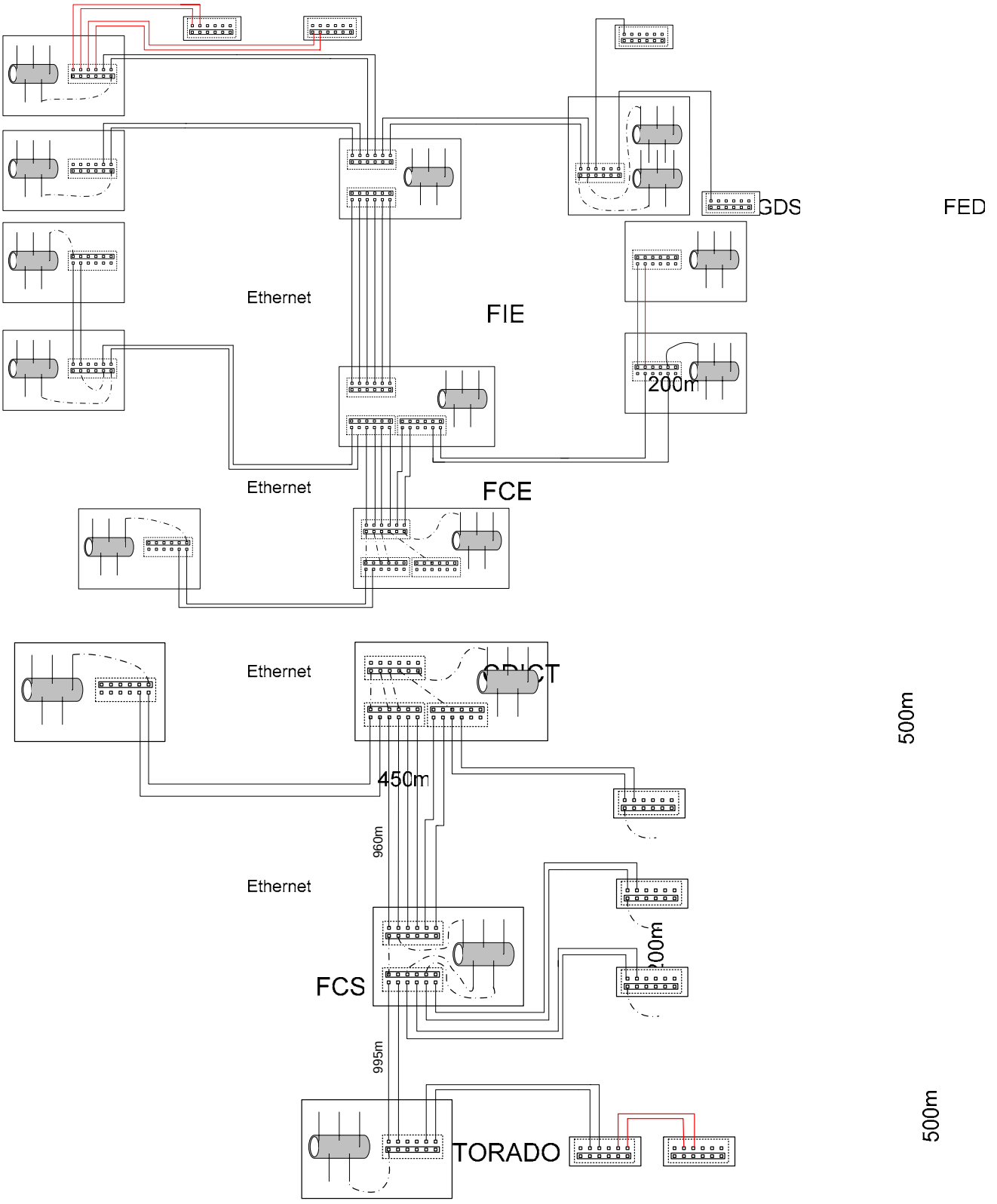

Figura 11 Diagrama de cableado.

II.4.2 *Backbone* de Fibra Óptica 4ta Parte

Esta etapa de cambios deberá finalizarse dentro de dos años, o sea en el 2006. El objetivo fundamental es aumentar la velocidad de transmisión de datos a través del *backbone* de la UCLV desde 100 Mbps a 1000Mpbs. Para lograr esto hay que descentralizar la estructura actual. Debido al tipo de fibra óptica usada (62.5/125) y las distancias entre los nodos se hace necesario establecer otro nodo central en el local del CEI. Esto resuelve la problemática para las áreas de FIE, FCE (Facultad de Ciencias Empresariales), FIM (Facultad de Ingeniería Mecánica) y QF (Facultad de Química Farmacia).

Los nodos que se encuentran en FC, AGRONET (Red de la Facultad de Ciencias Agropecuarias) y la planta del CBQ solo podrán conectarse a la velocidad de 1Gb mediante el uso de extensores, estos también son vendidos por *Allied Telesyn* pero a un costo de 3000 USD la unidad. Existe otra posibilidad que es el cambio de la fibra óptica instalada por una de 9/125, pero el costo de este tipo de fibra y lo complicado del proceso de tendido hacen que la primera opción sea la más viable.

La Figura 12 muestra la estructura de la Red UCLV luego de aplicadas las modificaciones previstas.

II.5 Valoración de las mejoras tecnológicas implementadas

Todo cambio debe estar orientado a lograr mejoras. En el caso que se trata, los cambios en la infraestructura de la Red UCLV están orientados a aumentar la cantidad de usuarios existentes y a mejorar la calidad del servicio que se brinda. Aunque la calidad de un servicio no es algo que dependa totalmente de la infraestructura instalada, si existe una dependencia muy fuerte entre los dos. Con el fin de valorar los resultados de los cambios efectuados se realizaron algunas pruebas para medir la capacidad de transmisión de paquetes entre nodos que están interconectados al *backbone*.

Las mediciones fueron realizadas con el programa *Chariot* de NetIQ, empresa líder a nivel mundial en la administración de redes. Este software es recomendado por algunas empresas especializadas en asesorías a redes de computadoras y dispone de una amplia gama de pruebas pre-configuradas que

pueden ser aplicadas. Es posible además, la creación de nuevas pruebas programándolas con un exhaustivo nivel de detalle.

