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

Herramientas para la Gestión de Equipos de la Red de Transmisión de Datos de ETECSA

Tesis presentada en opción al Título Académico de
Máster en Telemática

Maestría de Telemática

Autor: **Ing. Nora Vivian Torres Leonard**

Tutores: **Dr. Félix Álvarez Paliza**
MSc. Vitalio Alfonso Reguera

2004

Agradecimientos

A mi mamá, que se quedaba con el pecho oprimido cada tercer domingo del mes.

A mi esposo, por su ayuda incondicional, su apoyo y su comprensión, sin él me hubiera sido imposible llegar a la meta.

A Julio y Raulito, mi amigos, por tanta paciencia y por compartir conmigo sus conocimientos.

A todos los profesores de la Maestría en Telemática de la UCLV por su magnífica actuación, en especial a Vitalio, mi tutor, quien soportó mis desesperos y apuros, GRACIAS

A todos mis colegas de la Maestría, porque de cada uno aprendí algo diferente y sobre todo algo nuevo, por la ayuda profesional que recibí de muchos y por los gratos momentos que pasamos juntos, riendo, nerviosos o indignados por una decisión no aceptada por el grupo.

Agradecimientos muy especiales para mis AMIGAS Odalys, Mayra y Ana por servirme de apoyo, de consejeras, de calmantes cuando estaba alterada y por ¡ayudarme a conseguir el teléfono!

A Consuelo y al Pollo, a Cuca mi vecina.

Dedicatoria

A MI NENÉ…

RESUMEN

La Empresa de Telecomunicaciones de Cuba, ETECSA, creada en 1994, ha dado pasos agigantados desde el punto de vista tecnológico y social. Desde sus inicios la tendencia ha sido renovar el equipamiento existente, con el objetivo de ofertar mayor calidad en los servicios. La Red de Transmisión de Datos no queda exenta de este desarrollo y el avance alcanzado desde 1996, cuando se instaló la primera red de ETECSA, la X.25/FR Alcatel, es sustancial y palpable.

Todo el equipamiento no se encuentra administrado y es objetivo fundamental en este trabajo, hacer una valoración de la gestión de las redes de ETECSA y proponer la implementación de un sistema que se encargue de gestionar los modems Telindus, ya que existe un gran número de equipos de este fabricante en las Redes de ETECSA. Actualmente, al no estar centralizada esta gestión, las fallas se detectan cuando el cliente las reporta, lo cual aumenta los tiempos fuera de servicio y contribuye negativamente en la reputación de la empresa. Estos equipos de Telindus ofrecen la posibilidad de ser gestionados y la implementación de este sistema ahorrará a la Empresa muchos gastos por concepto de salarios, hospedaje y combustible, además de que la inversión hecha en el mismo se recuperará en breve tiempo.

Se usará el “software” propietario de Telindus TMA, el cual se montará sobre la plataforma HP Openview, cuya integración ofrece un resultado muy bueno para la gestión de redes, además de brindar la posibilidad de integrar en el futuro la gestión de otros equipos que no se gestionan actualmente y otros que si lo están, pero sobre otras plataformas, cuestión que también se trata en este trabajo.

Además, se realizó un estudio de los diferentes sistemas y plataformas de gestión existentes, para lo que se efectuó una profunda investigación bibliográfica, ofreciendo variantes para lograr a la larga una gestión centralizada, considerando al HP Openview, nuestra mejor propuesta.

El ahorro, la disminución de tiempos fuera de servicio y sobre todo la elevación de la calidad en los servicios de ETECSA, son logros a obtener con la implementación de este trabajo.

TABLA DE CONTENIDO

INTRODUCCIÓN 1
CAPITULO 1: ESTADO DEL ARTE DE LA GESTIÓN DE REDES 6
1. INTRODUCCIÓN 6
2. DESARROLLO 8
2.1 PRIMEROS TRABAJOS PARA LA GESTIÓN DISTRIBUIDA DE REDES 8
2.2 TECNOLOGÍAS ACTUALES. 9
2.3 SISTEMAS DE GESTIÓN BASADOS EN POLÍTICAS. 9
2.4 SISTEMAS DE GESTIÓN DISTRIBUIDOS (DISTRIBUTED OBJECT COMPUTING) 11
2.5 GESTIÓN BASADA EN WEB 13
2.5.1 PROPUESTAS DE ARQUITECTURAS DE GESTIÓN BASADA EN WEB 14
2.6 GESTIÓN DE RED BASADA EN JAVA 15
2.7 MOVILIDAD DEL CÓDIGO PARA GESTIÓN DE REDES. 16
2.8 AGENTES INTELIGENTES. 18
2.9 REDES ACTIVAS 21
2.10 TEORÍA ECONÓMICA 23
2.11 PLATAFORMAS DE GESTIÓN DE REDES 23
2.11.1 SNMPC, DE CASTLE ROCK COMPUTING. 25
2.11.2 3COM TRANSCEND ENTERPRISE MANAGER DE 3COM. 27
2.11.3 WHATSUP GOLD, DE IPSWITCH. 29
2.11.4 CISCOWORK FOR WINDOWS 33
2.11.5 OPENVIEW WORKGROUP NODE MANAGER DE HP 35
3. CONCLUSIONES 36
CAPITULO 2: ESTADO ACTUAL DE LA GESTIÓN DE REDES DE TRANSMISIÓN DE DATOS DE ETECSA. 38
1. INTRODUCCIÓN 38
2. DESARROLLO 38
2.1 ARQUITECTURA DE REDES 38
2.1.1 RED DE CONMUTACIÓN DE PAQUETES X.25/FR 38
2.1.2 RED “BACKBONE” ATM/FR 39

2.1.3 INFOCOM 41
2.1.3.1 NAP 42
2.1.4 REDES DE TERCEROS 42
2.2 REDES DE GESTIÓN 42
2.2.1 GESTIÓN DE RED X.25/FR 42
2.2.2 GESTIÓN DE RED “BACKBONE” ATM/FR 48
2.2.2.1 GESTIÓN DE FALLAS 49
2.2.2.2 GESTIÓN DE CONFIGURACIÓN 50
2.2.2.2.1 CONFIGURACIÓN IP 51
2.2.2.2.2 CONFIGURACIÓN DSL 51
2.2.2.2.3 CONFIGURACIÓN ATM 51
2.2.2.3 GESTIÓN DE TRÁFICO 51
2.2.2.4 GESTIÓN DE DESEMPEÑO Y CONTABILIDAD 52
2.2.2.5 GESTIÓN DE SEGURIDAD 53
2.2.2.6 GESTIÓN DE SERVICIO 54
2.2.2.7 GESTIÓN DE NODO 54
2.2.2.8 GESTIÓN DE RED 54
2.2.2.8.1 ENLACES Y CAMINOS CPSS 57
2.2..2.8.2 PROTOCOLO DE GESTIÓN DE RED SIMPLE (SNMP) 58
2.2.2.8.3 INTERFACES OSS 58
2.2.3 GESTION DEL NAP 60
2.2.4 RED DE INFOCOM 61
2.2.5 REDES DE TERCEROS 61
3. CONCLUSIONES 61
CAPITULO 3: PROPUESTA DE SISTEMA DE GESTION PARA REDES DE TRANSMISIÓN DE DATOS DE ETECSA. 63
1. INTRODUCCIÓN 63
2. DESARROLLO 64
2.1MODEMS TELINDUS 64
2.1.1 MODEM BANDA BASE HDSL. 65
2.1.2 MODEM HS. 65
2.1.3 MODEMS SDSL 66

2.2 HERRAMIENTAS NECESARIAS PARA LA GESTIÓN DE EQUIPOS TELINDUS 67
2.2.1 PRODUCTOS DE TELINDUS....67
2.2.1.1 TMA....67
2.2.1.2 TMA CLI....68
2.2.1.3 TMA FOR HP OPENVIEW....69
2.2.1.3.1 FUNCIONES DE ADMINISTRACIÓN....70
2.2.1.3.2 FUNCIONALIDAD DEL HP OPENVIEW®....70
2.2.1.3.2.1 TIEMPO REAL DE VISUALIZACIÓN DE STATUS DE RED....70
2.2.1.3.2.2 SEGURIDAD DE ACCESO....71
2.2.1.3.2.2.1 SEGURIDAD DEL ADMINISTRADOR DE ALARMAS....71
2.2.1.3.2.3 ADMINISTRACIÓN DISTRIBUIDA....72
2.2.1.3.2.4 FUNCIONALIDAD PARA TMA FOR HP OPENVIEW®....72
2.2.1.3.2.5 INSTALACIÓN DE TMA FOR HP OPENVIEW....74
2.2.1.3.2.6 INTERCONEXIÓN CON OTROS EQUIPOS....75
2.2.1.3.2.7 DIRECCIONAMIENTO EN TMA FOR HP OPENVIEW....77
2.2.3 ORCHID 1003 LAN....77
2.2.3.1 MODO DE DIRECIONAMIENTO....80
2.2.3.2 ENCAPSULAMIENTO DE PROTOCOLOS....82
2.2.3.2.1 ENCAPSULAMIENTO MAC....82
2.2.3.2.2 ENCAPSULAMIENTO FRAME RELAY Y X.25....82
2.2.3.2.3 ENCAPSULAMIENTO PPP....83
2.2.3.2.4 TOPOLOGIAS MIXTAS....84
2.2.4 ESPECIFICIDADES DEL SISTEMA DE GESTIÓN PARA MODEMS TELINDUS EN REDES DE TRANSMISIÓN DE DATOS DE ETECSA. 84
3. CONCLUSIONES....86
CONCLUSIONES Y RECOMENDACIONES....87
REFERENCIAS BIBLIOGRAFICAS....89
GLOSARIO DE TERMINOS....94
ANEXOS....99

INTRODUCCIÓN

Uno de los procesos de negocio más característicos de una compañía operadora de Telecomunicaciones es la gestión de las redes y de los servicios que opera. Generalmente, por razones técnicas, económicas y estratégicas, las redes que soportan los servicios son heterogéneas en los elementos que las constituyen, pero el servicio es único y la percepción del cliente no debe depender ni de espacios geográficos ni de condicionantes tecnológicos.

Por ello, una operadora de Telecomunicaciones necesita soluciones de gestión que sean independientes de los elementos de las redes. Estas soluciones también deben ser suficientemente flexibles para poder adaptarse a los procesos de reingeniería, tan necesarios en el sector de servicios, un sector en constante lucha competitiva.

Pero el proveedor de sistemas de gestión debe ofrecer, además, otra característica esencial: rapidez en el desarrollo de los sistemas y en su operatividad. Si es cierto que el tiempo de desarrollo de un servicio es esencial para su éxito en el mercado, no lo es menos que no habrá servicio a los clientes si no va acompañado de un sistema de gestión que agilice su provisión, supervisión, operación y mantenimiento.

La proliferación de redes de datos a lo largo de la década de los 90, tanto LANs como WANs, y el interfuncionamiento entre ellas hace que los aspectos relativos a su control y gestión cada vez sean más tenidos en cuenta, convirtiéndose en algo a lo que todos los responsables de redes han de prestar una gran atención.

Dado que la tendencia natural de una red cualquiera es a crecer, conforme se añaden nuevas aplicaciones y más y más usuarios hacen uso de la misma, los sistemas de gestión empleados han de ser lo suficientemente flexibles para poder soportar los nuevos elementos que se van añadiendo, sin necesidad de realizar cambios drásticos en la red.

Este punto, el de gestión de red, es uno de los más controvertidos en Teleinformática, ya que prácticamente, no existe una solución única, aceptada por todos y que sea fácilmente implantable. Las soluciones existentes suelen ser propietarias -Netview de IBM, OpenView de HP, etc.- lo que hace que en una red compleja, formada por equipos multifabricante, no exista un único sistema capaz de realizar la gestión completa de la misma, necesitándose varias plataformas, lo que dificulta y complica enormemente la labor del gestor de red.

En nuestro país existen diferentes sistemas de gestión de equipos. En el caso específico de la Transmisión de Datos existe la gestión de los conmutadores de la Red CUBADATA, conformada por equipos X.25/FR y ATM/FR y la gestión de los equipos del NAP (Centro de Conmutación de ISPs), cuya gestión se encuentra en fase de instalación.

Las dos tecnologías que conforman la Red CUBADATA, o sea, la X.25/FR y la ATM/FR tienen sistemas de gestión de redes independientes.

Quedan sin gestionar los conmutadores, en su mayoría Cisco, de la red INFOCOM y los modems Telindus que se usan en nuestras redes.

La complejidad de la red de ETECSA, dada por su gran extensión y diversidad tecnológica, hace difícil la integración de la gestión, aunque la capacidad de plataformas como HP Openview, de integrar la gestión de múltiples equipos en un mismo sistema ayuda a reducir la complejidad del mismo y hace más fácil su manejo.

Detallar en una propuesta para la integración de la gestión de toda la red con un adecuado nivel de profundidad, es una tarea bastante compleja y extensa que escapa de los marcos de este trabajo. En tal sentido la gestión de los Modems Telindus se presenta como un paso hacia la integración de la gestión en una plataforma común, en este caso la HP Openview.

Los equipos de acceso de Telindus son lo más difundidos en nuestras redes y la inexistencia de un sistema centralizado de gestión y supervisión de estos equipos en las Redes de Datos con las que contamos actualmente, implica la no atención a tiempo de fallas y cambios en las configuraciones y por tanto el deterioro del servicio de la empresa ETECSA. Debido a esto nos dedicaremos en este trabajo, a realizar un bosquejo de la gestión implementada en las redes actuales de ETECSA y a proponer la implementación futura de un sistema de gestión que supere las deficiencias existentes y eleve la efectividad de nuestra empresa, utilizando plataformas de gestión universales que permitan la integración a otros sistemas.

Para alcanzar este objetivo tenemos algunos objetivos específicos como son:

- Analizar el sistema de gestión centralizada
- Caracterizar el estado de sistemas de gestión de Transmisión de Datos en Cuba

- Estudiar la aplicación de "Softwares" para implementar un sistema de gestión de modems Telindus, que sirva para en la medida de las posibilidades, ir integrando redes que así lo permitan.

- Proponer un sistema de gestión centralizada para emplear en ETECSA, en base al equipamiento de los modems Telindus.

Las tareas a realizar en este trabajo son:

- Análisis exploratorio de la bibliografía y búsqueda de información automatizada.

- Elaboración de un diagnóstico para conocer la situación del sistema.

- Caracterización de la gestión actual con la que cuentan las redes de Datos de ETECSA.

- Dando un primer paso hacia la integración, hacer la selección del "Software" adecuado para la gestión específica de estos equipos.

- Propuesta de configuración de un servidor con el sistema Operativo Windows 2000 e instalación de los softwares HP Open View y TMA for HP Open View.

- Propuesta de aplicación de los "Softwares" seleccionados.

- Elaboración del documento de Tesis donde se recogen todos los datos y las propuestas hechas para la implementación del sistema.

Con el trabajo pretendemos dar a conocer:

¿Qué características tiene el sistema centralizado?

¿Cómo implementar un sistema centralizado de gestión y supervisión?

¿Cuál es el estado de la gestión de Redes de Transmisión de Datos en Cuba?

¿Qué beneficios técnicos y sociales implica la aplicación de un sistema de gestión centralizado?

El trabajo tiene valor teórico, pues se adentra en el análisis y selección de la literatura desde un punto de vista crítico, que permite realizar el estudio correspondiente y sirve para futuros trabajos.

Desde el punto de vista práctico:

1. Se comenzará un trabajo profundo con el objetivo de integrar en la medida posible, la gestión de Redes de Datos, para lo cual será necesario hacer un estudio exhaustivo de las herramientas necesarias para esta integración.

2. Se logrará una mejor eficiencia y calidad e n los servicios ofertados por las Redes, permitiendo la satisfacción de las necesidades del cliente.

3. Se obtendrá un mejor control del sistema, así como una mayor rapidez en el mantenimiento y reparación del mismo frente a posibles averías.

4. Se tendrá una administración centralizada de todo el equipamiento Telindus.

En cuanto a la metodología, en el trabajo se emplearán métodos como la búsqueda de información automatizada, la actualización en el terreno del equipamiento en cuestión, el trabajo con las herramientas necesarias desde el punto de vista de las Telecomunicaciones y la Informática, díganse por ejemplo, “softwares” a usar y se aplicará el método de revisión bibliográfica.

Como ya mencionamos, existen en ETECSA diferentes subredes de Transmisión de Datos, cuyo entrelazamiento conforma la Red de ETECSA. Estamos hablando de redes como CUBADATA conformada por equipos Alcatel X.25/FR y ATM/FR. La red X.25 consta de Conmutadores PSX-C y PSXC-MC, con sus respectivos modems para llegar a los usuarios y el “backbone” ATM/FR del suministrador Newbridge, que consta de potentes conmutadores como el 7470 MSP y el 7670 RSP, con sus respectivos equipos de acceso y modems, también de Newbridge. La Red de INFOCOM, configurada con “Routers” de la firma Cisco en su mayoría y modems Telindus, y redes de terceros como Colombus, Infomed y Turismo.

La complejidad y heterogeneidad de la red de ETECSA hace bastante difícil la integración de la gestión, pero este trabajo constituye el punto de partida para este análisis.

Para comenzar a trabajar en este sentido, nos ocuparemos en este trabajo, de la propuesta de implementación de un sistema de gestión para los modems Telindus, que permitirá, debido a la plataforma propuesta después de hacer el estudio correspondiente, integrar otras gestiones a este sistema, y de esta manera lograr la calidad en la prestación de los servicios, que persigue

ETECSA, racionalizando al máximo cuanto recurso se necesite, para lo cual es imprescindible la supervisión y control de la técnica instalada.

El documento esta constituido por la introducción, tres capítulos, las conclusiones y recomendaciones, las referencias bibliográficas, un glosario de los términos utilizados y al final, los anexos.

En el primer capítulo se discutirá el estado del arte general de las plataformas de gestión y se hará una comparación entre ellas, destacándose las limitaciones y ventajas de cada una. Ya en el segundo se hace una descripción general de los sistemas de gestión con los que cuenta ETECSA hoy en día, y el tercer capítulo se dedica a la propuesta de implementación del sistema de gestión de los modems Telindus.

CAPITULO 1: ESTADO DEL ARTE DE LA GESTIÓN DE REDES

1. INTRODUCCIÓN

La gestión de redes [60] se define como todos los medios que aseguran el eficaz y eficiente desempeño de un sistema, adecuando sus recursos a un objetivo [17]. Para lograr esto, la administración de redes controla los recursos de red, coordina los servicios, monitorea los estados de la red y reporta el estado y anomalías.

Los objetivos de la gestión son:

Administrar servicios y recursos de red: Control, supervisión, actualización y reporte de estados de la red, configuración de dispositivos y servicio de redes.

Simplificar la complejidad de la gestión de la red: Traducir la información de gestión a un lenguaje fácil de entender por el administrador, por lo que estos sistemas tienen la habilidad de interpretar objetivos de gestión de alto nivel.

Servicios confiables: Proveer a la red de una alta calidad de servicio, minimizar el tiempo "fuera de servicio". Los sistemas de gestión deben detectar y reparar las fallas y errores de la red, además de proteger a la misma de todo ataque a su seguridad.

Costo: Dejar trazabilidad de los recursos de la red y también de los usuarios. El uso de todos los recursos y servicios debe dejar una traza y ser reportado.

OSI posee un modelo de administración de red muy bien definido [18], a propósito de los diseños de arquitecturas de gestión de redes actuales. Este modelo separa las funciones de gestión en cinco áreas funcionales:

Gestión de fallas: Comprende la detección, recuperación y documentación de anomalías y fallas de redes.

Gestión de configuración: Se ocupa de guardar y mantener la configuración de la red, actualizar los parámetros de configuración para asegurar la operación eficaz de la misma.

Gestión de contabilidad: Consiste en actividades de recolección de información de contabilidad y su procesamiento para propósitos de cobro y facturación. Estas actividades

establecen un límite contable para que un conjunto de costos se combinen con recursos múltiples y se utilicen en un contexto de servicio.

Gestión de desempeño: Garantiza un desempeño confiable y de alta calidad a la red. Esto incluye calidad de servicio, regulando parámetros como el rendimiento, la utilización de recursos, demora, niveles de congestión y pérdida de paquetes.

Administración de Seguridad: Proporciona protección contra los ataques piratas a los recursos de la red, sus servicios y datos. Además asegura la privacidad del usuario y controla sus derechos de acceso.

Además de los objetivos de gestión de redes anteriores y las áreas funcionales de OSI, la dirección de la red también debe cumplir requisitos adicionales, de manera similar a los modelos de servicio comerciales de hoy: rapidez para comercializar, diferenciación y personalización del servicio, y flexibilidad.

Se prevee que el futuro de la infraestructura de la red cambie drásticamente la manera en que se hace la gestión de la red y presenta nuevos desafíos para la misma. En primer lugar, como el tamaño de la redes continúa creciendo, cada vez más y más dispositivos de red necesitan ser gestionados eficazmente, exigiendo una mejor modularidad en los diseños de la gestión de redes.

Como resultado del tal aumento del tamaño, las directivas humanas sólo pueden darse a un nivel muy alto de abstracción y generalización. El sistema de dirección de red subyacente debe tener cuidado al interpretar estas directivas de alto nivel en configuraciones de red realizables y vigilar su entrada en vigor. En segundo lugar, como las infraestructuras de redes de varios sectores convergen, tecnologías heterogéneas de redes deben co-existir y trabajar entre si. Los sistemas de gestión de redes deben proporcionar tal integración mediante interfaces de servicio comunes, haciendo transparente tal heterogeneidad tecnológica a los usuarios de la red. En tercer lugar, la naturaleza competitiva de los servicios de red actuales exige operaciones económicas de las redes.

La gestión de la red también debe ser más autorreguladora y autónoma, para ser económicamente beneficiosa. Al mismo tiempo, las soluciones de gestión de red deben mantenerse simples y elegantes, ya que el desarrollo de Internet ha demostrado que sólo simples y elegantes soluciones prevalecerán en redes heterogéneas de gran escala. Por último, como los dispositivos de la red se vuelven más y más poderosos, hay una presión

creciente para utilizar sus capacidades de procesamiento. Esto lleva al aumento de la gestión distribuida de la red a nivel de dispositivo.

2. DESARROLLO

2.1 PRIMEROS TRABAJOS PARA LA GESTIÓN DISTRIBUIDA DE REDES

En la arquitectura tradicional de gestión gestor-agente, tal como SNMP, el agente se trata de la manera más simple posible, él solo realiza tareas de reportes de estado del dispositivo y actualización, mientras el peso de la gestión y el procesamiento de datos lo realiza el gestor. Los estudiosos del tema se dieron cuenta de la inefectividad de este diseño a principio de los 90, cuando el rápido crecimiento de las redes a administrar, unido a la demanda en ascenso de redes eficaces y confiables, obligó por si solo a un re-análisis en cuanto al paradigma de la administración de redes.

SNMPv2 [21][42][55] es el primer gran paso hacia la gestión distribuida de redes. Las RFC (1441-1452) fueron publicadas en el año 1992. SNMPv2 introdujo el concepto de gestor intermediario, el cual puede verse como un gestor mediano. El gestor se comunica directamente con los gestores intermediarios e intercambia información de comandos, mientras que los gestores intermediarios intercambian datos con los agentes. De esta manera los gestores intermediarios manejan algunos procesamientos de datos del lado del gestor y son capaces de desempeñar tareas simples, tales como obtener de manera periódica estados de los agentes sin la intervención del mismo.