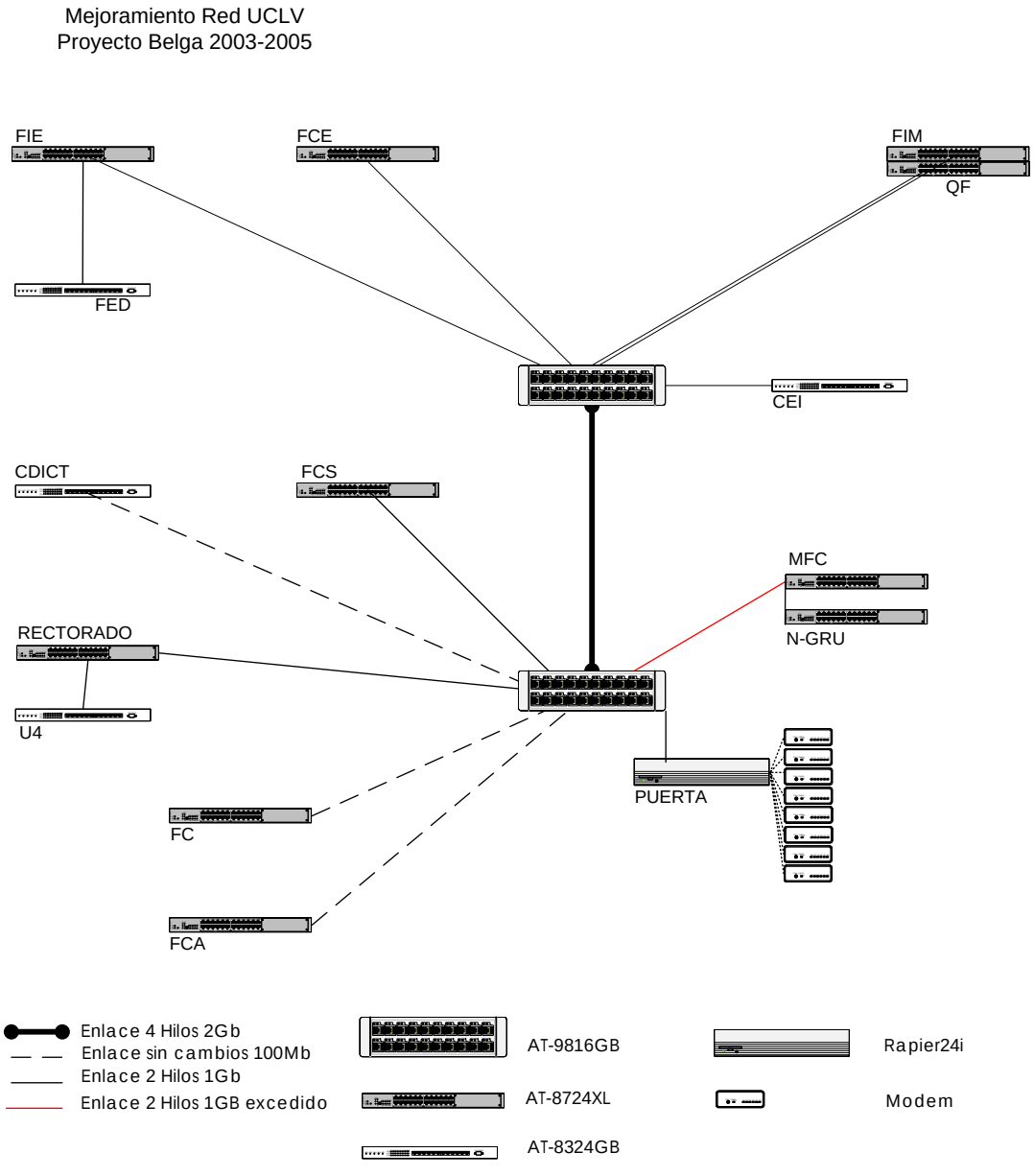

Figura 12 Backbone Gigabit

Los enlaces medidos fueron FIE-GRU y SOCIALES-GRU. La diferencia que existe entre estos nodos es que el primero está compuesto por dos segmentos de fibra y el segundo solo por uno. Las pruebas se

aplicaron dos veces, usando la estructura que existía y usando la que se propone, o sea la que incluye los *switches* de *Allied Telesyn* como *routers*.

Las Figuras 13 y 15 muestran los resultados de las mediciones con la estructura que existía anteriormente y en las Figuras 14 y 16 pueden constatarse las mediciones con la estructura propuesta. Se puede notar en ambos enlaces un aumento de la capacidad de transmisión, que se explica fundamentalmente por la eliminación de los *gateways* usados y de su sustitución por un equipo dedicado y especializado en esta labor.

Antes de concluir este epígrafe es bueno recordar algo que ya fue mencionado: La calidad de *backbone* de la Red de la UCLV no es lo que garantizará el correcto funcionamiento de los servicios brindados. Las inversiones realizadas pueden asegurar la estabilidad y la calidad en la conectividad y el tráfico entre los nodos existentes, ni más, ni menos.

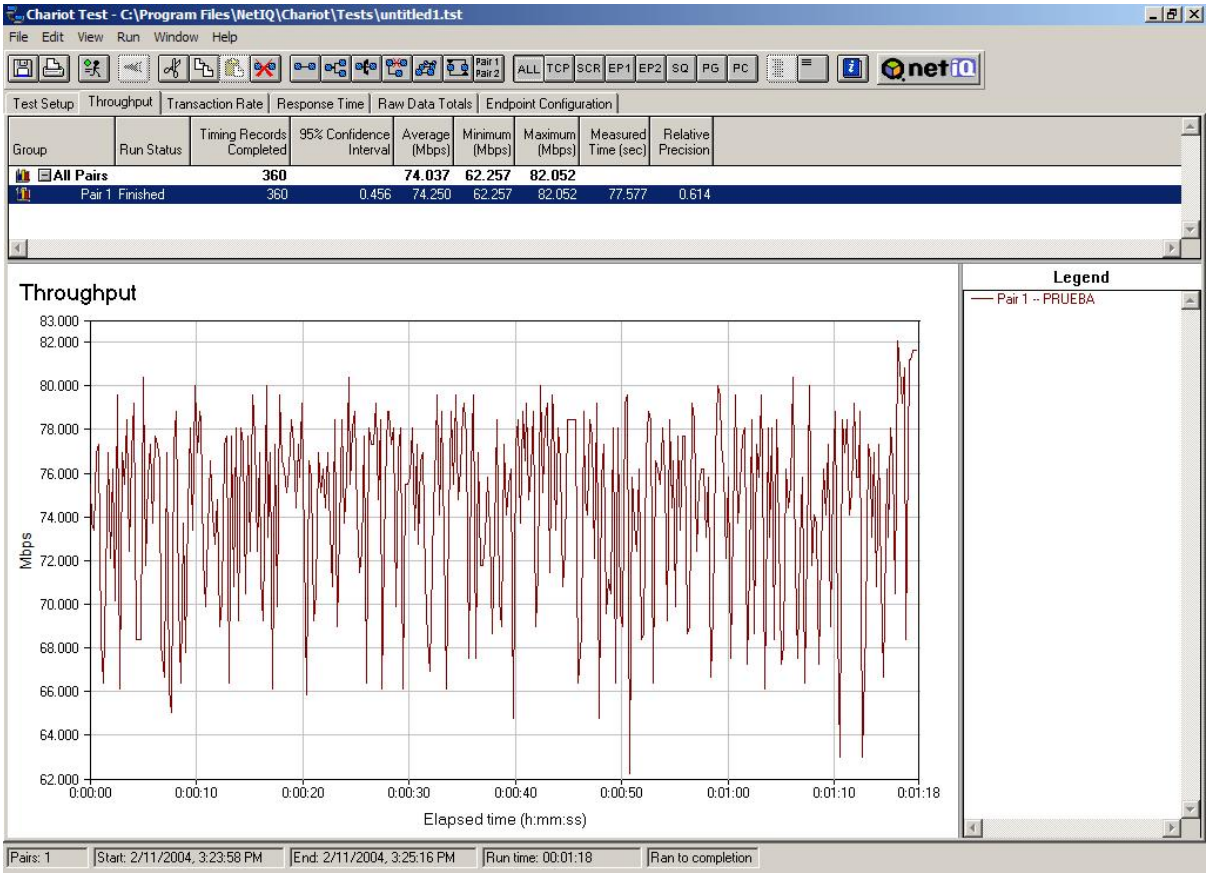

Figure 13 Capacidad del enlace FIE-GRU usando como *gateway* una PC

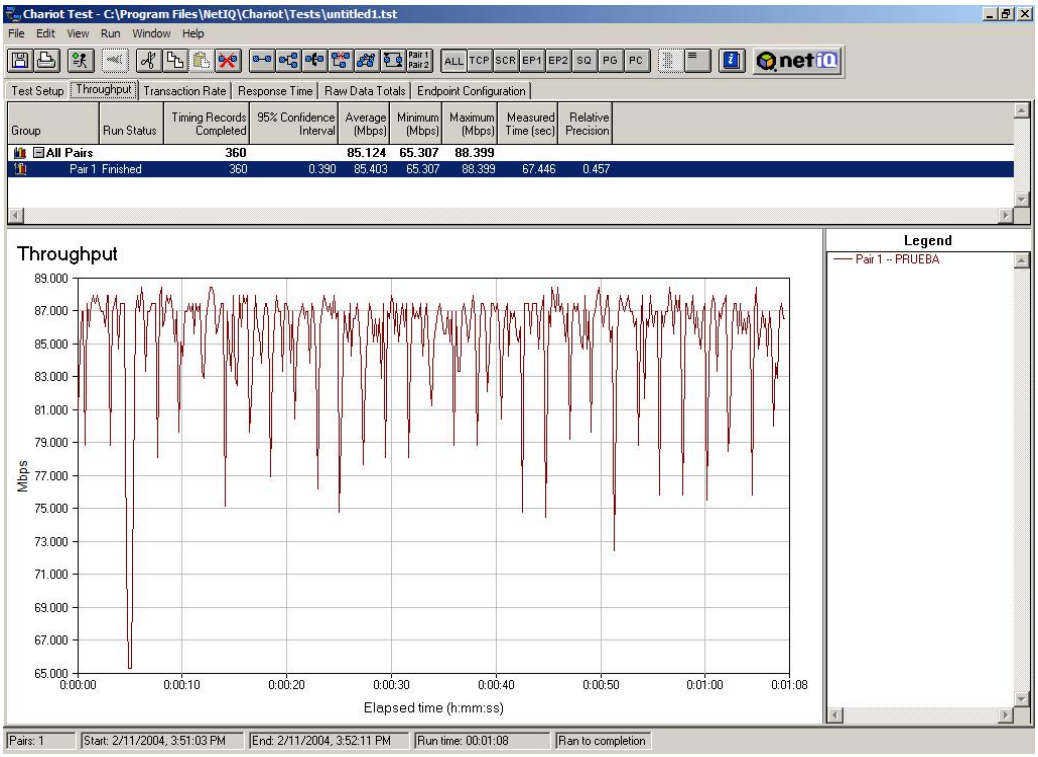

Figure 14 Capacidad del enlace FIE-GRU usando como *gateway* un AT-8724XL

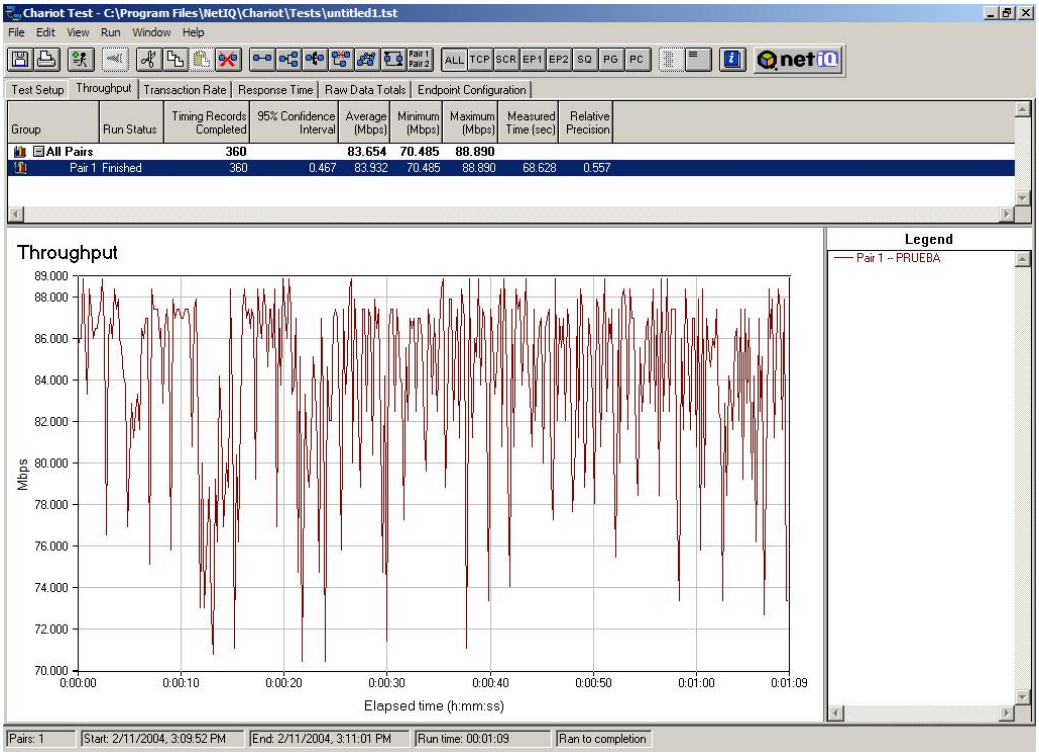

Figure 15 Capacidad del enlace FIE-SOCIALES usando como *gateway* una PC

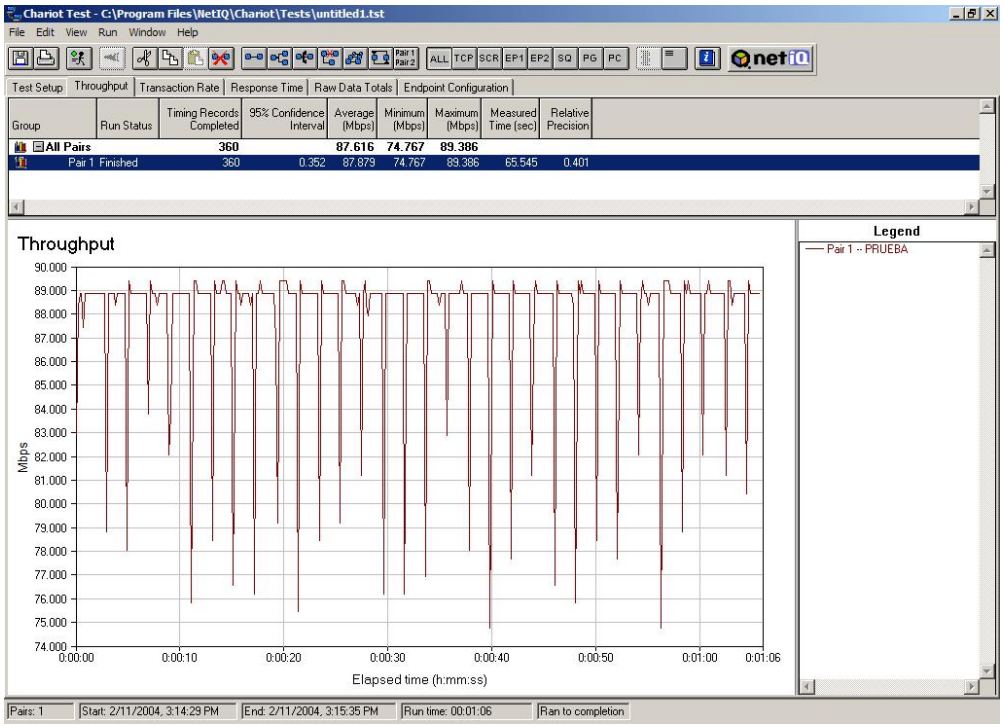

Figure 16 Capacidad del enlace FIE-GRU usando como *gateway* un AT-8724XL

II.6 Consideraciones finales

Este capítulo ha abordado la historia, la estructura y las principales etapas por las que ha transitado la Red UCLV. Se identificaron las principales debilidades del *backbone* de fibra óptica y se comentó sobre la necesidad de solucionar estos problemas.

La solución propuesta consta de dos partes: la ampliación de la Red UCLV creando nuevos enlaces sobre fibra óptica y la instalación de nuevos equipos de ruteo que cumplan con los requisitos identificados. Los *switches* del fabricante *Allied Telesyn* resultaron escogidos para realizar la segunda tarea.

Las Figuras 13, 14, 15 y 16 muestran que la capacidad de transmisión de los enlaces probados aumentó con el cambio de equipamiento, pero esto no es lo más importante: una nueva plataforma con capacidades de gestión fue creada y necesita ser configurada.

CAPITULO III: Gestión de red en el *backbone* de la UCLV

En el capítulo anterior se enfocó el problema de la mejoría de la Red UCLV solo desde el punto de vista de los cambios en equipos, en este capítulo se analizará la parte relacionada con el *software*.

Como se ilustró en la primera parte del capítulo I, el hecho de poder supervisar el comportamiento de los equipos que integran la red posibilita que se pueda controlar mejor su funcionamiento, como unidades aisladas, y el funcionamiento de la red como una sola entidad.

Una de las debilidades citadas en el epígrafe II.2 está relacionada con la escasez de una plataforma de gestión, esto es consecuencia directa de otra de las debilidades citadas: la existencia de muy pocos equipos gestionables. Con la compra e instalación de varios equipos con una gran gama de posibilidades en los puntos fundamentales de la red el panorama cambia radicalmente.

Corresponde crear un plan para paulatinamente y de forma muy bien organizada ir instalando un sistema que permita la supervisión y el control de (en una primera etapa) los recursos considerados críticos, y (posteriormente) de los que solo aporten información de estado.

La calidad del sistema final dependerá en gran media del nivel de organización con el que sea enfrentada esta tarea, el resultado puede ser un sistema de supervisión y control que permita a los administradores de redes “tener la red a sus pies” o “tener la red en el piso”.

III.1 Identificación de los elementos a monitorear y controlar

El primer paso en la instalación de una plataforma de gestión es la identificación de las variables que se desean monitorear. Este proceso esta sujeto a uno de los axiomas básicos de los sistemas