En 1995, la IETF (Internet Engineering Task Force), dio un paso más hacia la gestión distribuida, con la propuesta del monitoreo remoto [59]. RMON [52] monitorea o sondea, a través de dispositivos de monitoreo del tráfico de la red. El sondeo puede realizarse a través de aplicaciones integradas a los dispositivos o a través de dispositivos separados. Su tarea es monitorear el tráfico de la red de manera local y reportar las anomalías, si las hubiera, en forma de alarmas, a su gestor. Mediante la definición de distintos tipos de alarma y el umbral o comienzo de las mismas, el gestor es capaz de descargar algunos datos recolectados para el sondeo. Además, mediante el sondeo se puede realizar un pre-procesamiento de datos antes de ser enviados al gestor. De manera general, los primeros trabajos encaminados hacia la gestión distribuida de redes, tuvieron una pobre contribución. Las tareas de gestión se centran todavía en el lado del gestor y solo algunas tareas menores son delegadas a las entidades intermedias (filtrado, notificación y pre-procesamiento de datos).

2.2 TECNOLOGÍAS ACTUALES.

Hace ya casi una década, el paradigma centralizado Agente-gestor clásico se convirtió en la arquitectura de gestión de red, lo cual se ve muy ejemplificado en el modelo de referencia OSI, el protocolo simple de gestión de Red (SNMP) y la Red de gestión de Telecomunicaciones (TMN) [19]. Con el aumento de tamaño y complejidad de las redes, además de los requerimientos de servicios de las redes actuales, tal paradigma no se adecua a las exigencias existentes, y tiene que ser sustituido por paradigmas distribuidos de gestión. Esta tendencia se evidencia de manera profunda en [40].

La tecnología de los últimos años ofrece facilidades y ventajas para la distribución de la administración de redes. Los agentes de administración ya no son calificados como “terminales mudos”, si no como dispositivos sofisticados y son aprovechados como tal.

La inteligencia distribuida denota la capacidad y autonomía de un agente de gestión.

En este epígrafe haremos una breve reseña acerca de las tecnologías existentes a la hora de gestionar redes. Las mencionaremos y examinaremos sus ventajas, desventajas y perspectivas. Presentaremos las tecnologías de acuerdo al grado de capacidad de gestión que se les confiere a los agentes.

La inteligencia distribuida a los agentes de gestión es una tendencia inevitable de las redes de gestión y una cuestión esencial para el éxito de los diseños de administración para las redes futuras. Primero veremos las políticas en las que se basa la gestión, lo cual será seguido del cálculo distribuido y los sistemas basados en WEB y Java, los cuales usan objetos remotos estáticos para facilitar las tareas de descargas de los agentes a los gestores. A partir de ahí, hablaremos de la movilidad de la programación, en la cual los agentes exhiben una gran capacidad en el proceso de gestión. Un paso en este sentido lo constituyen los agentes inteligentes, donde cada unidad de procesamiento coopera con sus semejantes, asumiendo los roles de gestores y agentes de manera intercambiable. Por último hablaremos de las redes activas y de las teorías económicas asociadas a la gestión de redes.

2.3 SISTEMAS DE GESTIÓN BASADOS EN POLÍTICAS.

Las políticas en las que se basa la gestión de redes, se comenzaron a implementar a principios de los 90 [43][30]. A pesar de que la idea de las políticas había aparecido antes, ellas fueron usadas primeramente como una representación de información en un área

específica de la gestión de redes: la gestión de seguridad [14]. La idea de las políticas es aplicable a cualquier estructura. En realidad todas las compañías, ya sean de mediano o gran tamaño, aplican políticas y regulaciones que los empleados deben cumplir. Estas políticas están basadas en los objetivos y metas de las empresas.

En el caso de la gestión basada en políticas, las políticas se definen como las reglas que rigen el estado y comportamiento del sistema de red.

Este sistema de gestión se encarga de:

- La transformación de las metas de gestión que quieren las empresas en reglas confiables encargadas de verificar el estado de la red.
- La interpretación de algunas reglas de las configuraciones de los dispositivos.
- La distribución y ejecución de estas configuraciones por las entidades de gestión.

El modelo de referencia de gestión basada en políticas se apoya completamente en el modelo gestor-agente, el cual comprende los puntos de decisión de políticas (PDPs) y los puntos de ejecución de políticas (PEPs) [24][25]. Las primeras dos tareas son manejadas por los PDPs y la última por los PEPs.

Los protocolos de asignación de recursos (RAP) de IETF (Internet Engineering Task Force) juegan un papel clave en la gestión basada en políticas con sus servicios de políticas de apertura común (COPS) [26] y su extensión (COPS-PR) [10]. Algunos trabajos recientes se refieren a la interpretación de directivas de negocios de las políticas a nivel de red [9] y a la resolución de conflictos de políticas [34]. Más significativo aún es el concepto de meta-políticas propuesto en [4], cuya introducción induce a tareas de decisión de políticas desde los PDP y los PEP. Esto representa un nuevo intento en la potencialización de los agentes, concediéndoles más capacidades a la hora de la gestión, y llevando la gestión basada en políticas hacia un diseño de inteligencia distribuida.

El aporte más significativo de la gestión basada en políticas es que promueve la automatización de los objetivos establecidos para el nivel de gestión sobre un amplio rango de dispositivos de red. El administrador de la red puede interactuar con la misma, debido a la existencia de políticas de alto nivel. Dichas políticas son dispositivos independientes y asequibles a los operadores. El proceso de interpretación automatizada

oculta la complejidad de las configuraciones de los dispositivos de bajo nivel, derivadas de las políticas de nivel alto y por tanto facilita el intercambio de los objetivos de negocio para las configuraciones de red. Comparada con la interpretación de las políticas hechas por el administrador, esta automatización provee una representación más consistente de los objetivos de negocio. Debido a que el estado de las redes cambia constantemente, las políticas son actualizadas automáticamente, para asegurar consistencia en la operación sin la intervención humana. Como las redes crecen constantemente, esta automatización es esencial. A diferencia de otras tecnologías de administración, como las basadas en Java y en agentes móviles, la gestión basada en políticas permite la modificación mucho más rápida de los requerimientos de administración, después del despliegue. Este tipo de gestión, puede adaptar rápidamente los cambios a través de re-configuraciones, en lugar del re-diseño de nuevos módulos para el despliegue. La introducción de nuevas políticas no invalida la correcta operación de la red, las nuevas políticas no entran en conflicto con las existentes.

Para grandes redes con cambios frecuentes, este tipo de administración ofrece una atractiva solución, a medida que dinámicamente se traduce y actualizan los objetivos de negocio de alto nivel en configuraciones de red factibles. Sin embargo, uno de los problemas claves de la gestión basada en políticas radica en su rigidez funcional. Después del desarrollo y despliegue de un sistema de gestión basado en políticas, se definen los servicios primarios. Alternando políticas de gestión y modificando restricciones, se obtiene un alto grado de flexibilidad de acuerdo a las directivas de administración. Sin embargo no se pueden modificar o añadir nuevos servicios de gestión al sistema, a diferencia de la programación móvil ó los agentes de “softwares”.

2.4 SISTEMAS DE GESTIÓN DISTRIBUIDOS (DISTRIBUTED OBJECT COMPUTING)

DOC (Distributed Object Computing) utiliza la metodología de Orientación a objetos (OO) para construir las aplicaciones distribuidas. Su adaptación a la gestión de redes provee el soporte para la arquitectura de la gestión de redes distribuidas, hace la integración con la soluciones de gestión de redes heterogéneas existentes y proporciona herramientas de desarrollo para los componentes de gestión de las redes. DOC provee una distribución de los servicios y aplicaciones de una forma transparente, mediante la separación de la complejidad de la distribución de objetos, de la funcionalidad de la gestión de redes. Otra ventaja de esta separación es la habilidad de proveer protocolos de comunicación de gestión múltiples a los cuales se accede a través de interfaces compactas API (Abstract

Programming Interface), las cuales se encargan de la interoperatividad de los protocolos de administración de las redes heterogéneas, tales como SNMP (Simple Network Management Protocol) para redes IP y CMIP (Common Management Information Protocol) para redes de Telecomunicaciones. Además, DOC (Distributed Object Computing) provee plataformas distribuidas para la implementación de robustos servicios y aplicaciones. Las dos adaptaciones fundamentales de DOC a la gestión de redes son: CORBA (Common Object Request Broker Architecture) [49] y DCOM (COM distribuido) [53]. La principal aplicación de DOC a la gestión se manifiesta en dos áreas. Primero, DOC es usado para diseñar sistemas de redes de gestión distribuidas, en trabajos de estandarización hechos por TINA-C (Telecommunication Information Network Architecture Consortium) [51], JIDM (Joint Inter Domain Management) [20], y proyectos de investigación, como MESIS [3]. Todas estas entidades proveen servicios remotos transparentes mediante el uso de DOC. De esta manera, los servicios y procesos de gestión no necesitan ser situados en lugares centralizados dentro de la red, pero si en lugares remotos de manera distribuida. Esto permite que las tareas se deleguen por regiones ó áreas funcionales a las entidades intermedias. En segundo lugar, DOC se utiliza para aumentar las infraestructuras de gestión de redes existentes con capacidad distribuida.

Las funcionalidades básicas que debe ofrecer un sistema de gestión distribuido son las siguientes.

- **Escalabilidad**: Permite satisfacer las necesidades de gestión crecientes de recursos y de cantidad de información almacenada.

- **Capacidad de distribución**: Debe ser capaz de distribuir, entre las distintas estaciones remotas de la red, las funciones de supervisión, recogida de datos, sondeo y control del estado de los componentes de la red.

- **Capacidad de gestión heterogénea**: Debe tener la capacidad de gestionar ambientes enormemente heterogéneos en cuanto a tipo de red y a sus elementos integrantes.

- **Interoperabilidad**: Debe poseer la capacidad de incorporar nuevas aplicaciones e integrar a las existentes.

CORBA esta basado en el modelo cliente / servidor, aunque aplicado a cada transacción, con lo cual un cliente en una transacción puede ser servidor en otra. La negociación de petición de objetos (Object Request Broker), componente básico de CORBA, se encarga

de transportar las peticiones que hacen los clientes a los servidores y devolver las respuestas que se generan. La principal característica de ORB es la transparencia con que realiza las operaciones, independientemente de la localización de los objetos y la independencia que posee con el lenguaje de programación utilizado para su implementación. La independencia con el lenguaje de programación ofrecido por CORBA permite la interoperatividad entre clientes y servidores implementados en lenguajes de programación diferentes.

CORBA es más potente que SNMP y menos complejo que CMIP. A esto se añade la ventaja que tiene CORBA por su proximidad a C++ y Java, dos lenguajes de gran difusión.

La gestión distribuida en general, CORBA en particular, es una tecnología bien aceptada para el desarrollo de la gestión integrada. El éxito de CORBA puede atribuirse a que ha establecido un ambiente de soporte para la distribución de objetos y un conjunto de servicios asociados. En este caso, DOC es muy útil como herramienta de integración para los dominios de gestión de redes heterogéneas y arquitecturas de gestión de redes existentes. Sin embargo, DOC usa aún distribución estática de objetos, lo cual no le da la flexibilidad que ofrece la movilidad del código. Además, requiere soporte dedicado de tiempo de ejecución, lo cual no se alcanza siempre en todos los dispositivos de una red. Este último detalle, restringe el área de despliegue de esta tecnología.

2.5 GESTIÓN BASADA EN WEB

La gestión basada en “web” es una de las tendencias actuales de los sistemas de gestión. Es un nuevo paradigma que permite la gestión de los dispositivos de red usando navegadores estándares de “web”. Los sistemas de gestión basados en web facilitan el uso de las tecnologías de gestión mejorando significativamente el servicio de la red debido a que:

- La simplicidad y omnipresencia de la interfaz de navegación web (“Browser”) puede reducir significativamente la curva de aprendizaje del administrador de red.
- Los navegadores (“browsers”) están disponibles sobre una gran diversidad de hardware.

En la era de los estándares y la simplicidad, el bajo costo juega un papel determinante en la búsqueda de nuevos modelos de gestión. Puede ser que por esa razón, la gestión

basada en Web aventaje a los modelos de gestión existentes [45]. La idea básica es simple: emplear el navegador de Internet y la tecnología asociada, por ejemplo la tecnología Java, para la gestión de redes. Debido a esto, los fabricantes de equipos ya están desarrollando equipamientos con servidores HTTP integrados y las compañías que desarrollan soluciones de gestión están integrando a las mismas esta nueva tecnología.

2.5.1 PROPUESTAS DE ARQUITECTURAS DE GESTIÓN BASADA EN WEB

El desarrollo de las tecnologías web y java permiten el acceso a la información de forma fácil y flexible. Usando tecnología web el usuario accede a la página web y el servidor ejecuta una Interfaz de acceso común (CGI, Common Gateway Interface) y genera la respuesta, insertando la información en un fichero HTML que el usuario descarga y visualiza en su navegador. La facilidad de acceder a la información de gestión por medio de paginas web ofrecida por esta tecnología, la ha hecho muy atractiva para el desarrollo de ciertos sistemas de gestión.

Algunas propuestas de arquitecturas de gestión sobre web son: [45]

- WBEM (Web-Based Enterprise Management) [58]
- JMAPI (Java Management API)
- Modelo Three-tier y Two-tier de Wipro

Los servicios con servicios Web incorporados aplican la tecnología Web para todos los dispositivos gestionados, tales como se presenta en [28][39]. Cada dispositivo gestionado es un pequeño servidor Web, capaz de aceptar solicitudes HTTP, procesar los datos del dispositivo, construir presentaciones HTLM/XML de los datos del dispositivo y transmitir documentos construidos. Debido a la naturaleza auto-contenida de los servidores con servicio Web incorporado, no existen requerimientos para soporte adicional de gestión. El administrador de red, puede simplemente interactuar con un servidor con servicio Web incorporado a través de un navegador Web estándar. No obstante, estos servidores no tienen un amplio uso en dispositivos con limitación de recursos, debido a que dejan huellas. Además, no hay métodos eficientes y económicos de transformación de dispositivos existentes, en servidores con servicios Web incorporados. Por el contrario, las plataformas de gestión basadas en Web usan la tecnología Web como el núcleo en el diseño de plataformas de gestión, con sus propios

protocolos, modelos de datos y arquitectura. Los dos primeros tipos de infusión Web son los más usados en nuestros días. En ambos casos, el procesamiento preliminar de los datos de los dispositivos, la formulación de reporte de estado y la presentación GUI son manejadas por entidades separadas, diferentes de los gestionadores de red.

2.6 GESTIÓN DE RED BASADA EN JAVA

Java, un lenguaje de programación orientado a objeto es el instrumento para una gran variedad de paradigmas de gestión de redes, desde la gestión basada en Web hasta los agentes inteligentes. Debido a esta amplia variedad de aplicaciones, muchos ambientes basados en Java, han sido diseñados soportando aplicaciones de gestión de redes. Su amplio uso se debe en primer lugar a que las soluciones de “softwares” basados en Java, son relativamente baratos comparados con otras soluciones de “softwares”, tales como los de las aplicaciones basadas en CORBA. La máquina virtual Java (JVM) es el único soporte en tiempo de ejecución necesario por un “software” Java y es además muy fácil de desarrollar y requiere muy poco mantenimiento. En segundo lugar, cada vez más JVM se encuentran disponibles y esto facilita el soporte Java. Además, Java puede interoperar con navegadores Web, los cuales son buenos candidatos como consolas de gestión baratas y accesibles. En tercer lugar, la descarga de código dinámica permite la distribución dinámica de objetos. Esto no solo brinda la oportunidad de extensiones de servicio de tiempo de ejecución, sino que también ofrece la posibilidad de comisiones de gestión. Como cuarto aspecto, Java es una plataforma independiente, aplicable a cualquier plataforma de gestión existente que soporte JVM. Por último, los “softwares” Java, son fáciles de desarrollar y existen muchas herramientas y ambientes favorables para su desarrollo. Además es un buen lenguaje para encontrar nuevos conceptos de gestión de redes, como la movilidad del código.

A lo mejor, el mayor y más mencionado problema de Java es su desempeño. Java no es un lenguaje eficiente. Su desempeño puede ser lento, especialmente si se requiere descarga dinámica. La serialización e invocación de métodos remotos de objetos de Java son muy comúnmente usados en la gestión de redes. Ambos tienen problemas de desempeño. La serialización consume mucho espacio, lo cual no es un gran problema en estaciones grandes, pero si en dispositivos pequeños. La invocación de métodos remotos de Java (RMI) no es un recurso de red conciso en su operación y tiende a desperdiciar recursos de red en cada invocación.

Como una alternativa al desarrollo de WBEM, Sun Microsystems y otras 15 compañías desarrollaron y presentaron la Java Management API. JMAPI es un ambiente para desarrollar aplicaciones de gestión web usando el lenguaje de programación Java. Usa una simple Conectividad de bases de datos abierta (ODBC, Open Database Connectivity) para acceder a la información de gestión recolectada. Para acceder a los datos de gestión y analizarlos, se crean mini Applicaciones ("applets", Lenguaje de programación Java] que se ejecuten en cualquier sistema operativo, con maquina virtual de java. JMAPI soporta protocolo SNMP por lo que estas aplicaciones pueden acceder directamente a la información coleccionada por los agentes SNMP. [50] Esta siendo muy usado en las nuevas versiones de Aplicaciones de gestión realizadas por prestigiosas compañías como HP y Castle Rock computing.

Mucho más de lo que su nombre indica, JMAPI es un ambiente de desarrollo de aplicaciones de gestión de redes que permite una amplia lista de funcionalidades que los diseñadores se habían visto obligados a obtener por su cuenta en el pasado. Estas funcionalidades incluyen clases de interfaces de usuario para crear tablas y gráficos, APIs de red para SNMP, estructuras de RPC (Remote Procedure Calls) y métodos de acceso a bases de datos. En teoría, las aplicaciones basadas en JMAPI interoperan sin inconvenientes, usando las mismas capacidades y posibilidad de acceso en toda la Web. [12].

2.7 MOVILIDAD DEL CÓDIGO PARA GESTIÓN DE REDES.

En 1991, Yemini et al introdujeron por primera vez el concepto de Gestión por Delegación (MbD), y más tarde, en 1995, refinaron este concepto en sus trabajos [16]. Sugirieron además llevar las tareas de gestión hacia el lado agente. Esto puede ser logrado transportando de forma dinámica, programas desde los administradores hacia los agentes y realizando localmente las tareas de gestión delegadas.

Tres ventajas inmediatas del MbD se ponen de manifiesto; primeramente, la gestión no es más una entidad de procesamiento centralizada en la red. Muchos de sus procesos pueden ser descargados hacia los agentes a través de programas delegados. En segundo lugar, se ahorra una gran cantidad de recursos de red. Por ejemplo, la recolección de datos puede hacerse localmente.

Por último, es posible incrementar la funcionalidad de los agentes proporcionándoles programas delegados en el momento de la ejecución. De esta manera, algunos monitoreos

de la red y toma de decisiones pueden realizarse localmente, posibilitando respuestas más rápidas a las solicitudes de gestión y una mejor tolerancia a las fallas (en caso de caída de la gestión).

La movilidad del código puede ser considerada como la capacidad de una aplicación para distribuir y reubicar sus componentes en el tiempo de ejecución. Obviamente, debe existir alguna forma de comunicación y soporte de ejecución para las aplicaciones utilizando la movilidad del código.

Hay mucha confusión en la literatura en lo que respecta a las terminologías usadas para la movilidad del código, además la introducción de agentes inteligentes también oscurece el concepto. En este documento, nosotros no consideramos a los agentes inteligentes como parte del concepto de la movilidad del código. Por lo tanto, los agentes inteligentes se consideran más complejos y autogobernados que la movilidad del código, y serán tratados en otra sección.

En términos de la movilidad del código, existen dos tipos: movilidad débil y movilidad fuerte.

En la movilidad débil, programas completos ó fragmentos de codificaciones se transportan entre componentes distribuidos, sin retener estados de ejecución y datos después de la transportación. Llamamos codificación móvil a aquellas que exhiben una movilidad débil [32].

En la movilidad fuerte, el programa completo, junto con sus estados de ejecución y datos se transporta entre componentes remotos. El programa suspenderá su ejecución antes de terminar y resumirá la ejecución después del comienzo. A las aplicaciones que exhiben una movilidad fuerte las llamamos agente móvil. La mayoría de los trabajos de investigación, tales como [56][29][33], se centran en este concepto. Los términos codificación móvil y agente móvil se usan a menudo de forma intercambiable, y algunas veces tienen significados diferentes en las literaturas.

Con la movilidad del código, las tareas de gestión ya no tienen que ser realizadas por los administradores. Ellos simplemente generan objetivos de gestión y procedimientos de tareas perfiladas y la ejecución de las tareas se delega a los agentes. Baldi y Picco [2], definieron 3 paradigmas de movilidad del código basados en la interacción entre servicios y

fuentes: Código en demanda (COD, Code On Demand), Evaluación remota (REV, Remote Evaluation), y Agentes móviles (MA, Mobile Agent).

En el caso de Código en demanda, el administrador ha coleccionado las fuentes pero carece del código para el procesamiento. El código se descarga dinámicamente desde un servidor de códigos para su ejecución.

En la evaluación remota, el administrador retiene el código y el agente retiene las fuentes. El administrador dinámicamente carga el código al lado agente. El código cargado se ejecuta en los recursos, y el resultado regresa al administrador. En el caso de un agente móvil, el administrador retiene los servicios en forma de componentes de procesamiento y el agente retiene los recursos. El administrador reubica todos los componentes de procesamiento, lo cual incluye el código, el estado de ejecución y posiblemente los datos, hacia el agente. Si los datos requeridos están distribuidos a través de diferentes agentes, el agente móvil tiene la habilidad de reubicarlos de un agente a otro, realizando el procesamiento de los datos y dejando un rastro de los datos intermediarios generados.

El paradigma MA es característico de la movilidad fuerte, mientras el COD y los paradigmas REV son característicos de la movilidad débil.

Como el código móvil se transporta a través de la red, este debe ser cargado en el destino para la ejecución. El tiempo que demora para suspender la ejecución de un componente, empaquetar su código y datos, el transporte a través de la red, restaurar el componente y ejecutarlo puede ser bastante grandes. Así, la movilidad del código no es un buen candidato para las redes con solicitudes de servicios simples pero frecuentes. Además, para prevenir a los agentes móviles de recursos de red adversamente afectados, se ponen medidas de seguridad, ya sea restringiendo las operaciones que un agente móvil puede realizar en los recursos locales, como proporcionando algún tipo de puerta de acceso. Ninguna solución es satisfactoria ya que las restricciones de accesos restringen la capacidad operacional de los agentes móviles, mientras que las puertas de accesos añaden innecesarias sobrecargas de procesamientos.

2.8 AGENTES INTELIGENTES.

Los agentes inteligentes tienen las siguientes características: autonomía, habilidad social, reactividad, pro-actividad, movilidad, aprendizaje, y creencias.

Un agente independiente es una entidad independiente capaz de realizar acciones complejas y resolver problemas de gestión por él mismo. A diferencia de la movilidad del código, un agente inteligente no necesita que le den instrucciones para funcionar, sólo los objetivos de alto nivel. El uso de agentes inteligentes niega completamente la necesidad de utilizar entidades de gestión dedicadas, ya que los agentes inteligentes pueden realizar las tareas de gestión de red en forma coordinada y distribuida, a través de las comunicaciones entre ellos mismos.