supervisorios: “no hay que sobre-controlar”. Aunque se disponga de los mejores equipos, del mejor software para la estación de gestión y de todo el tiempo de procesamiento disponible, el encuestar, analizar y almacenar variables que nunca serán usadas representa una pérdida de tiempo, recursos y una abundante carga de complejidad adicional.

La correcta definición de lo que se quiere monitorear y de lo que se desea controlar mantendrá a la NMS ocupada en los puntos que mantienen a la red trabajando y a los servicios funcionado de forma correcta y estable.

En el caso de la UCLV solo se monitoreaban dos equipos, el *router* Cisco 1005 que posibilita la conexión a Internet y el *switch* centro de la estrella en el *backbone*. Las variables encuestadas eran la cantidad de *bytes* de entrada y de salida por la interfaz serie de estos equipos. En términos de SNMP eso se traduce en los OIDs siguientes:

- *Router* Cisco 1005
  ip: 200.55.45.9
  comunidad: public0
  OID: IF-MIB::ifInOctets.1 (.1.3.6.1.2.1.2.2.1.10.1)
  IF-MIB::ifOutOctets.1 (.1.3.6.1.2.1.2.2.1.16.1)

- *Switch* Lan Optics
  ip: 172.20.1.62
  comunidad: public
  OID: IF-MIB::ifInOctets.x
  IF-MIB::ifOutOctects.x

Con la instalación de *switches* gestionables en todo el *backbone* de la UCLV la cantidad de variables a monitorear aumenta exponencialmente. Estas variables pueden ser clasificadas en dos grupos fundamentales: el primero orientado al conocimiento del estado de las conexiones más importantes y el segundo enfocado a la ocurrencia de alarmas o eventos de seguridad.

En la Tabla # 1 se relacionan por áreas las variables más importantes pertenecientes al primer grupo.

Tabla # 1 Variables a monitorear en el *backbone* UCLV.

GRU		
switch LanOptics	172.20.1.62	public0
	Módulo 1 Puerto 1	Enlace GRU-FIE
	Módulo 1 Puerto 2	Enlace GRU-FCE
	Módulo 1 Puerto 3	Enlace GRU-CEI
	Módulo 1 Puerto 4	Enlace GRU-CVEP
	Módulo 1 Puerto 5	Enlace GRU-FIM
	Módulo 1 Puerto 6	Enlace GRU-QF
	Módulo 1 Puerto 7	Enlace GRU-MFC
	Módulo 1 Puerto 8	Enlace GRU-IBIS*[3]
	Módulo 2 Puerto 1	Enlace GRU-SOCIALES
	Módulo 2 Puerto 2	Enlace GRU-CDICT
	Módulo 2 Puerto 3	Enlace GRU-RECTORADO-U4
	Módulo 2 Puerto 4	Enlace GRU-FC
	Módulo 2 Puerto 5	
	Módulo 2 Puerto 6	
	Módulo 2 Puerto 7	VLAN-1
	Módulo 2 Puerto 8	VLAN-2
	Módulo 3 Puerto 1	VLAN-3
	Módulo 3 Puerto 2	VLAN-4
	Módulo 3 Puerto 3	
	Módulo 3 Puerto 4	
	Módulo 3 Puerto 5	Enlace GRU-FCA
	Módulo 3 Puerto 6	Enlace GRU-FEU
	Módulo 3 Puerto 7	Enlace GRU-VLIR*
	Módulo 3 Puerto 8	Enlace GRU-EST.EXP*
switch Rapier 24i	172.20.1.240	public0
	Puerto 1 – VLAN-1	CISCO – 200.55.145.9
	Puerto 2 – VLAN-1	MAIL – 200.55.145.10
	Puerto 3 – VLAN-1	PROXY – 200.55.145.11
	Puerto 4 – VLAN-1	JABBER – 200.55.145.12
	Puerto 5 – VLAN-1	eMEETING – 200.55.145.13
	Puerto 9 – VLAN-2	MERCH – 172.20.1.5
	Puerto 10 – VLAN-2	MAIL-01 – 172.20.1.6
	Puerto 11 – VLAN-2	MAIL-02 – 172.20.1.7
	Puerto 12 – VLAN-3	DATABASE-01 – 172.20.1.8

[3] Los enlaces o servidores marcados con asterisco * no existen actualmente pero están planificados para los próximos meses.

	Puerto 13 – VLAN-3	MAIL-03 – 172.20.1.9*
	Puerto 14 – VLAN-3	MAXWELL – 172.20.1.53
	Puerto 17 – VLAN-4	MAIL – 172.20.1.33
	Puerto 18 – VLAN-4	PROXY – 172.20.1.34
	Puerto 19 – VLAN-4	eMEETING – 172.20.1.31*
	Puerto 20 – VLAN-4	JABBER – 172.20.1.32
FIE		
switch AT-8724XL	172.20.1.210	Public0
	Puerto 1	Enlace FIE-GRU
	Puerto 2	Enlace FIE-CVEP*
	Puerto 3	Enlace FIE-GPS*
	Puerto 4	Enlace FIE-CEETI
	Puerto 5	VOLT
	Puerto 6	NEUMANN
	Puerto 7	GAUSS
FCE		
switch AT-8724XL	172.20.1.211	Public0
	Puerto 1	Enlace FCE-GRU
	Puerto 2	FRAVIA
	Puerto 3	IRC
	Puerto 4	CAPITAL
CEI		
switch AT-8024GB	172.20.1.212	Public0
	Puerto 1	Enlace CEI-GRU
	Puerto 2	PHP
CVEP		
switch AT-8724XL	172.20.1.213	public0
	Puerto 1	Enlace CVEP-GRU
	Puerto 2	SEPAD
FIM		
switch AT-8724XL	172.20.1.214	public0
	Puerto 1	Enlace FIM-GRU
	Puerto 2	Enlace FIM-SOLDADURA
	Puerto 3	ARQUIMIDES
	Puerto 4	ZSEVER
QF		
switch AT-8724XL	172.20.1.215	public0
	Puerto 1	Enlace QF-GRU
	Puerto 2	Enlace QF-CBQ

	Puerto 3	QF-MX
	Puerto 4	SION
MFC		
switch AT-8724XL	172.20.1.216	Public0
	Puerto 1	Enlace MFC-GRU
	Puerto 2	MFCSERVER
	Puerto 3	SUS-MFC
SOCIALES		
switch AT-8724XL	172.20.1.217	public0
	Puerto 1	Enlace SOCIALES-GRU
	Puerto 2	Banda Humanidades
	Puerto 3	CERVANTES
	Puerto 4	DANTES
	Puerto 5	ATENEA
CDICT		
switch AT-8724XL	172.20.1.218	public0
	Puerto 1	Enlace CDICT-GRU
	Puerto 2	Enlace CDICT-DRI
	Puerto 3	SERVER CDICT
RECTORADO		
switch AT-8724XL	172.20.1.219	public0
	Puerto 1	Enlace RECTORADO-GRU
	Puerto 2	Enlace RECTORADO-U4
	Puerto 3	CASTOR
U4		
switch AT-8024GB	172.20.1.220	public0
	Puerto 1	Enlace U4-RECTORADO
FC		
switch AT-8724XL	172.20.1.221	public0
	Puerto 1	Enlace FC-GRU
	Puerto 2	Enlace FC-SEDER
	Puerto 3	Enlace FC-P.CBQ
	Puerto 4	FC-MAIL
	Puerto 5	AFRODITA
FCA		
switch AT-8724XL	172.20.1.222	public0
	Puerto 1	Enlace FCA-GRU
	Puerto 2	Enlace FCA-IBP

	Puerto 3	SABIO
	Puerto 4	SERWIN

La lista aunque parece grande no lo es pues no están incluidos aún la mayoría de los *switches* o los *hubs* que se conectan a los nodos en las facultades, que es en realidad donde están conectados la mayoría de los usuarios importantes.

El segundo grupo de variables está relacionado con la ocurrencia de eventos que pueden afectar el correcto funcionamiento de la red. Por ejemplo el incremento de paquetes con errores, un ataque de paquetes TCP-SYN o demasiados intentos fallidos de autentificación pueden ser una señal de que algo malo está por ocurrir, esta situación podría afectar la estabilidad de la red si no se toman las medidas adecuadas a tiempo. En el caso de los datos relacionados con el desempeño de una interfaz es muy fácil encuestar al agente desde una NMS, pero cuando se habla de la ocurrencia de un evento que tiene carácter aleatorio la mejor vía es que el agente avise a la NMS a través de un *trap* de SNMP.

Con el fin de no repetir la tabla anterior solo se indicarán los OIDs relacionados con el funcionamiento de las interfaces que se van a supervisar. Estos están en la rama: *iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry***.#**

IF-MIB::ifAdminStatus	1.3.6.1.2.1.2.2.1.7
IF-MIB::ifOperStatus	1.3.6.1.2.1.2.2.1.7
IF-MIB::ifInDiscards	1.3.6.1.2.1.2.2.1.13
IF-MIB::ifInErrors	1.3.6.1.2.1.2.2.1.14
IF-MIB::ifInUnknownProtos	1.3.6.1.2.1.2.2.1.15
IF-MIB::ifOutDiscards	1.3.6.1.2.1.2.2.1.19
IF-MIB::ifOutErrors	1.3.6.1.2.1.2.2.1.20

Por otra parte los eventos que se van a monitorear en todos los *switches* instalados aparecen en la Tabla # 2.

Tabla # 2 Eventos a monitorear por interfaces.