Muchos investigadores creen que los agentes inteligentes son el futuro de la gestión de redes, ya que existen algunas ventajas significativas en el uso de los agentes inteligentes para la gestión de redes. Primeramente, los agentes inteligentes, proporcionarían una solución completamente modular a la mayoría de las áreas de gestión de redes. La jerarquía de los agentes inteligentes, pudiera, cada una de ellas, asumir una pequeña tarea en su ambiente local y coordinar sus esfuerzos globalmente para lograr algunos objetivos comunes, tales como, mantener el uso completo de la red, al máximo posible. En segundo lugar el procesamiento de los datos y la toma de decisiones se distribuyen completamente, esto alivia los cuellos de botella de la gestión, que se dan en las soluciones centralizadas de gestión de redes. Además, el sistema resultante de gestión de redes es más robusto y tolerante a las fallas, ya que el mal funcionamiento de un pequeño grupo de agentes, no tiene un impacto significativo en la función general de la gestión. En tercer lugar, el sistema completo de gestión es autónomo, los administradores, solo necesitan proporcionar directivas a nivel de servicio para el sistema. Por último los agentes inteligentes son auto-configurables y auto-gestionables. En la actualidad es posible construir un sistema de gestión de redes que sea completamente auto-gobernado y auto-mantenido. Tal sistema facilitaría la carga de las rutinas de gestión de red que un administrador de red actualmente tiene que hacer.

Wooldridge and Jennings [62] definieron tres tipos de arquitectura para los agentes inteligentes: agentes deliberativos, reactivos e híbridos. Los primeros se basan en un sistema de símbolos físicos, el cual describe una configuración físicamente realizable de símbolos que pueden ser combinados para formar estructuras completas y es capaz de ejecutar procesos que operan en estos símbolos para generar acciones generales inteligentes. Trabajos actuales como [31] hacen uso de los agentes deliberativos.

Los agentes reactivos son lo contrario de los anteriores. Ellos no requieren una representación compleja de conocimientos ni representaciones precisas de información.

Estos agentes generan comportamientos basados en observaciones ambientales, ya que no incluyen modelos mundiales simbólicos. En la práctica, los agentes reactivos responden mejor que los deliberativos, debido a la falta de cualquier mecanismo complejo de razonamiento simbólico. Los agentes reactivos pueden ser exitosamente aplicados al monitoreo del tráfico, diagnóstico de fallas, control de congestión y de acceso, ya que estas funciones de gestión no requieren representación precisa de un modelo mundial. Además estos agentes son capaces de dar respuestas rápidas.

Los agentes híbridos están formados por ambos: agentes deliberativos y agentes reactivos. Un agente híbrido contiene un agente mundial simbólico, planes de desarrollo y toma de decisiones de la forma que lo hace un agente deliberativo. Sin embargo también es capaz de reaccionar a eventos que ocurren en el ambiente sin comprometerse en razonamientos complejos. El componente reactivo de un modelo híbrido sobrescribe su componente deliberativo para lograr una respuesta rápida. El componente híbrido parece ser un candidato apropiado para el diagnóstico de fallas [11]. No obstante, los agentes híbridos son mucho más grandes que los agentes deliberativos ó reactivos. Esto puede ser un problema cuando se esperan grandes niveles de movilidad en un sistema de gestión de red.

La aplicación de los agente inteligentes a la gestión de redes está aún dando sus primeros pasos y muchas cuestiones difíciles, aún permanecen sin resolver. Como las aplicaciones usando agentes inteligentes surgen en la gestión de redes, el problema de gestionar estos agentes, también se vuelve sumamente importante. Los agentes auto-gobernados no pueden vagar por la red libremente y acceder a recursos vitales. Actualmente es aún muy difícil diseñar plataformas de agentes inteligentes. Esto es principalmente debido a que hoy en día existen muy pocas prácticas en la vida real, usando agentes inteligentes. Aún tenemos que determinar, qué es una buena plataforma de agentes inteligentes, en términos prácticos. Debido al hecho de que se autoriza más inteligencia y posibilidades a los agentes inteligentes, su talla se vuelve una preocupación creciente para el transporte de la red. Además las comunicaciones Agente-agente, típicamente usa el lenguaje de tratamiento de encuestas (KQML, Knowledge Query Manipulation Language). KQML desaprovecha cantidades sustanciales de recursos de red, puesto que sus mensajes son muy voluminosos. Por último, la protección contra agentes inteligentes maliciosos está bien plasmada en la literatura actual.

2.9 REDES ACTIVAS

De acuerdo a Tennenhouse et al. [57], una red activa es un nuevo acercamiento a una arquitectura de red, en la cual los nodos, tales como “Routers” y “Switches” realizan cálculos personalizados en los mensajes que llegan a ellos. En las redes activas los “Routers” y “Switches” ejecutan servicios personalizados que son cargados dinámicamente desde servidores remotos de codificación o desde paquetes activos.

La característica de esta actividad tiene tres vistas. En la vista de equipo, las operaciones y servicios de un dispositivo pueden ser actualizados dinámicamente y extendidos activamente en el momento de ejecución. En la vista del proveedor de red, todos los recursos de la red pueden ser proporcionados y personalizados activamente según la base de los clientes. En la vista del usuario de red, los recursos asignados pueden ser configurados activamente, basados en las necesidades de aplicación del usuario.

Las redes activas, combinadas con la movilidad del código, presentan una tecnología efectiva para distribuir las tareas de gestión a nivel de dispositivo.

No solamente las tareas de gestión pueden ser descargadas a dispositivos individuales de red, sino que el proveedor de tareas de gestión no tiene que ser más gestor de las entidades. Dicha solución proporciona personalización completa y provee los medios para los procesos distribuidos a través de todos los dispositivos de la red; se puede operar mediante plataformas usando código activo independiente del dispositivo, sostiene innovación de usuario y personalización del servicio basado en el usuario, acelera nuevo servicio y despliegue de tecnologías de red, desviando el proceso de estandarización y el consenso del vendedor, permite asignación de recurso basado en características del servicio individual. En la literatura, existen dos acercamientos generales para llevar a cabo las redes activas: acercamiento de conmutador programable y acercamiento en cápsula. El primero usa canal fuera de banda para la distribución del código. La transportación del código activo se separa completamente del tráfico regular de datos. Este acercamiento es más fácil de gestionar y seguro, ya que el código activo se distribuye mediante canales seguros y privados. Se ajusta a gestores de redes que configuran componentes de red. Por otro lado, los paquetes de acercamiento de cápsula activan el código en paquetes de datos corrientes. El código activo se envía a los nodos activos a través de canales de datos corrientes. Este acercamiento permite una personalización abierta de los servicios específicos de los usuarios, sin embargo, es más propenso a amenazas de seguridad. [5] analizó los beneficios de las redes activas para emprender la gestión de red.

Se han hecho trabajos bastante recientes en la exploración de redes activas para la gestión de red, tales como: proposición Red activa virtual (VAN, Virtual Active Network) [8] y la arquitectura de red activa basada en agentes [23].

No obstante, la seguridad sigue siendo una barricada mayor para la aplicación práctica de la red activa. No solamente la integridad de los recursos de red y datos de usuarios tienen que mantenerse, sino que también el contenido de los datos de los usuarios debe permanecer confidencial. Esto último implica una gran confianza en los nodos activos que un paquete puede visitar en el camino hacia su destino, puesto que es necesario examinar y procesar de alguna forma los datos de los usuarios. Como expresó Murphy et al. [46], hay muchos objetos que asegurar en las redes activas, lo cual incluye: usuarios finales, nodos activos, ambientes de ejecución, y códigos activos. Los modelos de confianza para estos objetos son también bastante complejos. Además de la seguridad, la provisión de recursos y tolerancia de fallas son los otros dos tópicos principales que necesitan ser dirigidos en las redes activas.

Primeramente, debido a que los recursos se emplean para el procesamiento personalizado de los paquetes de datos en la red, tienen que establecerse algunos medios para controlar la prioridad de acceso a los recursos y el límite del consumo de los mismos. Este asunto crea nuevos requerimientos para la gestión de red que deben ser dirigidos. Otro elemento relacionado es el consumo de ancho de banda de la red. Después de todo, los servicios específicos de usuarios deben ser transportados a través de la red y cargados. Si se utiliza el acercamiento en cápsula, el transporte de estos servicios viene en contienda directa con la transportación de los datos de usuarios. Simplemente cobrar a los usuarios por el despliegue de los servicios pudiera no ser deseado ya que esto desalienta al usuario de personalizar los nodos activos en la red.

En segundo lugar, la tolerancia de fallas en la red tendrá problemas si servicios específicos de usuarios no se controlan adecuadamente.

Debido a que los usuarios ganan habilidad para gestionar los recursos de red y realizar procesos personalizados, más y más aplicaciones y servicios de usuarios se integran dentro de la red. La calidad de estos servicios/aplicaciones no puede determinarse tan bien como los servicios suministrados por el fabricante. La solución obvia es proveerle a cada servicio de usuario un ambiente de ejecución aislado y separado. Sin embargo, esta solución es muy costosa en términos de consumo de recursos y rendimiento de la red.

2.10 TEORÍA ECONÓMICA

La gestión de redes empleando la teoría económica propone modelar los servicios de red como un modelo de mercado abierto. La red resultante es auto-regulada y auto-ajustada, sin la presencia de ninguna infraestructura de gestión de red. Los administradores de red controlarían indirectamente las dinámicas de red induciendo incentivos y definiendo políticas económicas agregadas. Tal acercamiento puede parecer muy audaz, pero delinea su teoría a partir de las ciencias económicas bien establecidas. Las premisas para aplicar teorías económicas son: existencia de redes abiertas y heterogéneas, orientación multi-vendedor, y servicios competitivos. Se han hecho pocos trabajos en esta materia, y la mayoría de ellos están enfocados a usar la teoría económica como modelo de coordinación de agente [6][7]. Como se discutió anteriormente, la gestión de agentes inteligentes está aún olvidada en la literatura actual. Usar la teoría económica para gestionar sistemas multi-agente pudiera ser una alternativa viable debido a su simplicidad y naturaleza auto-sostenida.

Sin embargo, la aplicación de teorías económicas a la gestión de red está en una etapa experimental primaria. Muchos problemas críticos acarreados con estos experimentos generan dudas en la aplicabilidad de la teoría económica a la gestión de redes. Utilizar modelos de mercado para gestionar redes es una idea nueva. No obstante, algunos elementos deben ser cuidadosamente considerados. En primer lugar, la fuerza de mando para un modelo de mercado es la autenticidad de su actualidad, por lo que los valores actuales y sus procesos de transacción deben ser seguros. Además, estas transacciones seguras deben ser realizadas muy eficientemente, ya que sería una operación muy frecuente. En segundo lugar, la política económica para el modelo de mercado debe ser diseñado de forma tal que estimule la competencia justa, y relacione fuertemente los recursos y sus precios. Por último, el modelo de mercado operaría en una escala amplia, requiriendo estandarización de sus elementos y operaciones. Esta estandarización puede ser un proceso muy lento y requeriría un consenso total de todos los vendedores participantes.

2.11 PLATAFORMAS DE GESTIÓN DE REDES

Existe en el mundo de las Telecomunicaciones, una amplia gama de plataformas para la gestión de Redes, por lo que a la hora de elegir una, se deben tener en cuenta diferentes aspectos, con la finalidad de aplicar la mejor de acuerdo a la red que se tenga y a las necesidades de gestión. Algunos de estos aspectos son:

Aplicaciones genéricas o propias: Son aquellas que forman parte del "software" de gestión. Proporcionan la supervisión coherente y eficaz de los elementos a gestionar en la red realizando el inventario de dichos elementos y la gestión de los mapas físicos, además de recoger y presentar en tiempo real todos los acontecimientos. También, deben proporcionar todos los servicios relativos al manejo de alarmas (registro de incidencias, historia de las alarmas, etc.) de un sistema de gestión registrando todas las alarmas que ocurren y manejando las activas.

APIs para la integración de otras aplicaciones de gestión: El "software" de gestión debe proporcionar facilidad para la integración de aplicaciones de gestión ya sean estas del proveedor de dicho "software" de gestión o de terceros. Las APIs garantizan la apertura del "software" y se recomienda estén basadas en estándares internacionales como por ejemplo la X/Open, JMAPI, etc. También los "softwares" pueden poseer herramientas para el desarrollo de agentes y aplicaciones de gestión.

***Seguridad que posee*:** La interfaz de usuario, o consola de gestión de los "softwares" de gestión, se debe proteger. Por esto se emplean nombres de usuario, contraseñas y perfiles de usuario. Además, el intercambio de la información de gestión entre agentes y gestor debe estar protegido a través de la autenticación.

Sistemas operativos sobre los que se soporta*:* El "software" de gestión debe estar soportado por los sistemas operativos más comunes, o sea Windows de Microsoft, Linux, etc. Cada sistema operativo tiene sus ventajas, pero el Windows es uno de los más usados en el mundo y es muy amigable. Es por ello deseable que el "software" de gestión seleccionado soporte Windows, garantizando así que el administrador y/o operador domine dicho sistema operativo, y con ello se facilite la instalación y uso del "software" de gestión.

Interfaz de usuario*:* La interfaz de usuario es el punto de contacto de los usuarios de la gestión con el "software", por lo que este debe proveer una interfaz gráfica de usuario (GUI), por las ventajas que ofrece la misma, la cual debe integrar a todas las aplicaciones de gestión aún cuando el "software" de gestión tenga una arquitectura modular donde cada módulo puede funcionar por sí solo con su consola independiente. Se recomienda además, la existencia de una interfaz en modo comando para situaciones de emergencias dónde no esté disponible la interfaz gráfica.

***Protocolos de gestión que soporta**:* Para gestionar las redes TCP/IP el protocolo empleado tradicionalmente es el SNMP, aunque es conveniente que el "software" de gestión soporte el mayor número posible de estos protocolos. Otros protocolos que no son de gestión pero que proporcionan algunas herramientas para estas funciones son: TCP/IP, IPX y NetBIOS.

Base Web: Se debe analizar si el software de gestión brinda soporte para la gestión basada en *web*.

Requerimientos del Sistema: El "hardware" necesario para el buen funcionamiento del "software" de gestión debe estar en correspondencia con las posibilidades reales de que exista o se pueda adquirir por la institución y con la arquitectura de gestión a emplear; distribuida o centralizada, con agentes inteligentes, etc.

Precio: Es otro aspecto a tener en cuenta a la hora de seleccionar entre varias opciones posibles.

Entre las plataformas más usadas tenemos el SNMPc, el "3Com Transcend Enterprise Manager", el "Whatsup Gold", el "CiscoWork for Windows", y el OpenView Node Network.

2.11.1 SNMPC, DE CASTLE ROCK COMPUTING.

Castel Rock Computing fue una de las primeras compañías que desarrolló la gestión SNMP basada en Windows, siendo considerada una de las más veteranas en el mercado de "software" de gestión TCP/IP [54]. Su aplicación SNMPc es considerada una de las mejores en el mercado [12].

El SNMPc es una suite ("software" que integra una serie de aplicaciones de gestión) para gestión distribuida de redes pequeñas y grandes. Tiene dos versiones, Enterprise Edition y Workgroup Edition cada una con sus especificidades.

Aplicaciones Genéricas o propias: El SNMPc brinda las aplicaciones que en general poseen los "softwares" de gestión, destacándose en:

- Arquitectura distribuida (solo Enterprise Edition): Cada aplicación gestora principal o "master" puede importar los mapas de una o varias aplicaciones gestoras remotas o "esclavas". Las alarmas se propagan automáticamente, a través de la arquitectura de gestión distribuida, desde los gestores "esclavos" hasta los "master". Puede

establecerse una arquitectura donde cada servidor se comporte como master y esclavo simultáneamente.

- Creación automática de estados de alarma: El agente monitoriza todas las variables durante un periodo de tiempo (una semana), llamado de aprendizaje, y calcula los valores típicos de estas variables para cada hora del día durante la semana. Después, los valores que se van obteniendo en los siguientes monitoreos se comparan con los valores típicos calculados y si la diferencia entre ambos es muy grande se genera una alarma. Los umbrales de alarma se pueden reconfigurar manualmente.

- Proporciona el mejor "browser" MIB del mercado: Según se plantea en un numeroso grupo de artículos especializados, no solo permite la fácil navegación a través del árbol de la MIB. Incluye, además, una descripción detallada de cada variable. Su soporte a las herramientas de análisis de desempeño RMON-1 también es muy bueno.

- SNMPc trabaja con más de 350 MIB: Puede monitorizar y gestionar casi todos los dispositivos de red actuales sin necesidad de incorporarle nuevas MIB de gestión. Las aplicaciones Bitview o Hubview proporcionan una vista del dispositivo monitoreado, mostrando todas sus interfaces y ofreciendo menús para realizar las encuestas SNMP mas frecuentes a los agentes.

- El algoritmo empleado por la herramienta de auto descubrimiento de nodos de la red, basado en TCP/IP y SNMP, no es muy efectivo en arquitecturas jerárquicas. No es capaz de colocar todos los nodos en las subredes correspondientes lo que provoca que los mapas resultantes no contengan una información fidedigna de la ubicación de los dispositivos en la red. Por lo anterior se recomienda solo buscar (*scanear*) dispositivos en una o dos subredes a la vez y crear manualmente el mapa general.

APIs para la integración de otras aplicaciones de gestión: Su escalabilidad y soporte de aplicaciones de terceras partes no es de los mejores aunque en las nuevas versiones han logrado avances en este sentido.

Seguridad que posee: Solo la que le brinda el sistema operativo donde esté instalada.

Interfaz de usuario y gestión basada en web : Es muy potente y permite, entre otras posibilidades, gestionar los nodos individuales directamente desde la estación de gestión solo haciendo doble click sobre su ícono correspondiente en el mapa de la red. La versión SNMPc Enterprise Edition proporciona acceso al sistema a través de la consola local y de una consola remota, ambas con las mismas posibilidades de acceso. La consola remota puede ejecutarse en cualquier estación Windows de la red, que tenga conexión TCP/IP. Si se quiere tener mayor número de consolas remotas hay que comprar el componente Remote Console, que también incluye una consola Java, la cual puede ser usada desde cualquier navegador web en la red. Este componente, además, posee un proxy Java-Telnet para la configuración de diferentes dispositivos. La versión SNMPc Workgroup Edition solo proporciona una consola local [41].

Protocolos de gestión que soporta: El protocolo de gestión empleado por este "software" es el SNMP. Además, usa la arquitectura de protocolos de red TCP/IP para algunas funciones de monitoreo.

Requerimientos del software y precio:

Parámetro	Enterprise Edition	Workgroup Edition
CPU	Pentium II 266 MHz	Pentium II 266 MHz
Memoria	128 Mb	64 Mb
Disco Duro (HDD)	500 Mb	100 Mb
Sistemas operativos (SO)	Win 2000, NT	Win 2000, NT, 98
SO para Consola Remota	Win 2000, NT	-
Precio	Más de $4000.00	$699,99

Este "software" de gestión es muy aconsejable para grandes LAN con numerosas estaciones y gran número de subredes.

2.11.2 3COM TRANSCEND ENTERPRISE MANAGER DE 3COM.

Esta herramienta es ofrecida por la compañía 3Com que actualmente es una de las líderes en el mercado del equipamiento para redes informáticas.

Aplicaciones genéricas o propias: Brinda un conjunto completo de aplicaciones para la gestión, que incluyen monitoreo y control de los dispositivos de ultima generación puestos en el mercado por 3Com. Permite descubrir todos los dispositivos IP en una red y los enlaces entre ellos. Este proceso de descubrimiento puede realizarse en la red local o incluir también subredes de hasta 512 nodos. Crea mapas de forma automática con la topología y la estructura de la red, proporcionando una imagen gráfica, o en forma de árbol, de las conexiones y los nodos de la red. A partir del mapa de la red el administrador puede: saber el nivel de congestión que presenta un nodo o enlace, obtener el conjunto de umbrales y alarmas empleadas por la aplicación, y generar reportes.

Algunas de sus aplicaciones son: [1]

Transcend LANSentry: Proporciona un soporte completo de RMON y RMON-2 para los dispositivos de 3Com, permitiendo a los administradores ver estadísticas y tráfico de LAN remotas de forma sencilla.

Transcend Central: permite a los usuarios navegar por los nodos de la red desde una sola pantalla y facilitando el rápido conocimiento y la evaluación de los problemas en la red.

Alarm Management: Permite controlar como serán manipuladas las alarmas procedentes de los dispositivos 3Com.

Network Admin Tools: Posibilita definir, para grupos de dispositivos, su configuración y la forma de realización de actualizaciones.

ATM and VLAN Management: Brinda facilidades para emular y configurar redes ATM y LANs virtuales.

APIs para la integración de otras aplicaciones de gestión: Es un “software” propietario y la versión que se ofrece junto con los equipos, no brinda posibilidades de integración con aplicaciones de otros fabricantes.