AUTHENTICATE_TRAP	Cada vez que se falla o se logra entrar a los *switches* para configurarlos.
DOSFLOOD	Un ataque de denegación de servicio donde el atacante envía continuamente trafico no deseado.
FRAGMENT	Ocurre cuando son enviados fragmentos muy grandes de paquetes TCP o cuando estos no pueden ser reensamblados.
HOSTSCAN	Orientado principalmente a descubrir estaciones en una Intranet.
IPSPOOF	Cuando se usan paquetes donde la IP origen fue alterada.
LAND	Ataque de denegación de servicio donde el paquete enviado lleva la misma dirección IP en el origen que en el destino.
PINGOFDEATH	Ataque donde se envían paquetes ICMP con tamaño invalido.
PORTSCAN	Orientado principalmente a descubrir servicios en una estación.
SMTPRELAY	Cuando un mensaje enviado por SMTP no tiene ni como remitente ni como destinatario un usuario local.
SMURF	Un paquete de ICMP *echo request* enviado a una dirección de *broadcast*.
SMURFAMP	Ocurre cuando una estación hace un *broadcast* de un paquete TCP SYN al puerto 25.
SYNATTACK	Se envían muchos paquetes SYN que nunca son usados.
TCPTINY	Cuando son enviados paquetes muy pequeños tipo TCP.
UDPATTACK	Envío de paquetes UDP para detectar posibles servicios en estaciones remotas.

III.2 Propuesta de una estructura para lograr una “red más inteligente”

Luego de seleccionar todos los aspectos que se desean monitorear en la Red UCLV corresponde la instalación de la estación de gestión. Teniendo en cuenta las arquitecturas vistas en I.5 y las ventajas de

una implementación distribuida se propone la instalación de una MNS en el local del GRU y de otra en la dirección de informatización donde radicaran los servidores de aplicaciones del la UCLV[4].

Como software para la estación de gestión se tienen dos propuestas que lejos de excluirse se complementan excelentemente: el *nagios* y el SNMPc.

Estos programas fueron brevemente explicados en el capítulo I, y aquí se citarán los elementos fundamentales de su funcionamiento dentro de la estructura de gestión de la Red UCLV.

III.2.1 Supervisor *Nagios*

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 cheque los servicios especificados y que avise en caso de que algo no este bien.

El proceso que monitorea 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. El estado actual y pasado puede ser encuestado a través de cualquier navegador de WEB.

La Figura 17 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. Los ficheros de configuración del *nagios* se relacionan en la Tabla # 3.

[4] Este segundo local aun se encuentra en fase constructiva por lo que la instalación y configuración de la NMS que radicara allí esta pendiente.

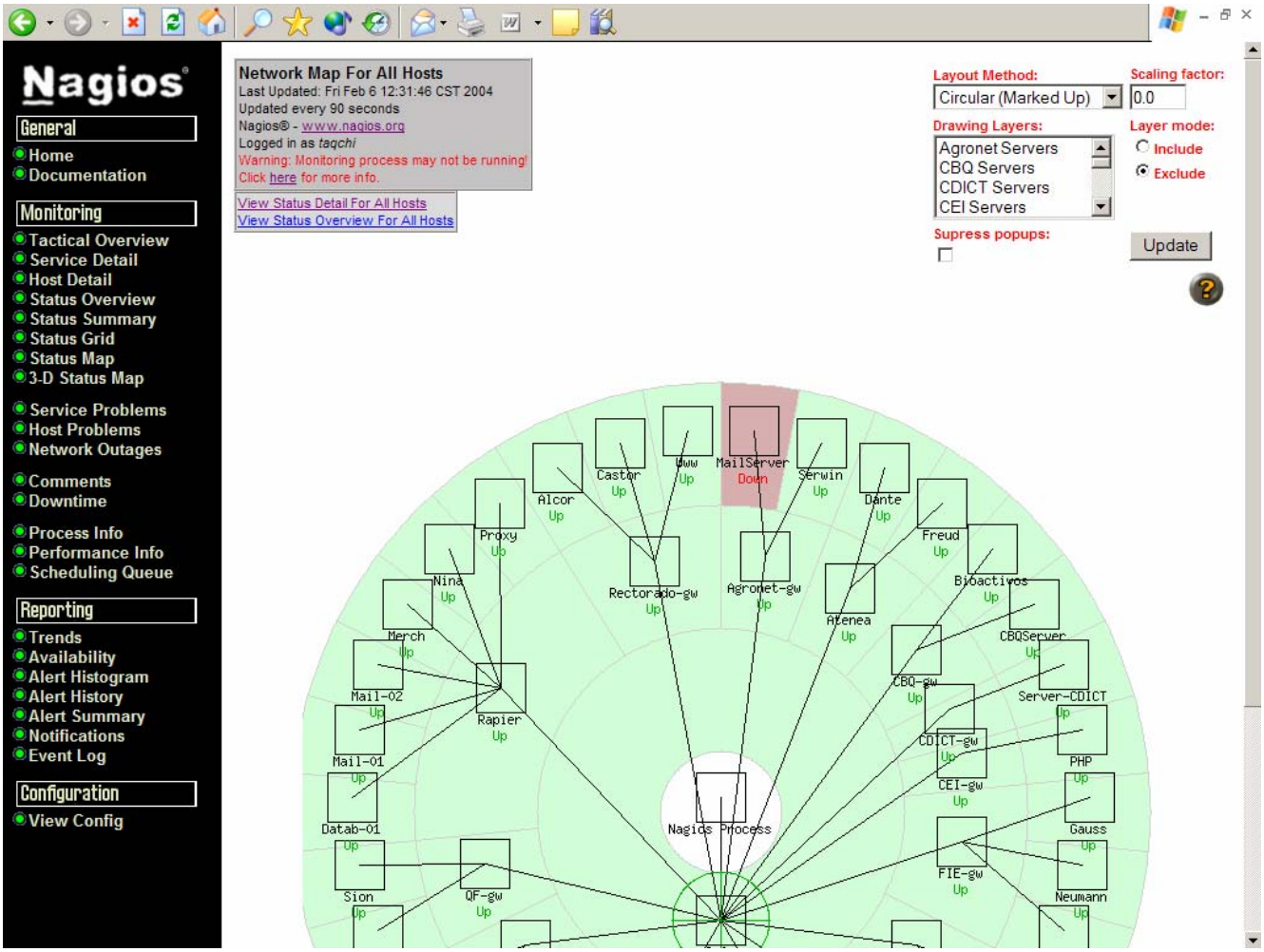

Figura 17 Mapa de estado del Nagios

Tabla # 3 Ficheros de configuración del *nagios*

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]

Para lograr una mejor visualización de los ficheros tratados se muestra un pequeño ejemplo de los más importantes. Una versión completa de estos ficheros se encuentra en el CD que acompaña este trabajo.

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 en 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.2.2 Programa SNMPc

El programa SNMPc de la empresa *CastleRock* dispone de la estructura de un NMS clásico. Cuenta con servicios como el graficado de la red, escaneo de estaciones basado en un rango de direcciones IP y el descubrimiento de agentes de SNMP.[SNMPC]

Su principal ventaja es una interfaz gráfica que permite ver y modificar la red que se está gestionando y las propiedades de los equipos. Los objetos que se muestran en estas pantallas se agrupan en subredes compartiendo propiedades que son comunes para todos los miembros de una red. La Figuras 18 y 19 muestran las estaciones que se encuentran en el *backbone* de la Red UCLV vistas a través del SNMPc.

Al contrario de *nagios,* el SNMPc no es una versión libre, se debe pagar por su uso, y esta es la principal desventaja de este *software*, pero mientras *nagios* no sea capaz de implementar todas las facilidades del SNMPc deberá continuar siendo usado.

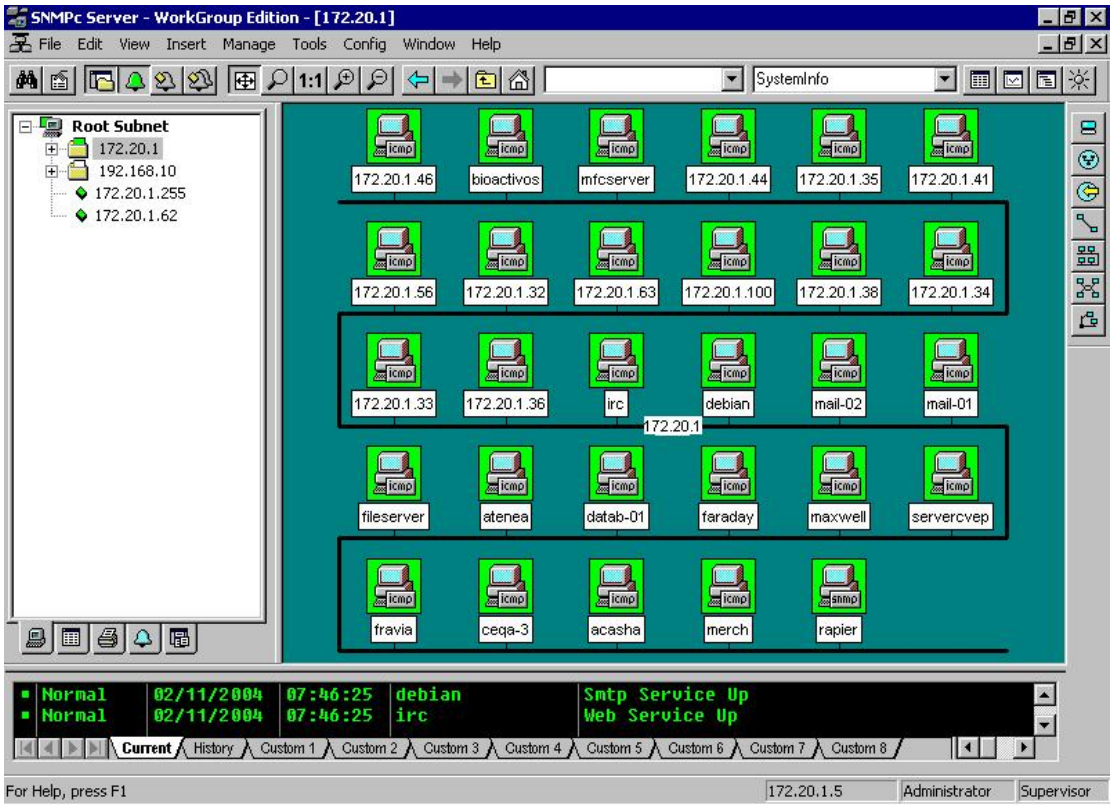

Figure 18 Estaciones pertenecientes al *backbone* de la UCLV

III.3 Desempeño de una "red inteligente"

El desempeño de una red es algo difícil de medir, cuando se busca bibliografía al respecto se encuentran respuestas orientadas principalmente al desempeño físico. Se cita al tiempo promedio de atraso desde que un paquete está listo para ser transmitido y el momento en que se transmite exitosamente, el flujo máximo soportado y el porcentaje de utilización del canal como los principales parámetros que definen el desempeño de la red. A estos parámetros se le pudieran agregar otros que describan mejor lo que es más usado de una red de computadoras: sus servicios.[Black, 1993]

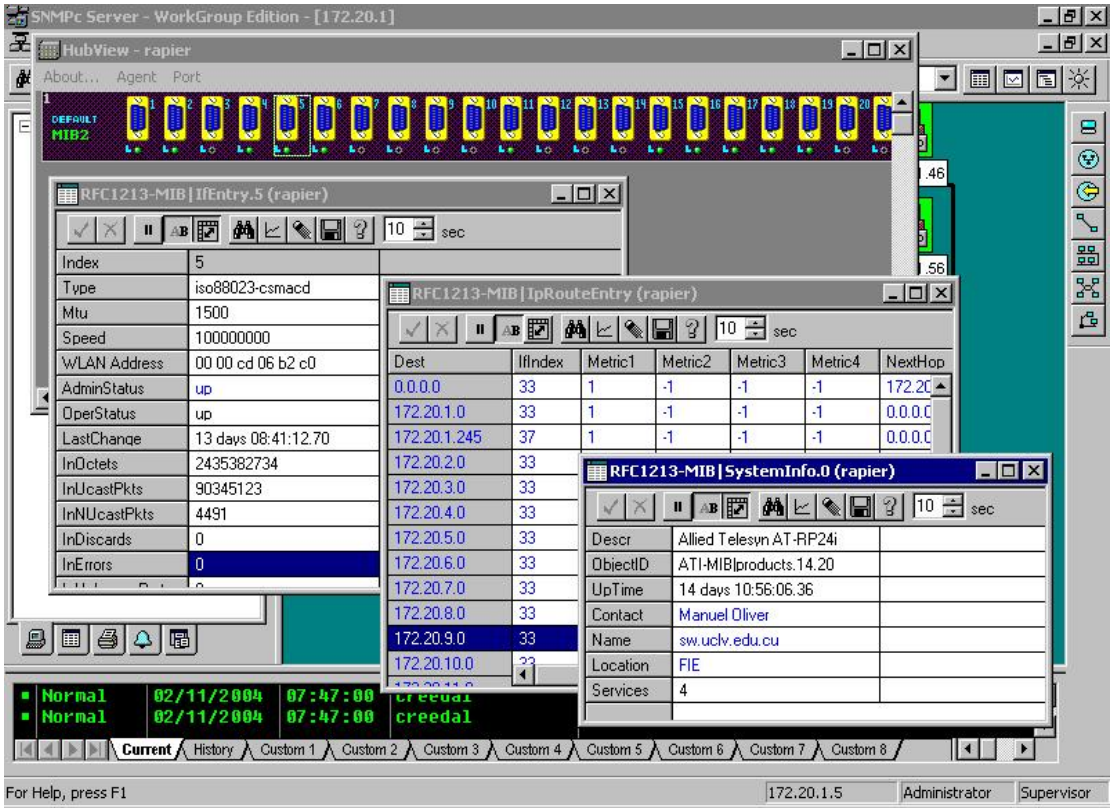

Figure 19 Propiedades del Rapier 24i que se encuentra en el GRU mostradas por el SNMPc

Como se expresó en el capítulo I, las redes valen por sus servicios, si estos fallan o trabajan intermitentes existirán más problemas que si la red sencillamente estuviera completamente fuera de servicio. Por esta razón deben medirse las cantidades de interrupciones de los servicios más importantes, el tiempo que demoran en recuperarse y calcular la frecuencia con que ocurren estos fallos. La idea es por supuesto minimizar la cantidad de ocurrencias de estos casos negativos pero es conveniente recordar que todo servidor necesita mantenimiento y que toda aplicación necesita ser reiniciada cada cierto tiempo.