Seguridad que posee: Solo la que brinda el sistema operativo donde esté instalada**.**

Interfaz de usuario y gestión basada en web: Posee una interfaz gráfica intuitiva pero no brinda la posibilidad de gestión basada en web. Aunque la mayoría de los

equipos de 3Com ofrecen un servidor web para su gestión, que no brinda todas las posibilidades de la gestión directa por consola

Protocolos de gestión que soporta: Basa su funcionamiento en el protocolo SNMP

Requerimientos del Sistema y precio:

Parámetro	Transcend Enterprise
CPU	Pentium 166 MHz
Memoria	32 Mb (64 Mb recomendada)
Disco Duro (HDD)	50 Mb
Sistemas operativos (SO)	Win 9x, NT 4.0
Precio	Incluido en el costo del equipamiento

Una característica muy importante de la estrategia de gestión de red usada por 3Com es el uso de agentes inteligentes distribuidos a lo largo de la red los que se comunican directamente con los dispositivos, monitorizándolos automáticamente. En algunas ocasiones estos agentes pueden realizar acciones correctivas independientes de la consola de gestión. Seleccionando la información a enviar a la consola, los agentes inteligentes pueden reducir el tráfico por la red. Esta facilidad está presente en todos los productos de hardware proporcionados actualmente por 3Com. [1]

2.11.3 WHATSUP GOLD, DE IPSWITCH.

EL Whatsup Gold (WUG) de Ipswitch es un “software” de monitoreo gráfico de redes, diseñado para redes multiprotocolos (TCP/IP, IPX y NetBIOS). Usa alarmas visibles y sonoras para avisar de problemas en los dispositivos o servicios más importantes de la red. Además, puede enviar bajo ciertas circunstancias avisos remotos por medio de beeper, *WinPopup*, e-mail, teléfono o ejecutar un programa determinado. Proporciona una interfaz WEB que permite visualizar el mapa y el estado de la red, desde un navegador si se poseen los permisos adecuados para ello. Permite, además, realizar de forma remota varias pruebas de conexión (*ping*, *traceroute*, *loockup* y *scan*). No se precisa de un entrenamiento especial para su configuración y puesta a punto. [61]

Aplicaciones genéricas o propias:

Auto-descubrimiento: Con este "software" se puede crear el mapa de la red de varias formas. Los métodos de auto-descubrimiento son:

- Encuesta SNMP a los dispositivos de la red IP en los cuales esta conectada la estación de gestión.
- Identificación de cualquier dispositivo TCP/IP, NetBIOS o IPX.
- Servicio automático para graficar redes Windows
- Crea el mapa de la red usando un ícono diferente para cada tipo de dispositivo (estaciones, servidores, "routers", subredes, "hub", "printer", etc.). Cada dispositivo se asocia a su dirección específica, puede ser IP o IPX. Además de descubrir los dispositivos TCP/IP, puede conocerse qué servicios (HTTP, SMTP, POP3, DNS, etc.) están activos y seleccionar de ellos, cual debe ser monitorizado

Monitoreo de la Red: El WhatsUp Gold realiza la monitorización de los recursos conectados a la red TCP/IP las 24 horas del día y los 7 días de la semana. Soporta un amplio rango de protocolos usados comúnmente en las redes actuales, por ejemplo ICMP, TCP/IP, NetBIOS, IPX, y SNMP. ICMP proporciona el mecanismo básico que utiliza el WhatsUp Gold para la mayoría de las labores de monitorización, mientras el TCP/IP es usado para monitorizar sistemas fuera de la pared de fuego que no permiten el paso de paquetes ICMP. El SNMP se usa para monitorizar cualquier agente SNMP presente en la red, recibe y registra los "traps" SNMP. Genera notificaciones relacionadas con cada "traps" específico, visualiza la información SNMP de los elementos de red y grafica sus valores en tiempo real. Ofrece soporte NetBIOS para supervisar el estado de las redes Microsoft Windows locales y soporte IPX para monitorizar los servidores de ficheros e impresión de las redes Novell NetWare. Monitoriza además cualquier recurso que sea reconocido en la red TCP/IP, específicamente "routers", "switches", "hosts", servidores, puentes ("*bridges"*), "hub" y otros dispositivos. Por otra parte, puede monitorizar servidores RADIUS, web, email y DNS, que son servicios definidos en el "software". Además, se pueden añadir nuevas capacidades de monitorización a través de módulos *"Plugins"* desarrollados por terceras partes. Monitoriza los servicios comunicándose directamente con el puerto

donde el servicio esta ejecutándose. Además brinda la opción de definir otros tipos de servicio que no son estándares de forma personalizada. [48]. Monitorea de manera limitada a los dispositivos que soportan SNMP, porque utiliza los estándares de Internet: SNMP versión 1 y MIB II. Es posible hacer ampliaciones a la MIB original con nuevas MIB propietarias suministradas por los fabricantes. Las versiones modernas de WhatsUp Gold incluyen ya SNMPv2.

Obtención de información del mapa de la red: El mapa ofrece información gráfica sobre problemas reales o potenciales de la red. Si ocurre un evento se reflejará un cambio de color en la representación sobre el mapa. La forma de usar el código de colores, y la definición del número de encuestas perdidas para reconocer un fallo, puede configurarse para cada uno de los dispositivos monitorizados.

Reportes: WUG registra dos tipos de datos: cambios en el estado de la red (llamados eventos), como la salida de un dispositivo de la red; y estadísticas de sondeo (*polling*) para cada dispositivo. A partir de los datos registrados, este software puede crear, usando el menú de reportes los siguientes reportes y gráficos que muestran el estado de la red en diferentes formas:

- **Gráfico de rendimiento**: Muestra los dispositivos de mejor o peor rendimiento
- **Reporte de eventos**: Muestra los momentos de entrada y salida de dispositivos, activación o desactivación de servicios y la apertura y cierre de los mapas del WhatsUp.
- **Reportes estadísticos**: Muestra las estadísticas *MaxAvgRTT* y *MinAvgRTT* (por ciento máximo y mínimo del RTT (tiempo de respuesta) de un servicio para n solicitudes), así como *StdDeviation* (Desviación estándar de los valores anteriores) en los sondeos a cada dispositivo.

APIs para la integración de otras aplicaciones de gestión: Brinda la posibilidad de interaccionar con servicios de chequeo desarrollados por terceras partes a través de una API externa. Esta API esta basada en el *Component Object Model* (COM) de Microsoft. Además, permite la integración con otras aplicaciones de gestión como por ejemplo el CiscoWork. Las bases de datos que emplea este software son ficheros en

formato texto (.txt) lo que permite desarrollar, de forma sencilla, aplicaciones graficas que hagan uso de esta información.

Seguridad que posee: La interfaz de usuario no posee ningún tipo de seguridad cuando el software esta instalado en Win 98. Si se instala como un servicio de NT entonces adquiere la seguridad que dicho sistema operativo brinda a todas sus aplicaciones. La interfaz Web si posee un sistema de seguridad, basado en la autentificación de los usuarios y perfiles de usuario, que incluye el acceso a la información que puede tener cada usuario.

Interfaz de usuario y gestión basada en web: Ofrece una interfaz gráfica con barras de tareas, iconos y cuadros de diálogos intuitivos y amistosos para los usuarios. Brinda además un grupo de comandos para el trabajo directamente desde la consola. Proporciona además un servidor web, que permite visualizar el estado de los dispositivos en la red, elaborar reportes y casi todas las facilidades que brinda la consola del WUG, además, permite cambiar la configuración del servidor web del WUG utilizando para estas funciones como navegador, Internet Explorer 4.0 o Netscape 4.0, desde cualquier computadora conectada a la red. La interfaz web tiene varios niveles de seguridad que permiten personalizar los privilegios de los usuarios sobre cada mapa.

Usando la interfaz web del WUG existen dos formas para visualizar los mapas, una gráfica con formato JPEG muy similar a la GUI del WhatsUp Gold; y otra, tipo texto, que muestra un listado de los dispositivos.

Requerimientos del Sistema y precio:

Parámetro	Whatsup Gold
CPU	66 MHz
Memoria	16/32 Mb
Disco Duro (HDD)	5 Mb
Sistema operativo (SO)	Win 98, 2000, NT 4.0
Precio	$ 699.00

Desventajas

Existen dos importantes desventajas a considerar en este “software”: la primera es que no permite transferir información de gestión entre diferentes gestores de forma automática. Hay que desarrollar una aplicación que realice esta tarea y la otra es que es completamente dependiente de la plataforma Microsoft.

2.11.4 CISCOWORK FOR WINDOWS

Cisco es una de las compañías líderes en el mercado de “hardware” y “software” para redes de cualquier tamaño.

Aplicaciones genéricas o propias: El *CiscoWork for Windows* está compuesto por cuatro aplicaciones de gestión que pueden ejecutarse de forma independiente. Estas son:

CiscoView : *H*erramienta grafica para la gestión de dispositivos, que proporciona vistas actualizadas de los paneles trasero y delantero de los dispositivos de Cisco, pantallas gráficas actualizadas dinámicamente, que emplean códigos de colores para mostrar con mayor facilidad el estado de los dispositivos, el resultado de los diagnósticos de componentes específicos de los dispositivos y la posibilidad de ejecutar otras aplicaciones.

*E*s ejecutado en una estación de gestión central desde donde se puede monitorear datos vitales de los recursos Cisco usando una simple Interfaz Grafica de Usuario (GUI). Esta GUI muestra información estadística y reportes dinámicos del estado y desempeño. También es posible solicitar, configurar y monitorear otros datos. [35]

Threshold Manager**:** mejora la capacidad para establecer límites (umbrales) en los dispositivos. Emplea para esto Cisco RMON (*Cisco Remote Monitoring*), lo que reduce los gastos fijos de administración y suministra mayor capacidad para la solución de problemas. Cada tipo de dispositivo Cisco tiene asociado un perfil de políticas por defecto. Además de estas políticas definidas por el fabricante para cada tipo de dispositivo, se pueden crear otras nuevas que respondan a intereses específicos de la red en particular [44]. Cuando una política definida es violada ocurre un evento. En este caso el agente RMON del dispositivo realiza diferentes funciones:

***StackMaker*:** permite a los usuarios combinar varios dispositivos de Cisco (solo los: Catalyst 1900, Catalyst 2800, y Catalyst 2820) en una sola pila y administrarlos visualmente en una sola ventana.

***Show Commands*:** muestra información detallada de los protocolos y del sistema utilizado por los dispositivos Cisco que son objeto de gestión, sin que sea necesario que el usuario recuerde complejos comandos de Cisco IOS(r).

Proporciona acceso a los comandos EXEC de los dispositivos Cisco, a través de una GUI basada en Java. Además, oculta el proceso del establecimiento de la sección *telnet.* Con solo seleccionar el comando deseado de un cuadro de dialogo con arquitectura de árbol, permite mostrar información detallada sobre el sistema y los protocolos. [13]

Requisitos de hardware y software:

Parámetro	**CiscoWork for Windows**
CPU	PC IBM ó Pentium a 166 MHz
Memoria	64 Mb
Disco Duro (HDD)	500 Mb, aunque se recomienda 1 Gb
Sistema operativo (SO)	Win 95,98 (seg. Edición),NT 4.0 (Service Pack 5 preferentemente)

Se requiere de Netscape 4.61 o Internet Explorer 5.0 para visualizar la ayuda en línea.

El uso del *CiscoWork* es imprescindible para la adecuada gestión de una Red que cuente con un numeroso grupo de dispositivos Cisco, como es el caso del NAP en la Red de ETECSA, pero su gran limitación es estar enfocado solamente a este tipo de dispositivos, porque no se puede pensar en un sistema de gestión integral soportado sobre el CiscoWork for Windows. Sin embargo, puede asociarse con algún “software” de gestión que sea el encargado de gestionar el resto de los recursos de la red, como pudiera ocurrir con el HP Openview en la Red Infocom. Es recomendable su uso solo cuando una tarea de gestión específica lo requiera, debido a que consume muchos recursos de la máquina y los datos obtenidos por esta aplicación no pueden ser usados por otros “softwares” de gestión.

2.11.5 OPENVIEW WORKGROUP NODE MANAGER DE HP

OpenView es actualmente el producto número uno en el mercado de gestión de red. Ofrece una plataforma admirable con sólidas bases en todas las categorías de gestión. Su principal característica está basada en la posibilidad que ofrece a productos de terceros para extender y desarrollar las capacidades de la plataforma. Su mayor inconveniente es el costo.

Aplicaciones genéricas o propias: OpenView Network Node Manager (NNM) proporciona, como la mayoría de los "softwares" de gestión de red herramientas para la gestión de configuración prestaciones y fallos de recursos sobre redes TCP/IP e IPX/SPX. NNM se puede usar para: [45]

- Descubrir automáticamente los componentes de la red, así como monitorizar su estatus.
- Obtener la topología de la red actualizada a partir del descubrimiento automático
- Diagnosticar y resolver fallos y problemas de prestaciones desde un punto de control.
- Gestionar los recursos de distintos fabricantes que soporten los protocolos de Gestión estándar.
- Correlacionar eventos para determinar la razón principal por la que produce un fallo.
- Observar la configuración de la red a través de gráficos y tablas.
- Personalizar la estación de gestión adicionando herramientas en la barra de menú.
- Analizar necesidades futuras de la red, pues permite almacenar la información que recolecta y graficarla para su análisis.

APIs para la integración de otras aplicaciones de gestión: OpenView ofrece una interfaz para la programación de aplicaciones destinadas a la gestión de redes. Esta es una de las razones por la que resulta muy difícil encontrar una plataforma de gestión de red que sea más difundida que OpenView.

Seguridad que posee: La seguridad que posee esta aplicación se basada en el sistema operativo donde este instalada.

Interfaz de usuario y gestión basada en web: Interfaz de usuario basado en Java. Lo que proporciona un acceso fácil a los mapas de la red y permite la gestión web desde cualquier punto de la red. Brinda una vista de la red en forma gráfica muy intuitiva. [47]

Protocolos de gestión que soporta: CMIP, SNMP

Requerimientos del Sistema y precio

Parámetro	OpenView NNM
CPU	150 MHz
Memoria	64/96 MHz
Disco Duro (HDD)	570/620 Mb
Sistema operativo (SO)	Windows NT y Unix
Precio	De $4,995.00 a $16,995.00

3. CONCLUSIONES

Todas las tecnologías discutidas en este documento intentan proporcionar inteligencia distribuida a los agentes de gestión. La gestión de redes basada en políticas permite a los administradores delegar parcialmente las tareas de gestión a los agentes en forma de políticas concretas. La gestión de redes web descarga el procesamiento, presentación y despliegue de información de dispositivos a vías de acceso web o servidores web integrados. El estimado de objetos distribuidos, tales como CORBA, y gestión de redes basados en Java provee el medio para la distribución de tareas de gestión en la red, mediante el despliegue de objetos estáticos distribuidos.

La movilidad del código y las redes activas delegan tareas de gestión a los agentes de gestión a través de la descarga de códigos móviles dinámicos. Los agentes inteligentes avanzan la inteligencia distribuida aún más lejos, definiendo agentes autónomos que son capaces de tomar decisiones complejas de gestión. El papel de tales agentes inteligentes no está ya confinado ni al gestor ni al agente, ya que los agentes inteligentes pueden adoptar estos roles de forma dinámica, basados en sus tareas asignadas ó en sus propias

motivaciones. Por último, las teorías económicas niegan completamente la necesidad de una infraestructura de gestión de red, modelando la red como un mercado abierto auto-regulado.

Para influenciar completamente los beneficios de las tecnologías presentadas. Los diseñadores de gestión de red deben balancear todos los beneficios y desventajas, como se discutieron en este documento. Creemos que la inteligencia distribuida es una de las tendencias más importantes en la gestión de redes complejas a gran escala en el presente y el futuro. A pesar de la diversidad de estas tecnologías, su uso en la investigación de gestión de redes apunta hacia la inteligencia distribuida en la red.

Como pudimos apreciar, cada plataforma de gestión analizada, tiene sus características propias, cada una con sus ventajas y desventajas, destacándose la potencialidad de NNM HP Openview, con excepción de su precio. El CiscoWork y el 3Com son “softwares” propietarios, el primero se usa como detallamos en la gestión de los equipos del NAP, cuyo equipamiento es de Cisco en su totalidad.

Posee NNM HP Openview, al igual que la mayoría de las plataformas de gestión, una potente interfaz de usuario y una gestión basada en Web, mejor que SNMPc y mucho mejor que 3Com. El uso de los protocolos de gestión, por HP Openview, supera a todos los “softwares“mencionados, pero su mayor ventaja es la posibilidad que ofrece para la integración con otros fabricantes.

CAPITULO 2: ESTADO ACTUAL DE LA GESTIÓN DE REDES DE TRANSMISIÓN DE DATOS DE ETECSA.

1. INTRODUCCIÓN

En ETECSA existen actualmente diferentes Redes de Transmisión de Datos, las cuales tienen puntos de presencia en todas las capitales de provincias del país y en muchos municipios de las mismas. Estas redes son: CUBADATA, conformada por la Red de Conmutación de paquetes X.25/FR y la Red “Backbone” ATM/FR, Enet ó Infocom y redes de Terceros como Turismo, Infomed, Citmatel, etc. De ellas se gestionan actualmente de manera centralizada, los conmutadores de las redes X.25 /FR y los equipos Newbridge del “backbone” ATM/FR.

Además de estas redes, existe un centro de Conmutación de todos los ISP, el cual se denomina NAP. Los conmutadores usados son Cisco y se encuentra en fase de instalación un sistema de gestión para los mismos, quedando sin administrar los modems usados en las redes.

2. DESARROLLO

2.1 ARQUITECTURA DE REDES

2.1.1 RED DE CONMUTACIÓN DE PAQUETES X.25/FR

La Red X.25 de Conmutación de paquetes está conformada por conmutadores PSX de la firma Alcatel: PSX-C en nodos principales y PSXC-MC en nodos secundarios. Ambos se apoyan en equipos de acceso para llegar a los usuarios. El PSX-C consta de hasta 128 puertas, compartidas en enlaces de hasta 19,2 (Tarjetas ACTUJ), 144 (Tarjetas DCJ64 y DCV 35) y 2048 Kbit/s (Tarjetas DCMXE). Por su parte el PSXC-MC puede portar hasta 36 puertas y se configuran fundamentalmente con tarjetas DCMXE, DCV 35 y ACTUJ.

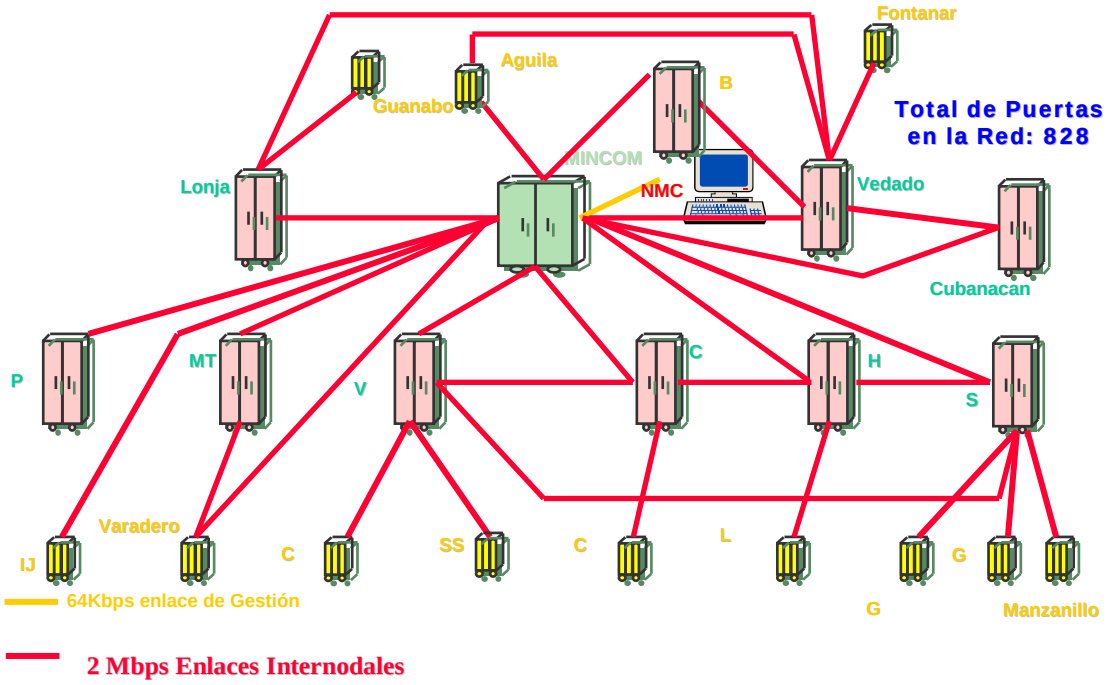


Figura 1. Red CUBADATA X.25 de ETECSA

Como se observa, los enlaces internodales son a 2 Mbit/s y de manera general los nodos secundarios se conectan a los nodos principales que geográficamente le quedan cerca, los cuales a la vez se enlazan con el nodo instalado en el MINCOM, el cual, por supuesto, es el más potente y está enlazado con el NMC, ente responsable de la gestión de la red, como explicaremos más adelante.

2.1.2 RED “BACKBONE” ATM/FR

Como evidentemente el “backbone” de datos del país no podía limitarse a la tecnología X.25, en 1999 se comienza la implementación de un “backbone” ATM con puntos de acceso F/R, lo que permite cubrir las expectativas de la casi totalidad de los clientes de datos en el país. Con esta red ya se pueden lograr altas prestaciones, brindando un servicio final de gran calidad. Como resulta evidente que

aún coexistirán clientes F/R en ambas redes, resulta necesario implementar puntos de cruce (Gateway) entre ambas técnicas, por ello se crean FRAMERs ó enlaces de alta velocidad entre ambas redes, permitiendo que los usuarios de CUBADATA se puedan encontrar conectados con cualquiera de las dos tecnologías, lo que en muchas ocasiones está determinado por la técnica existente en el lugar, y permanecer enlazados a través de sus servicios Frame Relay con usuarios de la otra red. La red consta de potentes conmutadores para el transporte como son: el 36170 ó 7470 MSP y el 7670 RSP, y de equipos de acceso como el 3600 y el 3630, los cuales incorporan fundamentalmente las tarjetas para enlaces a 2 Mbit/s (Dual E1) y tarjetas 2B1Q para enlaces por línea de cobre. Se usan modems Newbridge 2703, 2753 y 2801.

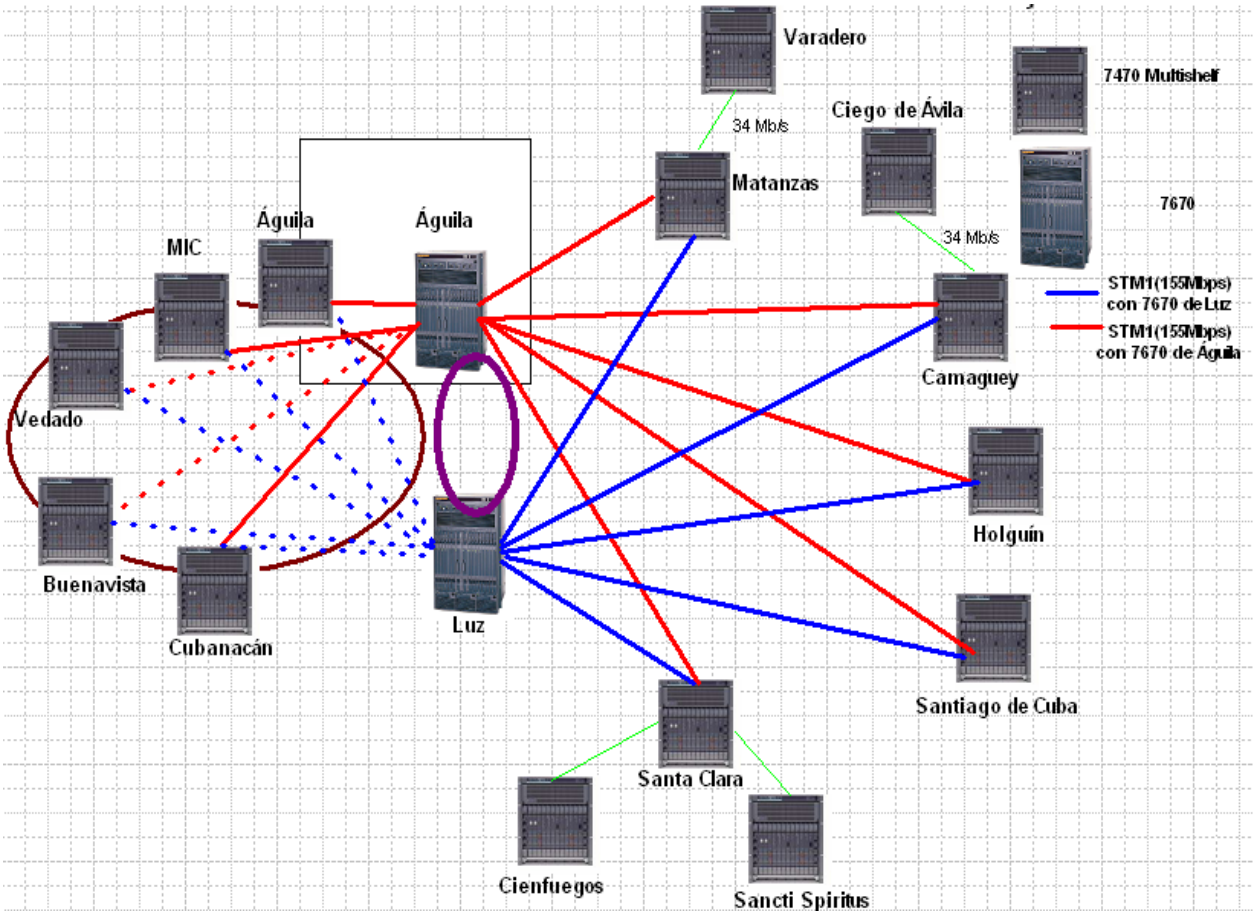


Figura 2. CUBADATA "Backbone" ATM /FR de ETECSA

Los STM-1 son ópticos y los enlaces discontinuos todavía no están en funcionamiento.