El *nagios* puede ser usado para medir los niveles de disponibilidad de un servicio o de una estación siempre y cuando sea de los que el monitorea. Una imagen del reporte que brindado se muestra en la Figura 20.

Existen otros métodos menos cuantitativos que pueden ayudar a medir el desempeño de una red. La aplicación de encuestas que soliciten información a los usuarios es un ejemplo de ello. Casi todas las

empresas en el mundo se preocupan por las opiniones de sus usuarios, principalmente gigantes como Microsoft, Yahoo y Google. Ellos usan generalmente una página Web y es el usuario el que decide participar o no.

Service State Breakdowns:

State	Type / Reason	Time	% Total Time	% Known Time
OK	Unscheduled	6d 23h 59m 51s	99.999%	100.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	**6d 23h 59m 51s**	**99.999%**	**100.000%**
WARNING	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	**0d 0h 0m 0s**	**0.000%**	**0.000%**
UNKNOWN	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	**0d 0h 0m 0s**	**0.000%**	**0.000%**
CRITICAL	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	**0d 0h 0m 0s**	**0.000%**	**0.000%**
Undetermined	Nagios Not Running	0d 0h 0m 9s	0.001%	
	Insufficient Data	0d 0h 0m 0s	0.000%	
	Total	0d 0h 0m 9s	0.001%	
All	Total	7d 0h 0m 0s	100.000%	100.000%

Figura 20 Disponibilidad de un servicio monitoreado por el *Nagios*

III.4 Respuesta a interrupciones

Las interrupciones son algo inherente a todas las redes de computadoras. Las interrupciones pueden ser programadas, o forzadas. Las programadas como su nombre lo indica están planificadas y se efectúan principalmente para cumplir con los ciclos de mantenimiento de los equipos o de los sistemas. Las forzadas ocurren siempre por anormalidades o alteraciones en el ciclo de trabajo de la red.

Las interrupciones planificadas deben ser avisadas con tiempo suficiente para que los usuarios las conozcan y no se cree un estado de opinión negativo sobre el trabajo de la Red o de sus administradores. Deberán efectuarse dentro de lo posible en horarios de poca demanda del servicio que se afectará y se debe minimizar el tiempo de duración.

Las interrupciones forzadas son las más problemáticas, pues no son esperadas y en su solución entra a jugar un rol determinante el nivel de conocimientos y cohesión del grupo de administradores.

Como es de esperar el nivel de complejidad de las interrupciones forzadas no es siempre el mismo, en algunos casos la forma de recuperarse es trivial y compuesta por órdenes secuenciales que nunca cambian de orden. En esos escenarios es donde el *nagios* y el SNMPc entran a jugar su papel. La posibilidad de ejecutar ficheros con comandos y órdenes como respuesta a un evento hacen de estos programas algo muy útil, principalmente para los “horarios de descanso” y lo “fines de semana”.

A modo de ejemplo de estas respuestas automatizadas se tiene la activación de un segundo servidor de correo, o de un *Proxy Server* en caso de fallo de los principales. La activación de un puerto con un enlace de respaldo es otra forma de respuesta.

III.5 Consideraciones Finales

En este capítulo se ha tratado sobre la estructura de un sistema de gestión de redes para la Red UCLV. En este se identifican las variables más importantes para el trabajo de la red, estas están orientadas principalmente a mantener la conectividad entre las diferentes áreas y los servidores que se encuentran en cada una de ellas. También se definen los eventos que se van a monitorear en los equipos seleccionados en el capítulo anterior.

La selección de los programas que servirán en la NMS es otro aspecto analizado en este último capítulo. El *nagios* y el SNMPc fueron los elegido para realizar esta labor. El primero se destaca por su flexibilidad y su carácter de *software* libre y el segundo por su facilidad de uso y su integración con dispositivos SNMP.

Conclusiones

Como resultado del trabajo realizado y argumentado por este proyecto de tesis se ha llegado a las conclusiones siguientes:

- El análisis de la estructura del *backbone* de la Red UCLV permitió la detección de un conjunto de deficiencias que atentaban contra un óptimo aprovechamiento de las capacidades instaladas, entre estas se encontraban la escasez de equipos gestionables y el uso de *gateways* no especializados.

- La implementación de este proyecto de tesis posibilitó actualizados y en algunos casos la elaboración de esquemas correspondientes a la distribución del cableado de la casi totalidad de los nodos de la Red UCLV, además se estandarizó la norma de conexión usada en los gabinetes de los diferentes nodos. Todo esto contribuye a facilitar cualquier modificación o ampliación futura.

- Las deficiencias detectadas y las necesidades prospectivas de la Red UCLV posibilitaron el esclarecimiento de las características técnicas de los equipos a incorporar en el backbone UCLV. Aunque la selección de los dispositivos que se ajustasen a las características elegidas estuvo condicionada a la disponibilidad de financiamiento, los equipos adquiridos han tenido un desempeño satisfactorio.

- La selección del los programas encargados de la gestión y de la supervisión de los equipos instalados contribuye a un mayor aprovechamiento de estos. En la Red UCLV se seleccionaron *nagios* y SNMPc como los *softwares* para ejecutarse en las NMS. Para la correcta configuración de estos programas se identificaron las variables más importantes relacionadas con la conectividad y la disponibilidad de los servidores que están ubicados en la Intranet de la UCLV como son los enlaces entre los nodos que forman la red. Gracias a estos programas los servicios de la Red UCLV se han comportado de forma más estable y robusta.

Recomendaciones

Como recomendaciones propósito de garantizar el perfeccionamiento continuo de la Red UCLV se proponen las recomendaciones siguientes:

- Orientar el estudio del protocolo SNMP dentro del grupo de administradores de la UCLV, con el fin de lograr que una mejor comprensión de las posibilidades que se han creado con la instalación de los nuevos *switches*.
- Trabajar en la creación de módulos que permitan una mejor integración de *nagios* con redes compuestas por dispositivos SNMP.
- Crear un sitio Web que posibilite el conocimiento por parte de los usuarios de la Red UCLV del estado de los servicios y de los enlaces más importantes.
- Continuar expandiendo el backbone de la Red UCLV para lograr conectar las áreas de la UCLV que aún no disponen de una conexión permanente.

Referencias Bibliográficas

AD – Active Directory (2001) [En línea] Accesible en http://www.microsoft.com/windows/technologies/directory/ad/default.asp (Consultado 2004)

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.

Black, Uyless D. (1995). *TCP/IP and Related Protocols*. 2da Edición, 372 páginas. McGraw-Hill Osborne Media, EUA.

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

Held, Gilbert. (1996). *LAN Management with SNMP and RMON*. 371 páginas. John Wiley & Sons, 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)

NAGIOS (2003) [En línea] Accesible en http://www.nagios.org (Consultado 2004)

Mauro, Douglas. (1993). *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.

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.

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

Twonsend, Robert L. (1995). *SNMP Applications Developer's Guide*. 256 páginas. John Wiley & Sons, EUA.

ANEXOS