El 7470 MSP es un “Switch” multiservicio, escalable y de alta capacidad ATM. Puede encontrarse como “Standalone” simple “shelf” de una capacidad de 1.6 Gb/s ó “Multishelf” de una capacidad máxima de 12.8 Gb/s. Los “shelf” pueden irse agregando a medida que se requieran y sus elementos claves pueden tener redundancia, si así se determina.

De este equipo cuelgan los nodos de acceso 3600 y 3630, los cuales portan fundamentalmente tarjetas para llegar a los usuarios, como son la Dual E1 y la 2B1Q.

2.1.3 INFOCOM

Esta red es el ISP de ETECSA y usa “routers” de la firma Cisco, de la serie 3600 fundamentalmente, los cuales proveen las interfaces correspondientes para enlazarse a Internet a través de canales arrendados ó conmutados.

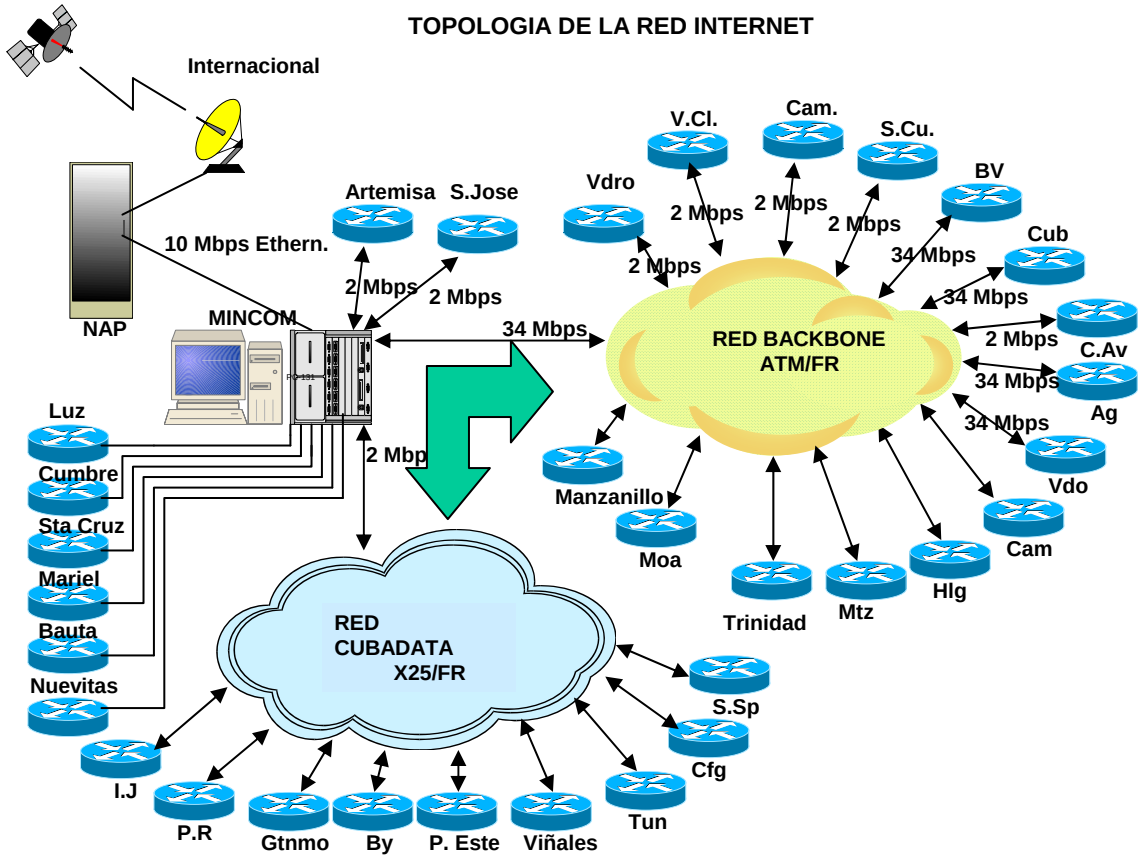


Figura 3. Red Infocom de ETECSA

Para llegar al usuario se usan modems de la firma Telindus, usando tarjetas HS, HDSL y SDSL fundamentalmente.

2.1.3.1 NAP

El NAP, como ya explicamos, se ocupa de recibir la información de todos los ISP y conmutarla. Se encuentra ubicado en el MINCOM y usa equipos Cisco. Se utilizan dos "swiitches" Catalyst 6509 de Cisco y nueve servidores (siete Compaq Proliant DL380G3 y dos de respaldo de información).

Estos equipos se gestionarán en breve. En este momento se instala el equipamiento involucrado.

2.1.4 REDES DE TERCEROS

Las Redes de terceros utilizan las instalaciones y el soporte de ETECSA para llegar a sus usuarios. En cuanto al equipamiento, este varía, pero hay un predominio de los conmutadores Cisco y los modems Telindus, Zyxel y Multitech para el acceso a los usuarios.

2.2 REDES DE GESTIÓN

2.2.1 GESTIÓN DE RED X.25/FR

La gestión de la red de conmutación de paquetes X.25/FR se encuentra instalada en un centro de gestión, ubicado en el MINCOM, cuyo principal ente es el NMC (Network Management Center), el cual provee funciones de operación y mantenimiento para todos los elementos de red. Un solo NMC puede manejar más de 100 conmutadores y varios miles de abonados. Cuando existe más de un NMC, las tareas pueden ser compartidas entre ellos. Él actúa como un abonado más de la red y se conecta a dos nodos principales a través de líneas síncronas. Para el intercambio de información entre los centros de gestión y la red se usa el principio de los circuitos virtuales. En caso de inaccesibilidad de un PSX, usando un canal lógico, un enlace por control remoto vía PSN permite conmutar, recargar ó hacer pruebas, como se muestra:

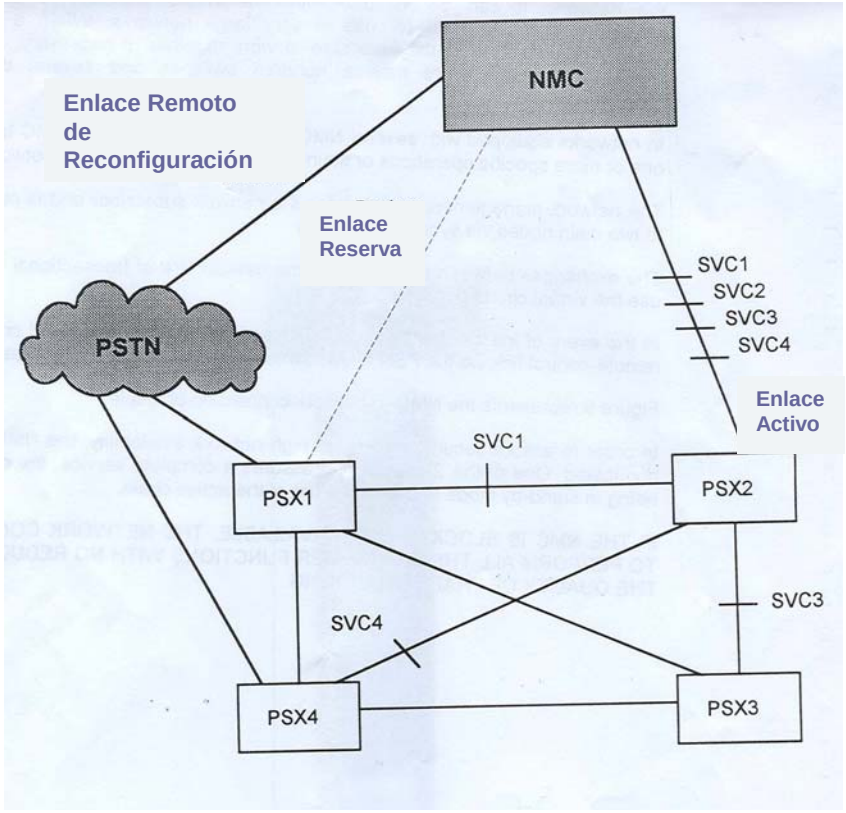


Figura 4. Conexión del NMC a la Red.

Para asegurar la confiabilidad de la gestión de la red, el NMC puede ser duplicado; uno de los dos asume todas las tareas requeridas, mientras el otro se encuentra en "standby", para entrar en servicio en caso de que ocurran fallas. Si el NMC se bloquea o no funciona correctamente en un momento determinado, la red continúa ejecutando todas sus funciones relacionadas con los abonados, sin ninguna afectación de la calidad del tráfico. En el caso de la red de ETECSA, existe un solo NMC, aunque su configuración interna es "master-standby".

La operación y administración de la red se ejecutan desde terminales de diálogo, que pueden ser, una computadora con el "software" PCRET, un terminal de video, o una estación NMU.

Los terminales pueden ser locales ó remotos con relación al NMC (abonados PSX) como se muestra a continuación:

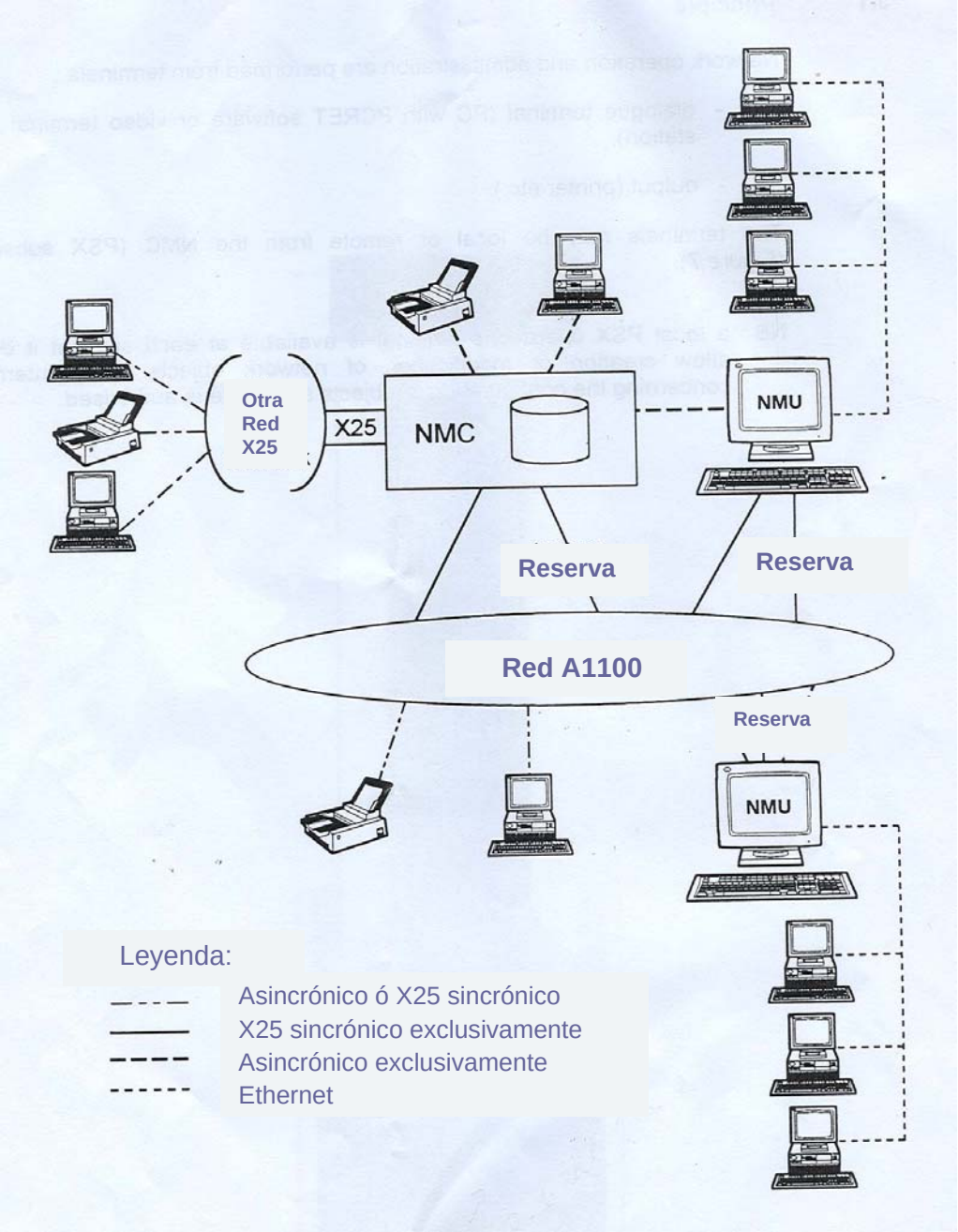


Figura 5. Terminales de Operación

Puede haber en cada sitio un terminal de operaciones PSX, pero el no tendrá la potestad de crear o modificar los objetos de la red, solo podrá encuestar acerca de la configuración de los objetos en el sitio correspondiente. El “software” NMC puede ser dividido en diferentes bloques: Operación del NMC, Interfaz del operador, de la red y los centros de funcionamiento (los técnicos, el de carga, y el de mediciones).

Operación del NMC: Incluye los sistemas de operación para el A8300 (gestión de archivos, de memoria, etc.) y sus operaciones específicas como son la administración de autorización geográfica y funcional de los operadores, la gestión de tiempo, etc.

Interfaz del operador: Provee diferentes servicios al operador, tales como la asistencia "on-line" y la lista de distribución. Esta última permite la inicialización de un número dado de comandos en todos o algunos de los PSX de la red y facilita la determinación de quién conmuta la inicialización automática de los comandos, provee además el registro y reflejo del historial de cada evento, la redirección de los resultados a cualquier terminal de operaciones y el modo de prueba. Este último permite chequear la validación de un comando, sin ejecutarlo.

Interfaz de Red: El NMC se considera un abonado de red, el cual establece por su parte un SVC con cada PSX que el supervisa en la red.

Centros de operaciones: Realizan cada uno, funciones específicas que se detallan en [36].

La gestión puede ser centralizada ó distribuida. En el caso de la centralizada, existe un solo NMC y todas las funciones se centran en él, no así la distribuida, como se muestra a continuación.

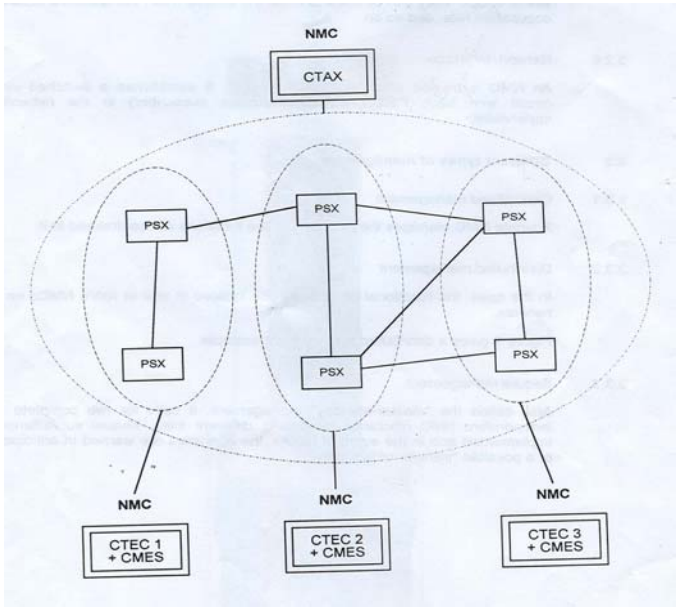


Figura 6. Ejemplo de configuración distribuida

La gestión de seguridad, también llamada, configuración “master-standby”, se basa en dos máquinas independientes, ubicadas en sitios diferentes. Se implementa una supervisión mutua y en caso de falla, los operadores son avisados con anterioridad de una posible transferencia de autoridad en cuanto a las máquinas, como ya explicamos, no contamos con esta variante.

El NMC se enriquece con herramientas externas en forma de módulos de “softwares” instalados en microcomputadoras ó microestaciones como se muestra en la siguiente figura.

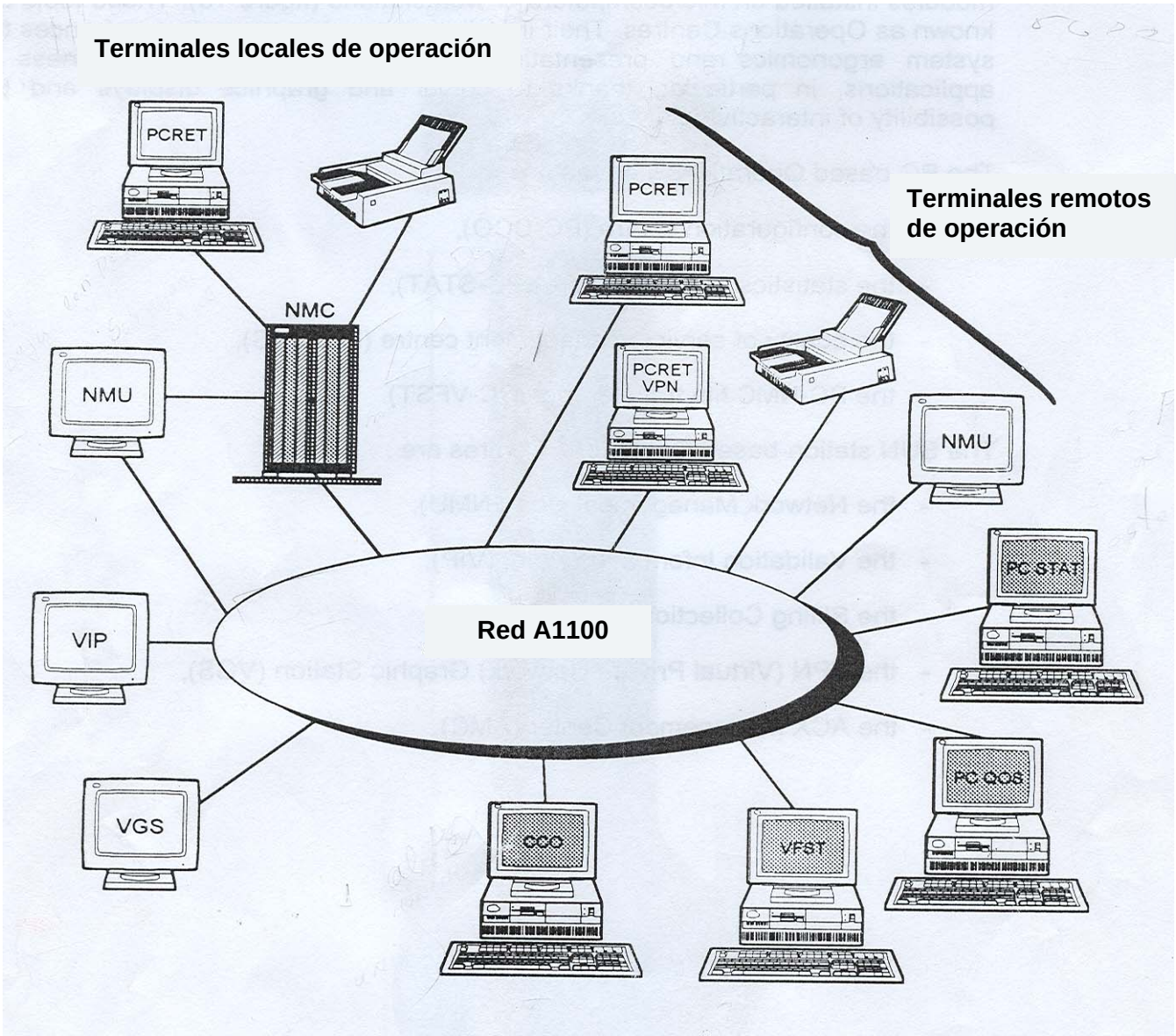


Figura 7. Equipamiento de gestión general en una red.

Estas herramientas son conocidas como centros de operación. Su instalación mejora la ergonomía y presentación del sistema y hace más amigables las aplicaciones, gracias fundamentalmente, a la representación gráfica y al color y a la posibilidad de los diálogos interactivos. Estos centros son el PC-CCO (Centro de configuración), el PC- STAT (Centro de análisis de estadísticas), el PC-QoS (Centro de gestión de calidad de servicio), y el PC-VFST (Herramienta de transferencia de ficheros). Los centros de operación basados en SUN son el NMU ó unidad de gestión de red, el VIP ó Punto de validación de información, el BCC para la facturación, el VGS que es una estación gráfica VPN y la AMC ó centro de gestión ACX.

El PCRET es un terminal de usuario opcional que provee al operador de una interfaz de usuario, con ayuda “on-line”. Contiene todos los comandos y sus parámetros, que se usan para soportar operaciones y procesos de mantenimiento. En el caso de nuestra red, existe un PCRET en cada nodo del país y cuatro en el MINCOM, tres de los cuales se conectan al NMC y el restante al PSX MINCOM, aunque solo tienen permiso de configuración los terminales ubicados en el MINCOM, no así los ubicados en los nodos restantes. El CCO y el VFST son “softwares”, el primero se usa para modificar y reflejar las versiones de configuración de datos y el segundo permite la transferencia de ficheros entre el NMC y la PC. Existe una máquina CCO en nuestra red, la cual se conecta al PSX MINCOM, no así el VFST, con la que no contamos.

Las mediciones QoS son tomadas en el PSX y usadas para determinar la calidad de servicio de la red. Pueden hacerse sistemáticamente y son recolectadas por el NMC desde donde son transferidas a la PC, allí las comparaciones analíticas determinan tráfico general de la red, tal como el intercambio entre los PSXs e información acerca de las actividades periféricas de la red, de esto se encarga el STAT, terminal con el que sí contamos en la red y a través de su conexión al PSX MINCOM se realiza el control estadístico de la misma.

El NMU es un producto de red opcional que agrupa diferentes facilidades de gestión en una única estación de trabajo que es conectada a la red a través de sus puertos síncronos y asíncronos, recibe alarmas y tiene acceso a sus privilegios a través de la conexión con el NMC. Sus facilidades incluyen el despliegue en pantalla del estado de la red, gestión de alarmas, y gestión virtual de VPN. Existen dos NMU en nuestra red de gestión, solo hay uno activo y conectado al PSX MINCOM. VPN y VIP son también servicios opcionales, el primero proporciona al usuario un rango de facilidades

equivalente a los servicios dedicados de una red privada. El terminal es controlado por el NMU y los comandos y alarmas que recibe son restringidos a los recursos del abonado en la VPN. El VIP provee la gestión de un NUI (Identificación de usuario de red) usado por los abonados de red. Existe un BBC ó centro de facturación que trabaja en ambiente UNIX, conectado al PSX a través del cual se realiza la tarificación de la red.

2.2.2 GESTIÓN DE RED "BACKBONE" ATM/FR

El 5620 NM es el sistema de gestión, ahora propiedad de Alcatel, usado para la administración de los equipos Newbridge, el cual combina la gestión y los servicios tradicionales con la nueva generación de Protocolo de Internet/servicios multiprotocolo (IP/MPLS). Permite simplificar el despliegue de los servicios DSL y constituye el corazón de una carpeta de productos de gestión de servicios y redes, que soportan gestión de multiservicio, multitecnología y multifabricante.

Los productos administrados incluyen, el 7770 RCP, el 7670 RSP, el 7670 RSP de servicio extendido (ESE), el 7470 MSP y el 7300.

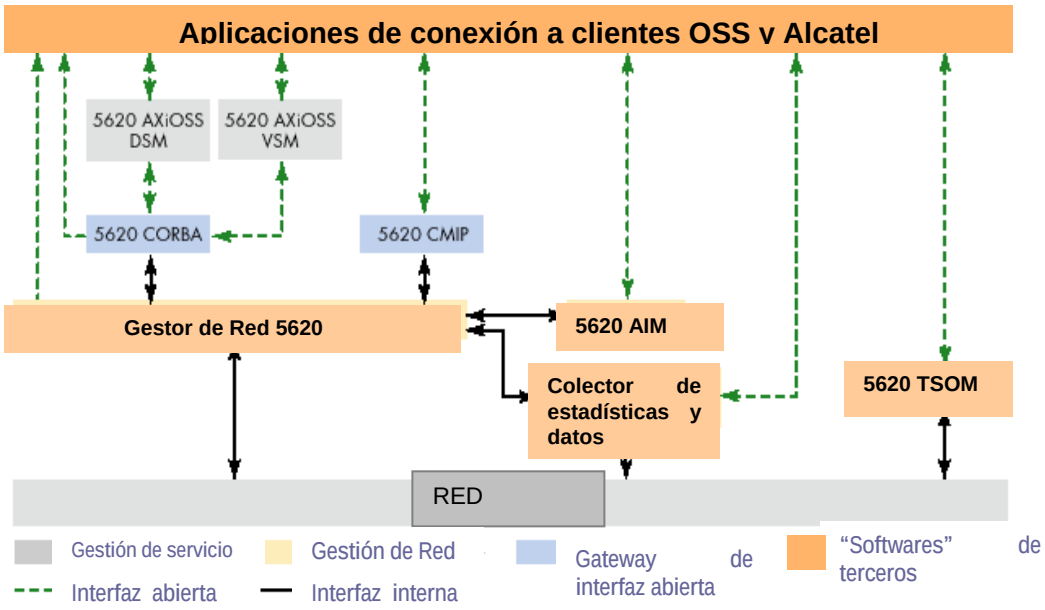


Figura 8. Gestión de multifabricante

En nuestro caso el centro de gestión se encuentra ubicado también en el MINCOM, la misma está constituida por un grupo de máquinas, dos de las cuales son las consolas principales, una es la activa y la otra la de respaldo. Existe además una máquina para la facturación y otra con un simulador para la red.

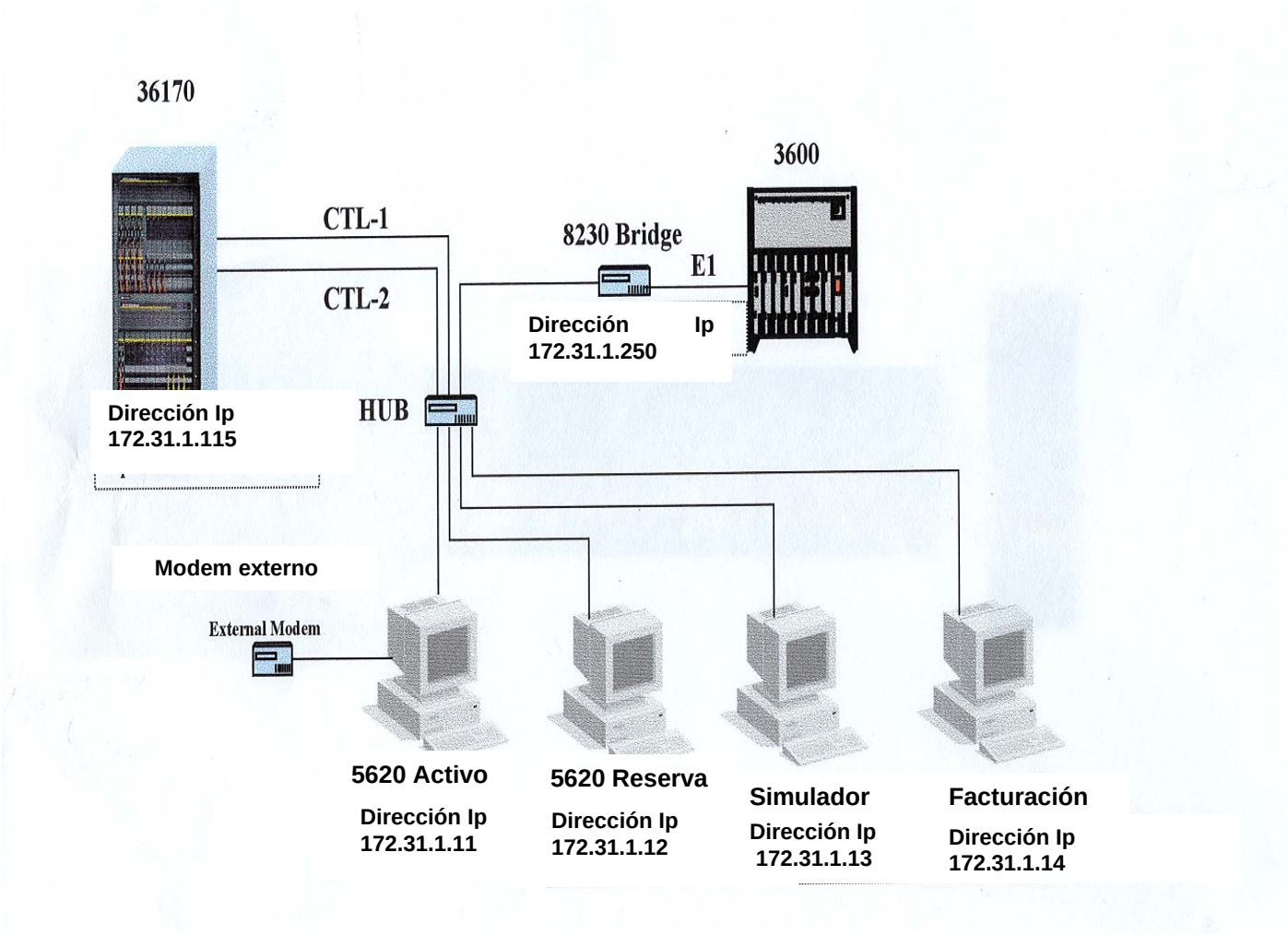


Figura 9. Equipamiento de gestión de Red CUBADATA ATM/FR de ETECSA

2.2.2.1 GESTIÓN DE FALLAS

El 5620 NM monitorea en tiempo real redes completas, incluyendo el aislamiento de las fallas. Una vista general de la red de voz y datos puede obtenerse a través del mapa de la red, el cual cambia rápida y constantemente a medida que el 5620 detecta nuevo equipamiento. Este sistema de gestión provee monitoreo del rendimiento de redes y la gestión de fallas tiene como ventajas los bajos costos de instalación, de operación,

administración y mantenimiento (OAM) y la optimización del costo del ciclo de vida (los equipos duran más y se deprecian en períodos de tiempo más largos).

Iconos estandarizados de los nodos permiten al operador identificar fácilmente los elementos de red. El mapa de la red también notifica cuándo el acceso al control del nodo se ha perdido, manteniendo al mismo informado acerca de qué elementos tienen dificultad y el estado de los mismos. Todas las alarmas son registradas y recolectadas centralmente. Los operadores pueden ubicarlas de acuerdo al del equipo, el tiempo ó la prioridad. Los problemas de la red se registran de acuerdo a AS (Supervisión de alarma integrada), mediante la cual se recibe, almacena y administran las alarmas en tiempo real desde los elementos administrados. La versión más actual es la 6.1 (nosotros contamos con la 4.2), la cual proporciona una solución que se complementa con el 1353, también de Alcatel y permite analizar además, redes de transporte. La implementación de este servicio sería de mucho beneficio para nuestra red de ETECSA.

Después que un problema en la red es identificado, el 5620 provee a los operadores de métodos de aislamiento, prueba y herramientas para resolverlo. Pruebas de diagnóstico a nivel de red aíslan las fallas en los enlaces primarios, indicando gráficamente las mismas, para su rápido reconocimiento.

2.2.2.2 GESTIÓN DE CONFIGURACIÓN

Recursos y conectividad a cada nivel de red, pueden ser configurados por el operador usando la GUI (Interfaz gráfica de usuario). El 5620 detecta automáticamente los nuevos nodos de la red, tarjetas y Objetos IP, cuando estos son añadidos a la misma. El mapa despliega la jerarquía de red y ofrece una vista estructurada de la misma. Los íconos en el árbol de la red representan grupos que contienen íconos de nodos individuales y las conexiones entre ellos. El mapa permite al operador de grandes redes ubicar los objetos en grupos de administración lógicos, facilitando la navegación de un área de la red a otra y la gestión de grupos de nodos.

Con la función “auto-discovery” (auto-reconocimiento) para los nodos, el sistema detecta automáticamente los nuevos nodos e inicia un proceso de reconocimiento, ahorrándole al operador, tiempo de entrada de datos.

2.2.2.2.1 CONFIGURACIÓN IP

La administración IP/MPLS permite ver objetos capa 3 en el mapa, incluyendo “routers”, enlaces IP y LSPs, configurar objetos capa 3 y monitorear fallas en las redes IP/MPLS. También existe una función auto-descubrimiento para las direcciones IP, a través de la cual el sistema detecta los dispositivos IP y después que tiene su configuración determina si será gestionado por el 5620 ó no. Se establecen enlaces IP entre los “routers”, sobre una infraestructura puramente IP, tal como PoS Ethernet y Gigabit Ethernet y redes capa 2, como FR, ATM y Ethernet. Se usa además un enlace IP para representar la conectividad IP entre “routers”.

2.2.2.2.2 CONFIGURACIÓN DSL

Atributos generales pueden aplicarse en la configuración simple ó múltiple de puertos ADSL o SHDSL. La duplicación de configuración se usa para configuraciones remotas. La posibilidad de realizar configuraciones voluminosas DSL, permite hacer encuestas voluminosas en versiones como la 4.2 ó anteriores, lo cual se usa para hacer configuraciones múltiples en objetos de red.

2.2.2.2.3 CONFIGURACIÓN ATM

El balance de carga de la red es soportado a través de las interfaces privadas (PNNI). Para PVCs, el 5620 utiliza un algoritmo de ruteo de bajo costo para establecer las conexiones de extremo a extremo. En el caso de SPVCs ó SVCs los elementos de red utilizan un protocolo de señalización para establecer las conexiones.

Una nueva herramienta de traza de conexión permite al operador listar todos las rutas SPVCs en la red e invocar una conexión SPVC en la base de datos del 5620 NM. Los resultados de esta traza son guardados en un fichero sencillo. También existen nuevas herramientas de conversión PVC-SPVCs.

2.2.2.3 GESTIÓN DE TRÁFICO

Primero debemos decir que el módulo de optimización de tráfico y servicio del 5620 (TSOM) es una solución de Alcatel para el diseño de tráfico. Este módulo es una herramienta LPS de optimización y provisionamiento. Ella implementa un conjunto de algoritmos que incrementan en un 30% el ancho de banda total usado por los servicios

en una red proveedora de servicios sin violar los acuerdos de nivel de servicio (SLAs), además de proveer gestión de rendimiento automatizado para las redes con MPLS habilitada. Este módulo ayuda a evitar la congestión en la red, mediante el re-ruteo LSPs antes de que esta ocurra, lo que permite al operador reservar ancho de banda para los servicios y el balance de la carga de tráfico resultante de los mismos, sobre toda la red.

El 7470 provee especificaciones de gestión de tráfico, versión 4.0 (TM4) y tarjetas de gestión de tráfico y control de congestión. Esto incluye la implementación del control de admisión de conexión (CAC) para determinar cuál petición de conexión se aceptará, sin afectar las conexiones establecidas. El “switch” también provee políticas de tráfico extensivas a través del UPC (Usage Parameter Control), compatibles con los estándares de la industria y el TM4.

SMART (scalability, multipriority, allocation of resources and traffic), implementado en el 7470, garantiza que la calidad de servicio se logre, mientras se optimizan recursos y desempeño del “switch”. Mediante esta capacidad superior de gestión, los proveedores de servicio pueden: optimizar el uso del ancho de banda, lograr ganancias estadísticas y garantizar calidad de servicio, todo lo que se traduce en un ahorro de costo significativo y una amplia gama de servicios para los clientes.

2.2.2.4 GESTIÓN DE DESEMPEÑO Y CONTABILIDAD

Este sistema de gestión ofrece una variedad de estadísticas de red, incluyendo histogramas, estadísticas de contabilidad de llamadas, y reportes administrativos, que influyen positivamente en el desempeño de la red. Esta información puede obtenerse en tiempo real, desde ficheros “ASCII flat” ó desde una interfaz de programa de aplicación (API) TCP/IP. Posee el 5620 un colector de datos de rendimiento, el cual se usa para recolectar la información de los caminos en relación con los PVCs, SVCs, SVCs (usando ATM y FR), troncos, enlaces de acceso (ATM, FR y TDM), redes privadas virtuales IP, LSPs y caminos (paths) MPLS. Esto incluye estadísticas a nivel físico, de trama y de celdas de la red, proporcionando información acerca del volumen de tráfico, congestión de la red, y condiciones de error. El sistema está diseñado además, para ofrecer alta disponibilidad de servicio en cualquier momento, incluso durante las fallas de la red, lo cual minimiza el tiempo fuera de servicio. La redundancia en caliente permite a una segunda estación ejecutar el “software” de gestión 5620 NM

y continuar actualizando. En caso de fallas, o durante la actualización, el control de la red puede conmutar a la estación de respaldo sin interrupción alguna.

El sistema está diseñado con aplicaciones de recuperación que permiten al usuario predefinir sitios “backup” (de respaldo), el mismo tiene la capacidad de re-enrutar, lo cual permite a la red recuperar su configuración sin requerir el concurso de los operadores para ejecutar procesos complicados, que además pueden incurrir en demoras. El operador puede especificar una ruta automática ó seleccionada por él en el momento de la configuración, lo cual asegura que los enlaces y rutas más prioritarias se encuentren altamente protegidas. El ancho de banda puede reservarse en ruta secundaria ó alternativa, por lo que si ocurre una falla en la ruta primaria, el sistema automáticamente conmuta la conexión a la ruta alternativa.

El Alcatel 5620 AIM (Módulo de análisis e inventario) es un nuevo módulo que complementa el administrador de red 5620. Este sistema proporciona un inventario y herramientas de análisis que convierten datos en información que le permite mantener y aumentar la estabilidad de la red. Facilita además la creación de reportes de alarmas, conexiones, inventario de equipos, e información de configuración de sincronización y estadísticas. Además de los más de 100 reportes estándares, los reportes pueden ser ajustados a las necesidades individuales de los clientes, usando la herramienta de creación de reportes “drag and drop” (arrastrar y soltar). Estos reportes pueden ser ampliamente usados por los clientes para anticipar problemas en sus redes, planear el crecimiento de las redes y colocar los recursos donde y cuando ellos lo necesiten.

2.2.2.5 GESTIÓN DE SEGURIDAD

Para proteger la seguridad de la red, cada usuario del 5620 NM debe tener una cuenta del 5620 NM y otra UNIX. Para incrementar la seguridad, las cuentas 5620 NM se restringen a una estación de trabajo específica. Solo el administrador tiene acceso a la cuenta. Cada usuario requiere acceso a la UNIX en la estación que el usará. Cuando las cuentas 5620 se crean, los administradores pueden limitar el acceso de los operadores a la red, mediante la definición de los equipos que él puede ver y configurar, según el administrador y los comandos del sistema de gestión a los que el puede tener acceso. La seguridad incluye la limitación del número de intentos de registro, el bloqueo y justificación de las cuentas, la restricción de cuentas a una

estación de trabajo específica y el envío de un “trouble ticket” (reporte de falla) ó un e-mail (correo electrónico) cuando los intentos de registro exceden los predeterminados.

2.2.2.6 GESTIÓN DE SERVICIO

El módulo AXiOSS de servicio DSL (DSM) es una aplicación que se centra en la reducción de los gastos de capital y en la entrega acelerada de servicios basados en DSL. Ofrece configuración de servicio, activación de servicio extremo a extremo, gestión de inventario y de manera opcional, gestión de orden plena. Con este producto se pueden ofrecer servicios basados en DSL a casas, escuelas y negocios.

2.2.2.7 GESTIÓN DE NODO

El sistema utiliza su propia interfaz de terminal de gestión de nodo (NMTI) para ejecutar la gestión del nodo. El NMTI, una interfaz de menú amigable en el equipo de acceso, se usa para configurar, administrar y monitorear el sistema.

Los parámetros y funciones configurados son almacenados en una base de datos en la tarjeta control-2. Esta gestión puede iniciarse desde un terminal de gestión de nodo o desde un sistema de gestión de red.

Un terminal ASCII (VT100) o una PC donde se corra el “software” correspondiente, pueden ser usados para la gestión. El terminal se conecta al nodo a través de uno de sus dos puertos serie:

SP1: Es un puerto DB-25 (CCIP), el cual automáticamente se conecta a la tarjeta de control.

SP2: Es un puerto RJ-45 ubicado en la tarjeta control-2 activa.

2.2.2.8 GESTIÓN DE RED

El 5620, se conecta a través de un puerto CCIP Ethernet ó un “cell relay”, provee acceso a la gestión de nodo, además de una avanzada GUI (Interfaz gráfica de usuario) para gestionar todos los nodos en la red y configurar los enlaces. Utiliza el protocolo CPSS (control packet switching system), propietario de Alcatel para administrar los nodos y recibir información desde ellos.

Los mensajes CPSS viajan sobre los enlaces físicos entre los nodos y el sistema de gestión de red. Sus parámetros se configuran a través de una sesión de gestión de nodo. Estos mensajes portan la siguiente información:

1. De control, la cual permite al sistema de gestión enviar comandos a los nodos.
2. De estadística, a través de la cual, el sistema obtiene información de monitoreo.
3. De alarma, la cual permite tener la información de diagnóstico.
4. Del diagnóstico de configuración desde los nodos.

Estos mensajes viajan de la estación de trabajo MainstreetXpress 5620 activa a la de respaldo y a cada sistema de enlaces CPSS (dentro y fuera de banda) [38].

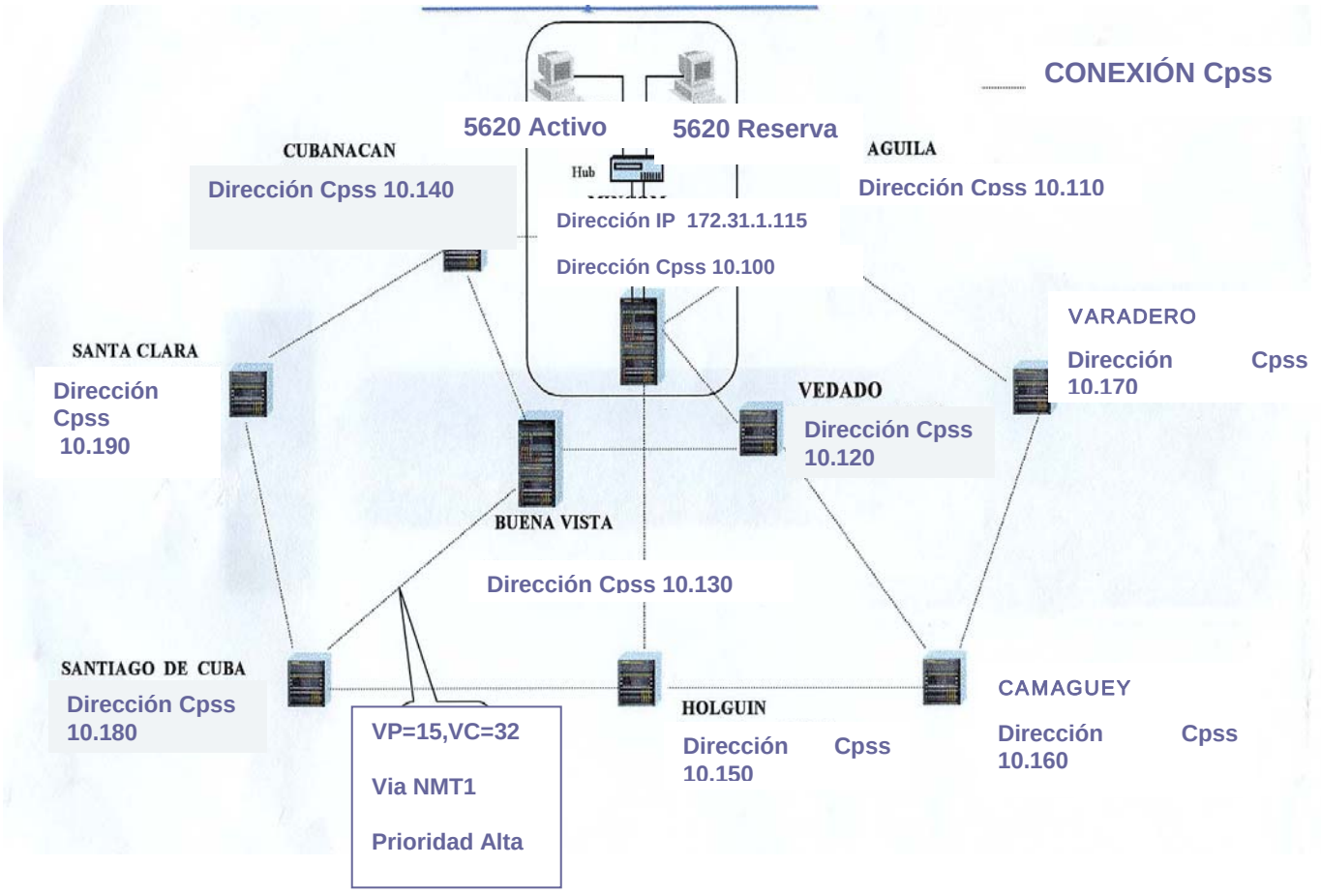


Figura 10. Red Cpss 36170, CUBADATA, ETECSA

Aparte de las estaciones activa y de respaldo, existen estaciones delegadas, las cuales no pueden agregar o quitar usuarios, pero sí encuestar a los nodos para obtener el estado de los mismos.

Este sistema 5620 NM permite la partición de la red, mediante la cual, redes físicas pueden ser lógica ó físicamente subdivididas, para un control y monitoreo simultáneo, por diferentes clientes, los cuales solo ven sus propias redes privadas virtuales (VPN). Una partición contiene todos los recursos de red que un operador es responsable de administrar. Las particiones pueden separar la red “backbone” en segmentos y de esta manera un operador puede controlar nodos en un área geográfica específica u otras estructuras de gestión.

Las particiones traen ventajas a los portadores y a los usuarios finales. Para satisfacer a ambos, Alcatel ofrece dos tipos de particiones, la partición “backbone” virtual y la de red de servicio virtual. [38]

Cada nodo tiene una dirección CPSS única, la cual contiene un número de dominio y uno de nodo, este último es único dentro del dominio.

Existen tres tipos de nodos CPSS:

- Enrutadores: Rutean tráfico a otros nodos dentro del dominio.
- Final (stub): Pueden terminar y originar tráfico CPSS, pero no pueden rutear. Estos nodos en la periferia (edge) de la red, aumentan el rendimiento de CPSS dentro de banda.
- Rama (leaf): Es un dispositivo de acceso que es un stub de un nodo enrutador CPSS.

Cada nodo enrutador conoce la topología CPSS de su propio dominio solamente y usa el camino de menor costo entre la fuente y el destinatario, cuando transmiten y reciben tráfico CPSS. El nodo final conoce solo al nodo ó los nodos con los que tiene una conexión activa.

Los nodos son ubicados en dominios para reducir la complejidad del ruteo CPSS y mejorar el rendimiento y la escalabilidad. Hasta 60 dominios pueden existir en una red, cada uno de los cuales puede tener hasta 50 nodos, de los cuales, no más de 30 pueden ser ruteadores. Cada dominio debe tener al menos un nodo ruteador (gateway), el cual se conecta a uno ó más sistemas de gestión. Para tolerancia de fallas, la red debe tener más de un “gateway”- en cada dominio. Cada nodo debe tener enlaces CPSS al menos con dos nodos más.

2.2.2.8.1 ENLACES Y CAMINOS CPSS

El 5620 ofrece una gestión sofisticada que proporciona un preciso control sobre el ancho de banda, mediante [38] la creación de enlaces IP, ATM, VPC, FR, ISDN, de acceso, ADPCM y de transporte, la creación de enlaces completos o fraccionados, el re-ruteo de enlaces demorados y a causa de problemas del enlace ó de los puertos, el control de ruteo y el ruteo y reruteo de enlaces cubiertos para eludir nodos en estado de ocupados ó fuera de servicio.

Esta gestión incluye la gestión de rutas de extremo a extremo, la agrupación de las mismas, su estado en tiempo real, la lista de las rutas configuradas y la protección de las rutas de alta prioridad.

Los enlaces CPSS se crean entre nodos del mismo dominio de ruteo y entre los nodos “gateway” y las estaciones de trabajo MainstreetXpress 5620 activa y de respaldo. El nodo ruteador soporta hasta 6 enlaces CPSS con otros nodos enrutadores, hasta 20 enlaces CPSS con otros nodos finales y hasta 5 enlaces CPSS con las estaciones activa y de respaldo, estaciones de red enrutadoras o colectores estáticos.

Pueden crearse enlaces CPSS redundantes entre los nodos, pero solo uno estará activo. Los valores máximos sostenidos de los enlaces CPSS sobre ATM, pueden configurarse desde un valor mínimo de 100 Kb/s hasta el valor término.

El 5620 utiliza el mapa para señalar los recursos que fueron considerados y los que no. El operador puede generar reportes de rutas para averiguar porqué el 5620 NM no utiliza ciertos objetos. Se usa el diagnóstico forzado de una reruta para conmutar de una ruta activa a otra alternativa.

2.2..2.8.2 PROTOCOLO DE GESTIÓN DE RED SIMPLE (SNMP)

El 5620 NM facilita la integración de dispositivos de distintos fabricantes. Con la capacidad que tiene el sistema para el control de gestión extendido, los operadores pueden reducir los costos y consolidar sus redes. Este sistema tiene un número reconocido de dispositivos administrados a través del protocolo simple de gestión de red SNMP (Simple Network Management Protocol), a través del módulo descriptor SNMP. Todos los valores del sistema se suministran a los elementos SNMP, incluyendo la gestión de caminos, estadísticas, gestión de fallas y aparecen en el mapa de la topología del 5620. El módulo SNMP está integrado con el 5620 NM para extender el poder de este último para la gestión de los dispositivos SNMP no Alcatel desde una simple GUI. Para la configuración, el 5620 NM provee una

gestión de elementos escalables y monitoreo de los dispositivos SNMP, tales como dispositivos de acceso y “routers” de Alcatel y de otros.

2.2.2.8.3 INTERFACES OSS

Los módulos de interfaz OSS CMIP y CORBA extienden las capacidades de administración a otros servicios de red y niveles de negocio OSS. Haciendo uso de ellos la gestión de red Alcatel permite al cliente OSS acceder a información gestionada por el 5620, tal como alarmas, inventarios e información de estados. También permite a cualquier OSS gestionar varios elementos dentro de una red.

Figura 11. Interoperabilidad de 5620

El 5620 NM es en el núcleo de la solución, quien direcciona la gestión del amplio rango de Redes privadas virtuales, tales como redes Ethernet, MPLS y Cell/FR.

Combinando el 5620 NM pre-integrado, con socios conectados a Alcatel, la red VPN Alcatel y las soluciones de gestión de servicio ofrecen grandes funcionalidades.

El simulador 5620 NM es un “software” de aplicación que luce y funciona exactamente como el 5620 NM, pero permite a los operadores de red simular y hacer pruebas a la red, sin usar recursos de ancho de banda, ni de equipos. Es útil para el entrenamiento de nuevos operadores, sin afectar las operaciones de la red y para el estudio de cambios en redes existentes.

El 5620 NM es hoy en día un sistema de gestión de red muy escalable, capaz de soportar hasta 10000 nodos ATM, 500000 dispositivos remotos, 1.5 000000 de rutas (una combinación de hasta 1000000 de PVCs e igual número de SPVCs), y 255

sesiones simultáneas de operadores, 1000000 de conexiones PVCs e igual número de SPVCs.

Este sistema de gestión es soportado por la última generación de las plataformas y servidores Sun Microsystems. Es soportado además por la “Sun SparcStation” y el multiprocesador Solaris. Otra característica incluye una arquitectura escalable y replicación de bases de datos para la sincronización del mantenimiento.

2.2.3 GESTION DEL NAP

El “software” de gestión a utilizar será el Ciscowork 2000 for windows [15], cuyas características principales se mencionan en el capitulo 1.

Cisco Works 2000 es un “conjunto de productos de gestión de redes de Cisco, y está compuesto por tres paquetes de “software”:

- RME (Cisco Resource Manager Essentials)
- CWSI (CiscoWorks for Switched Internetworks
- IPM Internetwork (Performance Monitor)

El RME está compuesto por varias áreas fundamentales, como son el administrador de inventario, el servicio de revisión de cambios, el área de configuración de dispositivos, la de “software”, la de disponibilidad, el analizador, el área encargada de la conexión de gestión de Cisco y las herramientas de servicio. El propósito fundamental de este paquete es proveer una serie de herramientas para el uso interno y externo. Incluye una base de datos SQL e interfaz Java. Posee una serie de vistas para el monitoreo y también para reportar las incidencias en la base de datos. También tiene pequeñas tareas relacionadas con la seguridad. [27].

CWSI es una herramienta de hallazgo y mapeo, compuesta por la herramienta de mapeo, el Ciscoview, los directores VLAN, ATM, y el de tráfico, además del rastreo de usuarios [27].

El IPM permite acceder fácilmente al RTR (reportero de tiempos de respuesta). De esta manera, IPM puede determinar y reportar los caminos usados entre dispositivos y ofrece los tiempos de respuesta para cada uno de los saltos, en cada camino. También mide el

desempeño de las sesiones IP, colecciona estos datos, provee información acerca de la tendencia actual y envía “traps” SNMP si los umbrales son violados.

Se usan específicamente para este propósito en el NAP, un “router” Cisco 2620, que da la posibilidad de gestionar de manera remota, dos “firewalls” Cisco Pix 515-E, y dos “switches” Cisco Catalyst 2950. El “software” se instala en los servidores.

En el centro de gestión, ubicado en el MINCOM, se instalarán tres estaciones de trabajo, las cuales serán conectadas a tres puertas Ethernet de uno de los “switches” 2950, usando cable UTP, categoría 5, para el monitoreo.

2.2.4 RED DE INFOCOM

Hasta ahora no se encuentra gestionada centralizadamente.

2.2.5 REDES DE TERCEROS

No se administran estos equipos de manera centralizada en nuestra red.

3. CONCLUSIONES

De manera general los conmutadores con los que se cuenta en las redes de ETECSA son gestionados.

La red CUBADATA, como se pudo apreciar, tiene gestionados sus conmutadores, aunque usando sistemas de gestión independientes, pues el sistema que gestiona los equipos Newbridge, a pesar de poseer un descriptor SNMP para integrar equipamiento de diferentes fabricantes, no comprende los X.25 de Alcatel, e integrar estas gestiones en este momento es muy costoso, y requiere de una solución para un equipamiento que ya no es fabricado por Alcatel.

El descriptor SNMP del 5620 NM comprende a los equipos de Cisco, por lo que estos podrían haber sido gestionados también mediante este sistema. Sin embargo, para administrar los equipos del NAP se decidió usar el Ciscoworks 2000, “software” que solo puede usarse para gestionar equipos Cisco.

Estas soluciones de gestión por separado encarecen el sistema, por lo que aunque no ha sido la tendencia por razones de política de Empresa hasta este momento, debía pensarse

en la reunificación de sistemas de gestión de nuestras redes de datos, cuestión, que sabemos es difícil, pero que merita un estudio.

Infocom ó Enet es una unidad de negocio dentro de ETECSA, y su tendencia ha sido la independización. Se podría integrar el “software” Ciscoworks for Windows, utilizado para gestionar los equipos del NAP, sobre la plataforma HP Openview y de esta manera gestionar también el equipamiento de Infocom, compuesto, como ya dijimos, en su mayoría, por equipos de Cisco.

Mientras esto se determina, podríamos dar un paso a favor de la integración, proponiendo la implementación de un sistema de gestión para los modems Telindus que se usan en nuestras Redes de ETECSA para acceder a los usuarios. El “software” es el TMA (Telindus Maintenance Application), una solución propietaria de Telindus, para la gestión de sus equipos.

CAPITULO 3: PROPUESTA DE SISTEMA DE GESTION PARA REDES DE TRANSMISIÓN DE DATOS DE ETECSA.

1. INTRODUCCIÓN

Como hemos comentado en varias oportunidades a lo largo de este documento, la Red de Transmisión de Datos de ETECSA solo gestiona de manera centralizada, los conmutadores de las Redes CUBADATA y dentro de poco tiempo, el equipamiento Cisco del NAP.

En el capítulo anterior pudimos apreciar que existe gran diversidad en la gestión de las redes con las que cuenta ETECSA en este momento. CUBADATA posee dos sistemas de gestión independientes y el NAP, el suyo propio, y esta heterogeneidad hace difícil la integración de la gestión, cuyo detalle se va más allá de este trabajo, pues se necesita hacer un profundo análisis y de esta manera proponer las herramientas necesarias.

La plataforma Openview de HEWLETT-PACKARD es una potente herramienta para la gestión de equipos de diversos fabricantes [22], ventaja que debe usarse para integrar paulatinamente la administración de la Red de Transmisión de Datos de ETECSA. Esta plataforma usa como protocolo estándar, el SNMP, particularidad que le permite la interconexión con otros equipos que también posean esta característica.

El 7270 ó 7470 de la red X.25/FR posee interfaz local y remota para la gestión a través del 5620 y SNMP. Para el soporte SNMP consta de:

- MIB II según RFC 1213
- Interface table MIB según RFC 1573
- SONET MIB según RFC 1595
- DS3/E3 MIB según RFC 1407
- ATM interfaces MIB según RFC 1695
- ILMI MIB según ATM Forum UNI v.3.1
- Enterprise MIB para PVC y S-PVC setup
- Servicios Frame relay MIB

- Call routing statistics MIB
- OSPF MIB
- MPLS statistics MIB

También posee el 7670 de ATM/FR soporte SNMP, lo cual pudiera servir para la integración con otros fabricantes. Este detalle ofrece la posibilidad futura de estudiar la integración de los equipos de la red CUBADATA ATM/FR a la plataforma HP Openview, por ejemplo.

En cuanto a Infocom, como ya se mencionó, pudiera usarse también el Ciscoworks 2000 que gestiona los equipos del NAP e integrar los dos en un sistema único, a administrar desde el MINCOM, pudiendo ser montados sobre el HP Openview.

La compleja estructura de la red de ETECSA, dada por su extensión y diversidad tecnológica, hace difícil encontrar una solución integral para la gestión de la red. Esta sería una tarea de una complejidad tal que rebasa los marcos de nuestro trabajo. En cambio proponemos un acercamiento paulatino que siga las pautas antes descritas. En tal sentido, y como trabajo de inicio hacia este acercamiento progresivo a una solución integral de gestión, dedicaremos el resto de este capitulo a una propuesta para la gestión de una parte esencial de la red de transmisión de datos. Nos referimos a la red de acceso compuesta por equipos Telindus, usados en Cubadata e Infocom.

2. DESARROLLO

2.1MODEMS TELINDUS

Uno de los modems más usados en nuestras redes, como se ha podido apreciar es el Telindus ó Crocus, de procedencia Belga. El grupo Telindus tiene alrededor de 30 subsidiarias en varios países europeos y una amplia red de agentes en prácticamente toda Europa, Sudeste de Asia, América del Sur, África y el Medio Oriente. Su base de clientes incluye a más de 50 operadores y un amplio espectro que abarca instituciones gubernamentales y financieras. Asimismo, la compañía cuenta con prestigiosas referencias en el sector de la industria, la distribución y los medios.

En nuestras redes se usan: el modem HDSL, el HS y el SDSL, este último en fase de prueba actualmente. En el lado de la central se usan generalmente bastidores de 19” (CN4) (ver figura 1 del anexo, capitulo 3), con capacidad para albergar hasta 15 tarjetas.

En el de usuario, de manera general se utilizan modems de mesa (stand alone). Figura 2 del anexo.

2.1.1 MODEM BANDA BASE HDSL.

El modem banda base HDSL opera a velocidades de hasta 2 Mbps sobre dos pares dedicados a distancias de hasta 7.6 Km, sin necesidad de repetidores. El mismo ha sido diseñado especialmente para conexiones LAN-to-LAN, interconexión de PABX, transmisión de video y otras aplicaciones que demanden altos anchos de banda.

Una de las capacidades incluidas en el Crocus HDSL permite, ante el corte de uno de los pares, la operación sobre sólo un par telefónico a la velocidad de 1 Mbps, conservando la mitad de los canales activos (G704 canalizado), con el objetivo de ofrecer continuidad de operación al cliente final. Las interfaces DTE son completamente modulares al modem, encontrándose disponibles interfaces del tipo V.36, V.35, X.21, G703 y bridge para redes de área local (LAN).
Este tipo de Modem permite la administración centralizada, a través de la cual se pueden configurar equipos remotos, obtener el estado actual de los enlaces o monitorear en tiempo real la calidad del mismo, con el objetivo de reportar alarmas, informes y análisis de fallas al operador. Posee modulación de línea del tipo 2B1Q, con un nivel de transmisión de 13 dBm de acuerdo con la norma ETSI DTR/TM 3017.

2.1.2 MODEM HS.

Otro tipo de modem muy usado en nuestras redes es el Crocus HS, el cual representa una nueva generación de modems administrables banda base de alta velocidad para líneas de cobre de subscriptor o líneas privadas. El modem opera a velocidades desde 48 Kbps a 144 Kbps sobre un par (2 hilos) dedicados a distancias de hasta 9 Km. Mediante la inclusión de ecualización de línea automática en conjunto con la modulación 2B1Q, es posible cubrir grandes distancias sin la necesidad de utilizar repetidores o líneas acondicionadas. Al igual que el modem HDSL, este equipo dispone de una gran variedad de interfaces DTE modulares.

Este tipo de modem HS de Telindus incorpora administración centralizada vía un canal secundario, el cual transmite la información entre equipos de forma rápida y segura. La administración puede ser integrada completamente al sistema HP Openview (M.R). El modem HS también dispone de indicadores luminosos de estado en el panel frontal, así

como de pruebas de DTE y líneas, tanto locales como remotas.

2.1.3 MODEMS SDSL

Los modems del tipo SDSL se han incorporado a nuestras redes, y aunque no están muy difundidos aún en las mismas, ya se encuentran dando servicio a modo de prueba en algunos nodos de la capital.

Estas tarjetas también pueden ser instaladas en “subracks” de 19” ó en versiones de buró en un “shelf”, con capacidad para cuatro tarjetas (figura 3 del anexo, capitulo 3). En cualquiera de los casos pueden combinarse con otro tipo de tarjetas como lo son: HDSL, FO10M, etc., proporcionando soluciones universales de acceso. Los “shelfs” son diseñados para tener alimentación redundante y para alimentarse lo mismo con –48 V DC ó 115/230 VAC.

Cada tarjeta de modems porta 4 interfaces conectados a 4 usuarios diferentes a través de pares trenzados de cobre. Cada enlace puede ser configurado para operar a velocidades múltiplos de 64 Kbit/s, hasta 1152. El tráfico de datos de los usuarios es incorporado a una trama E1 en una interfaz G.703. La asignación de los “time slots” es completamente controlada por el operador. Más de 4 usuarios pueden ser acomodados en una trama E1, para esto pueden “cascadearse” diferentes tarjetas.

Dos interfaces E1 canalizadas permiten concentrar usuarios de alta velocidad cuando la velocidad requerida es mayor que la de un E1.

Además de la conexión de usuarios remotos, la interfaz Nx64 Kbit/s permite la conexión simultánea de usuarios locales, los cuales deben conectarse a una velocidad múltiplo de 64 Kbit/s e interfaces X.21, V.35, V.36, RS-530, V.24 o Ethernet 10 Base-T.

Estos equipos pueden ser administrados, para lo cual se implementa un sistema de gestión, propietario de Telindus: TMA for HP Openview.

2.2 HERRAMIENTAS NECESARIAS PARA LA GESTIÓN DE EQUIPOS TELINDUS

2.2.1 PRODUCTOS DE TELINDUS

Debido a la evolución continua en el dominio de la tecnología de comunicación de datos, los dispositivos se vuelven cada día más complejos de instalar y controlar. Esto trae consigo la necesidad de tener herramientas sencillas de mantenimiento. Telindus ofrece productos como el TMA, TMA CLI, TMA for HP OpenView ®, Orchid 1003 LAN y Orchid DM, haciendo uso de protocolos como CMS2 y CMS: (propietarios de Telindus), SNMP, Telnet, ping, TFTP(Trivial File Transfer Protocol) y encapsulamiento IP, MAC, X.25, Frame Relay y PPP sobre otros protocolos.

2.2.1.1 TMA

El TMA (Telindus Maintenance Application) es una herramienta de gestión que ofrece un completo control sobre cualquier dispositivo Telindus existente en la red, por supuesto, con la ayuda de una máquina computadora. Los rasgos más importantes de TMA son:

- la conexión directa al dispositivo vía su puerto de control
- la conexión remota a la red o protección con contraseña, para el acceso al dispositivo
- lectura y cambio de la configuración del dispositivo
- puede guardarse la configuración de los dispositivos en el disco duro, para ser reusada
- información de calidad y alarmas actualizadas
- monitoreo en tiempo real de los circuitos de intercambio (RS-530, V.35, V.36, X.21, G.703, etc.)
- monitoreo en tiempo real de los parámetros de línea del módem
- la ejecución de pruebas de diagnóstico

- descarga de software al dispositivo

Necesita de requisitos mínimos del sistema para lograr una instalación exitosa. En cuanto a sistema Operativo, puede correr sobre Microsoft ® Windows 95 ®, Microsoft ® Windows 98 ®, Microsoft ® WINDOWS NT ® 4.0 y Microsoft ® Windows 2000 ®. Como dispositivo de entrada de datos pueden utilizarse: discos de 3 ½, torres de CD ROM ó el acceso a Internet, necesitando un espacio libre en disco de 4 MB sin los ficheros de modelos y 25 MB con ellos. Necesita un promedio total de RAM de 16 MB para Windows 95/98 ®, 32 MB para WINDOWS NT ® 4.0 y 64 MB para Windows 2000 ®.

Cada dispositivo de Telindus tiene su modelo. Este archivo contiene la información que el TMA necesita para conectar el dispositivo e intercambiar información con el mismo. Los ficheros se instalan separadamente de la aplicación, debido a que los modelos evolucionan a la par del dispositivo. Los modelos entregados con el dispositivo corresponden con el último "firmware" o "software" del mismo. Esto significa que si se agregan dispositivos a la red que contiene un "software" más reciente que los dispositivos actuales, entonces los modelos tienen que ser re-instalados. Los modelos más recientes soportan todos sus anteriores. Para la instalación ver sección 7 de [37].

Una vez la aplicación de TMA y los modelos de archivos se instalan, se está listo para interconectar la computadora con su TMA a un dispositivo de Telindus. Existen varios tipos de conexiones entre la computadora y los distintos dispositivos [37], secciones 23, 24 y 25, el uso de las cuales dependen del tipo de red y sus dimensiones. No necesita de la ORCHID, aunque su uso permite la conexión con todos los elementos de red, sin intercambiar cables.

2.2.1.2 TMA CLI

TMA CLI (Telindus Management Application Command Line Interface) es una interfaz ASCII que permite escribir los códigos personalizados con todas las posibilidades desde la aplicación de TMA interactiva. Ejecutando estos códigos en el modo background, algunas tareas de gestión pueden automatizarse. Por ejemplo, si se quiere mantener el registro del BER de los modems de una red en una base de datos diaria, se imprime una escritura para recolectar los valores de BER. Estos valores pueden añadirse a un archivo en el disco y los resultados se trabajan para dar la información estadística global finalmente. Esto puede ser presentado gráficamente,

usando herramientas estándares. TMA CLI usa la misma sintaxis de la interfaz de usuario Telnet CLI.

2.2.1.3 TMA FOR HP OPENVIEW

La solución que ofrece Telindus para administrar sus módem de una manera integrada, con la posibilidad de otros equipos en la red está basada en la plataforma de HP OpenView®. Esta será por su nivel de integración y escalabilidad, la que usaremos para la gestión de los equipos Telindus de ETECSA.

Esta aplicación colecciona las alarmas de las unidades de red, las registra en el HP Openview y las visualiza en los mapas de red. Las mismas pueden enmascararse y se les puede configurar un nivel de severidad, el cual es traducido por el HP Openview a través de códigos de colores.

Al observar una red administrada, pueden distinguirse tres tipos de equipos:

- El equipo administrado (el elemento de la Red): Éste es el equipo real que el operador quiere administrar. En el caso de una red de módems, éste es por ejemplo un Módem banda base Crocus.

- El sistema de administración de Red: Éste es el equipo con su software propietario, constituido por:

    1. Una plataforma del hardware con su Sistema operativo. La solución de Telindus se ofrece en Windows NT® y SOL Solaris®.

    2. Una aplicación de plataforma de administración: Una aplicación abierta que soporta los requisitos previos de dirección básicos para un número grande de aplicaciones de dirección específicas. La solución de Telindus se ofrece en el HP OpenView®.

    3. Un módulo específico (PSM): Una aplicación específica (generalmente entregada por el vendedor del equipo administrado) corre en la plataforma de administración, ofrece funciones específicas de administración para el equipo administrado. La solución de Telindus aquí es TMA para HP OpenView®.

- El dispositivo concentrador o de mediación, llamado ORCHID 1003 LAN, al cual nos referiremos más adelante.

TMA for HP OpenView está compuesto por dos bloques fundamentales:

- El TMA
- El administrador de alarmas

El TMA es una interfaz de usuario gráfica que permite al usuario administrar los dispositivos Telindus, se accede a los atributos de configuración y se tiene información del estado, desempeño y de las alarmas [37].

A causa de que el HP OpenView no maneja dispositivos No-IP y el mecanismo para el manejo de dispositivos No-IP (usando traps SNMP) no es óptimo, se creó el administrador de Alarmas, como parte de TMA para HP OpenView[37], capítulo 7.

Los requisitos del sistema en cuanto a memoria DRAM son de al menos 256 M para 2500 nodos. Lo ideal son 512 M y 800 disponibles en disco.

2.2.1.3.1 FUNCIONES DE ADMINISTRACIÓN

Al integrar TMA para HP OpenView® se integra con un nodo de administración HP OpenView®, los módems se representan en el mapa de OpenView® a través de íconos. Hacer doble clic en el ícono, permite al usuario acceder a las funciones de administración del módem seleccionado. Se reportan las alarmas en el registro de Eventos del nodo administrador del Nodo y puede cambiar el color de los mismos en el mapa HP OpenView®.

2.2.1.3.2 FUNCIONALIDAD DEL HP OPENVIEW®

2.2.1.3.2.1 TIEMPO REAL DE VISUALIZACIÓN DE STATUS DE RED

El estado de la red se refleja instantáneamente para el operador de la red. Por esta razón, el operador tiene una vista jerárquica de la misma. Pueden estructurarse las vistas geográficamente (los sitios diferentes, los locales diferentes, etc.), y también funcionalmente (módems de 64 Kbps, Nx64kbps), etc.

Siempre que un problema se detecte en la red (por ejemplo una calidad de la línea mala, una línea abierta, un problema de la aplicación), el operador es informado por una alarma para un equipo en particular. Cada condición puede atribuirse individualmente a una prioridad definida (existen 4 [37]). De esta manera, el operador puede hacer la distinción entre la severidad de condiciones diferentes y puede ejecutar las acciones necesarias en el orden correcto.

Cada alarma se refleja en un evento y se procesa más adelante.

2.2.1.3.2.2 SEGURIDAD DE ACCESO

El acceso al sistema de administración se asegura a través del registro del usuario en la estación de gestión de red (UNIX o Windows NT®).

2.2.1.3.2.2.1 SEGURIDAD DEL ADMINISTRADOR DE ALARMAS

Se puede definir una lista de contraseñas con diferentes niveles de acceso para proteger al administrador de alarmas, de intentos de acceso de personal no autorizado. Los atributos de seguridad contienen los siguientes elementos:

- La contraseña**:** que no más que una cadena de un máximo de 10 caracteres
- El **derecho de acceso:** que es un atributo que representa los niveles de acceso asignados a una contraseña y es una cadena de bits, donde cada uno de ellos corresponde un nivel de acceso (1111, por ejemplo).

Readaccess ‘on’ permite leer todos los atributos, excepto los elementos de seguridad. Writeaccess ‘on’ permite cambiar todos los atributos, excepto los de seguridad, además estos atributos no pueden ser leídos. Security access ‘on’ permite leer y cambiar los atributos de seguridad. EL TMA for HP Openview tiene como atributo de seguridad el alarmman/security. FileSystem Access se usa con propósitos futuros.

Si no se crean contraseñas, todos tienen total acceso al sistema. Si se define al menos una contraseña es imposible acceder al administrador de alarmas con el TMA, si no se entra la contraseña correcta, pero si se crea una lista, al menos una debe tener acceso de escritura y seguridad, sino no se podrán hacer

cambios de contraseña y configuración después de activar la nueva configuración.

2.2.1.3.2.3 ADMINISTRACIÓN DISTRIBUIDA

En grandes redes, los administradores pueden aligerar los cambios de configuraciones. Típicamente en una red de modems solo existe un número limitado de configuraciones. En lugar de enviar las configuraciones por separado, se puede enviar la misma a la ORCHID y ella se encarga de enviarla a las unidades, lo cual es más eficiente en términos de ancho de banda y tiempo de consumo. Para tal propósito la ORCHID tiene un sistema de ficheros en su memoria Flash. Una vez que las configuraciones están almacenadas en la ORCHID, la misma se configura para distribuir las configuraciones a las diferentes unidades de red, presentes en la red ó futuras a instalar.

Las capacidades de gestión distribuidas de HP OpenView® permiten separar la red en varias secciones. Cada sección puede tener su propia estación HPOpenView® (no es nuestro caso). Parte de la información recolectada puede enviarse a las estaciones de gestión (estaciones sombrilla). La Topología y filtros del mapa permiten la personalización del modelo de gestión distribuida por:

- Dispositivos específicos que son administrados por una estación recolectora en particular
- Información diseñada para ser enviada desde las estaciones recolectoras hasta las de administración
- Objetos específicos para ser vistos en el mapa

2.2.1.3.2.4 FUNCIONALIDAD PARA TMA FOR HP OPENVIEW®

TMA for HP OpenView® ofrece las siguientes características:

- Lectura y cambio de la configuración del modem
- Monitoreo en tiempo real de ITU-T V.24, V.35, V.36, RS530, “Bridge”, “Router” o circuitos de intercambio G.703.

- Monitoreo en tiempo real de los parámetros de línea.
- Recuperación del estado de la información (el funcionamiento actual) del módem y el puerto DTE , incluso el estado de la Alarma actual
- Recuperación de la información estadística del módem, los parámetros del puerto DTE y la capa de enlace como valores absolutos, valores durante 15 minutos, durante las últimas 2 horas y valores por 2 horas durante las últimas 24 horas.
- Pruebas de diagnóstico (lazo 3, lazo local 2, lazo remoto 2 y conteo de errores).
- El almacenamiento de la configuración y estadísticas y recuperación en el disco duro
- Pantallas interactivas que reflejan el equipo y el estado de los indicadores.
- El enmascaramiento de alarmas es configurable por cada módem
- Se envían las alarmas a los eventos del HP OpenView® . A cada alarma puede asociársele un código de color en el mapa del HP OpenView®.
- Descarga “flash” del software.

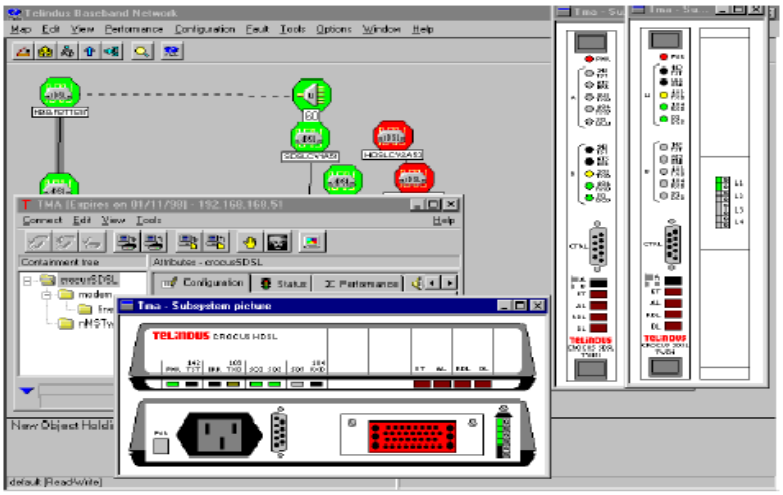


Figura 1 Aplicación TMA con pantalla interactiva

2.2.1.3.2.5 INSTALACIÓN DE TMA FOR HP OPENVIEW

Para la instalación del sistema sobre Windows 2000 ó NT debe reiniciarse el sistema, aunque no lo pida la propia instalación, sino la misma será incorrecta:

1. Antes de la instalación hay que asegurarse de que todos los servicios relacionados no estén en funcionamiento. En la barra de tareas, seleccionar Start/ Programs! HP OpenView ! Network Node Manager/Admin ! NNM Services – Stop.

2. Insertar el disco de instalación en la torre CD-ROM.

3. Windows automáticamente comenzará a correr el TMA, si no, se selecciona en la barra de tareas Start ! Settings ! Control Panel ! y se hace doble “click” en Add/Remove Programs ! Install…

4. El ”InstallShield ® Wizard” ayuda en el proceso estructuración.

5. En un momento, se tendrá la siguiente pantalla:

En este instante se instala el ejecutable de TMA y los ficheros modelos ó la clave de licencia.

6. El InstallShield ® Wizard guía a lo largo del proceso de estructuración

Antes de correr el sistema es necesario hacer ciertas configuraciones del HP Openview y Windows [37].

La instalación de los ficheros modelos debe hacerse independientemente de la instalación del TMA ejecutable, debido a que estos últimos evolucionan a medida que lo hacen los dispositivos. Los ficheros que se encuentran en el CD-ROM son la última versión existente cuando se creó el dispositivo y si se añaden dispositivos con una versión más reciente, se requiere una re-instalación de los ficheros [37].

2.2.1.3.2.6 INTERCONEXIÓN CON OTROS EQUIPOS

TMA para HP OpenView® puede usarse con otra aplicación para NNM 5.0X sobre una de las plataformas de hardware, antes mencionadas. Por ejemplo, una red SDH con nodos de un vendedor y módems Crocus. Los mapas de red HP OpenView® contienen iconos para los nodos e iconos para los módems Crocus. Se puede configurar dentro de HP OpenView® por tipo de dispositivo, que las alarmas cambien el color del ícono. Haciendo doble “click” en el icono del nodo SDH empieza la aplicación para este dispositivo, y haciendo doble “click” en el icono del Crocus, comienza la aplicación de TMA.

Un menú amigable con el usuario permite la configuración de cualquier elemento individual de la red, así como también, distribuir la misma configuración a otros elementos. Cuando se activa la consistencia de configuración, la administración

mantiene las configuraciones de los elementos de la red completamente consistentes con archivos de configuración almacenados centralmente, inclusive cuando un elemento de la red es reemplazado. Similar consistencia de código permite mantener al código Flash consistente con versiones "software" almacenadas centralmente.

Todos los equipos Telindus están soportados por un MIB SNMP privado, ideal para el monitoreo del rendimiento, basado en la configuración de diferentes parámetros (por ejemplo: niveles de ruido, atenuación de línea). La plataforma HP OpenView® ofrece la representación de estos resultados configurados en forma de gráficos. TMA para HP OpenView se integra en forma homogénea con otros módulos de administración, haciendo posible la integración de la administración de los módems Telindus y del "router", por ejemplo, en la misma plataforma, cuestión que puede ser aprovechada para la gestión futura de los “routers” de Infocom.

TMA para HP OpenView utiliza conectividad TCP/IP para direccionar el equipo Telindus. Cada elemento de la red es identificado por el sistema de administración mediante su dirección IP. Algunas unidades (como el Crocus Inverse Multiplexer) cuentan con un puerto Ethernet directo, mientras que otras unidades (como el Aster y la gama de módems Crocus) son conectados a un dispositivo controlador (Orchid 1003 LAN), el cual actúa como un proxy SNMP. Sólo el equipo instalado centralmente es conectado al Orchid 1003 LAN. Para dar acceso de administración a los equipos remotos se utiliza un canal auxiliar de banda externa en el vínculo del módem. Asimismo, es posible generar configuraciones más complejas como la gestión sobre vínculos extendidos.

En el caso de la administración a través de un Orchid 1003 LAN, este controlador puede encapsular el tráfico de administración IP directamente en SVCs X.25. Esto permite el transporte de la información de administración sobre un “backbone” que re-enruta los paquetes, sin la necesidad de una red cubierta. Otros protocolos de transporte tales como Frame Relay y PPP estarán disponibles como una actualización de memoria Flash para el Orchid 1003 LAN.

TMA para HP OpenView auto-descubre rápidamente todos los elementos de la red definidos sobre la Orchid 1003 LAN. En el mapa, los elementos de la red mantienen el nombre que les hubiese sido asignado en la Orchid.

2.2.1.3.2.7 DIRECCIONAMIENTO EN TMA FOR HP OPENVIEW

Existen diferentes tipos de dispositivos:

Los IP: Son dispositivos en los cuales se puede configurar una dirección IP y tienen un puerto dedicado LAN, a través del cual el dispositivo se conecta a la red LAN. Ejemplo de esto son: la ORCHID 1003 LAN, el multiplexor Crocus Inverse y el “Router” Crocus 2M

Los No-IP: Son dispositivos en los cuales no se puede configurar una dirección IP y por tanto no tiene un puerto dedicado para este propósito, ejemplos de estos dispositivos lo constituyen el modem Crocus SDSL banda F, el Aster 4 F, el HDSL F

Los “proxiados”: Son dispositivos No-IP, en los cuales no se puede asignar una dirección IP, pero al que se le otorga una, utilizando la ORCHID 1003 LAN como proxy IP, también llamado Agente proxy [37], sección 3.2.

En nuestro caso, nos interesan fundamentalmente, la ORCHID 1003 LAN, que es un dispositivo IP y los modems Crocus, que vienen siendo dispositivos “proxiados” a través de la ORCHID.

2.2.3 ORCHID 1003 LAN

La ORCHID 1003 LAN es un dispositivo de mediación dedicado a coleccionar la información de administración del equipo administrado (los módems), y pasarla al sistema de dirección de red [37]. Físicamente se sitúa entre las unidades de red y las aplicaciones NMS

Algunas de sus características fundamentales son:

- Concentración de información de administración y alarmas de la red en una aplicación de administración.
- Encuesta a las unidades de la red.
- Encapsulamiento de protocolos: MAC, X.25, Frame Relay y PPP.

- Proxy TCP/IP: Puede usarse los protocolos Telnet y SNMP para obtener y enviar información desde/hacia las unidades de red. Responde a las solicitudes de ping.

- Consistencia de la configuración: Esta puede ser almacenada en la memoria flash de la tarjeta. Si la configuración de una de las unidades difiere de la versión almacenada la ORCHID descarga la configuración almacenada a la unidad de red.

- Consistencia del ”software”: El “software”, también llamado “firmware” de las unidades de red puede ser almacenado en la memoria flash de la tarjeta, si el “software” de una de las unidades difiere de la versión almacenada, la ORCHID descarga el “firmware” a la unidad de red.

- Ruteador IP entre sus puertos.

Las encuestas del sistema de dirección son enrutadas hacia los elementos de la red y las respuestas se envían hacia atrás. Este dispositivo existe en dos modelos, uno de mesa (Orchid 1003 LAN TT) y uno de tarjeta para el CN4 (Orchid 1003 LAN CV). Este último será el usado en nuestra red.

El número de unidades de red que la ORCHID puede concentrar depende del protocolo escogido y de la topología de la red, sin embargo, de manera general puede concentrar más de 250 unidades de red. No hay límite en el número de las ORCHID en las redes.

La ORCHID 1003 LAN identifica cada elemento de red a través de sus puertos de salida y de la dirección NMS.

Consta de diferentes puertos, cuya denominación y usos se detallan en las tablas 3.2.2.3.1 del anexo.

Dos tipos de conexiones existen entre la Orchid 1003 LAN y los elementos de red: las conexiones asíncronas de velocidad baja (por ejemplo 9.6 Kbit/s) entre la Orchid y el módem stand alone, o las conexiones síncronas de velocidad alta entre la Orchid 1003 LAN y el módem, versión de tarjeta, que se instala en el "subrack" CN4.

Es importante decir que no sólo los módems locales se administran, también se administran los remotos. Para ofrecer esta funcionalidad, un canal de administración de baja velocidad se transporta sobre el canal de comunicación, sin afectar los datos del

usuario. Este canal se usa por la Orchid 1003 LAN para la comunicación con los modems remotos.

Hasta 14 modems “Stand alone” pueden ser conectados a la ORCHID a través de un enlace asíncrono de baja velocidad (9.6 Kbit/s).

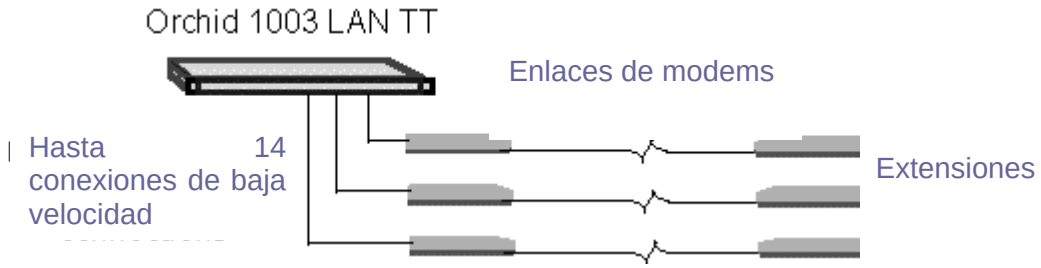


Figura 2.Gestión de modems stand alone locales y remotos

La conexión entre un "rack" de módems y la Orchid 1003 LAN se hace a través de un enlace de alta velocidad síncrono de 800 kbps. Hasta 7 tarjetas dobles pueden gestionarse con una Orchid 1003 LAN (versión de mesa). De nuevo pueden manejarse CV centrales y los módems remotos como se muestra:

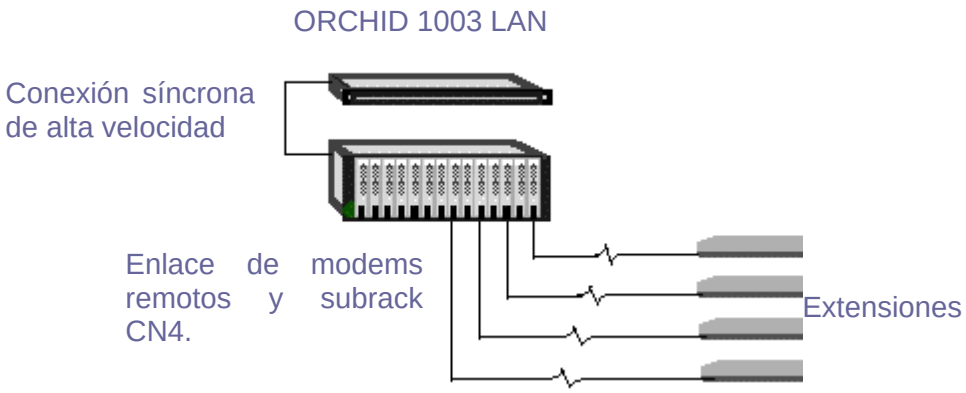
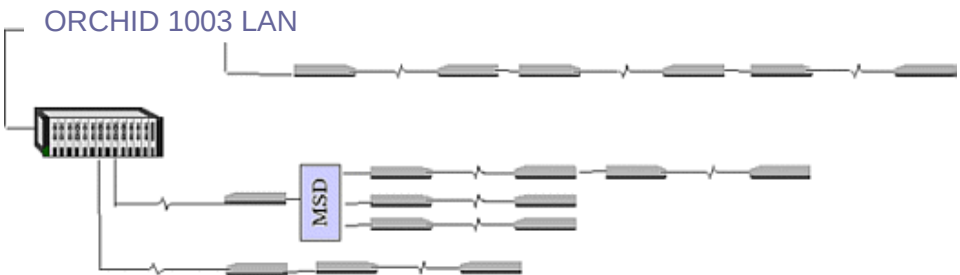


Figura 3 Gestión de modems en CN4, locales y remotos

En los sitios con un número limitado de módems, el costo de una Orchid 1003 LAN y su conexión al sistema de dirección central son demasiado altas. Por consiguiente, los enlaces y "multipoints" digitales extendidos en el nivel de dirección son posibles.



Enlaces extendidos

Figura 4.Gestión a través de enlaces extendidos

Los módems remotos pueden conectar su conector NMS vía un cable cruzado al conector NMS de otro módem. Alternativamente los módems remotos pueden conectar su conector NMS a un puerto de módem de dispositivo compartido (MSD). Los otros puertos MSD se conectan a los puertos NMS de otros modems en el lugar. El número de módems gestionados a partir de un módem central (al módem directamente o vía el bus de alta velocidad conectado a la Orchid1003 LAN) sólo está limitado por la velocidad del canal auxiliar del módem. Esta solución implica que solo una Orchid 1003 LAN se requiere en los sitios donde se usan modems de tarjetas, debido al bus de comunicación de alta velocidad existente entre las tarjetas y el concentrador. La Orchid 1003 LAN usa tráfico IP para comunicarse con el sistema de gestión central de red. Un puerto dedicado UDP se usa para encapsular el protocolo propietario de Telindus en IP. Se traducen las alarmas en los lazos SNMP por la Orchid 1003 LAN. Cada módem, así como cada Orchid 1003 LAN tiene una dirección IP que se define en el concentrador (Orchid). Este tráfico IP puede enviarse en la interfaz de Ethernet (encapsulamiento MAC) o en la interfaz del puerto serie A (Frame Relay, X.25 o encapsulamiento de PPP).

2.2.3.1 MODO DE DIRECIONAMIENTO

La ORCHID identifica cada elemento de red a través del “exit port” y de la dirección NMS. El “exit port”, dice si el elemento puede ser alcanzado a través de un bus de alta

velocidad ó un puerto asíncrono. En el caso de los modems de tarjeta, incluye la dirección del CN4, la posición de la tarjeta y el número de unidades en ella. La dirección NMS se usa para identificar el elemento de red cuando es conectada directamente a través del conector NMS a un elemento de red. Puede ser relativa ó absoluta:

- En el modo de direccionamiemto relativo, el modem de la central toma la dirección 0 y el remoto la 1. Si existen enlaces extendidos, el próximo elemento toma la dirección 2 y así sucesivamente. En este caso no se requiere de configuraciones

específicas por elemento de red. Su dirección depende de su posición relativa en la red. En la mayoría de las redes de modems se usa este tipo de direccionamiento

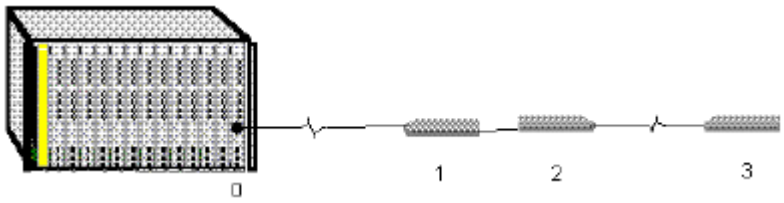


Figura 5 Direccionamiento relativo de modems

En el direccionamiento absoluto, cada elemento de red toma una única dirección NMS en el rango de 0 a 65535. La dirección es única para todos los elementos de red conectados a una ORCHID. Este tipo de direccionamiento permite usar el MSD, sin embargo la configuración es individual para cada elemento.

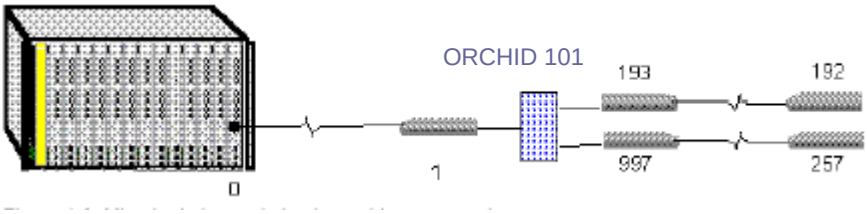


Figura 6 Direccionamiento absoluto de modems.

Por defecto, la ORCHID 1003 LAN utiliza el protocolo propietario CMS2 para comunicarse con las unidades de red, el cual permite buenos tiempos de respuesta sobre los canales auxiliares entre dos modems. Los nuevos dispositivos de Telindus trabajan con este protocolo, no así los anteriores, los cuales soportaban el CMS, aunque la ORCHID 1003 LAN convierte este protocolo anterior en CMS2. Unidades que usen protocolos diferentes pueden subsistir en una misma ORCHID, con la limitante de que para estar conectado a un mismo puerto sincrónico deben usar el mismo protocolo.

CMS2, SNMP, Telnet e ICMP son protocolos que pueden ser transportados sobre una red IP. En el caso de los protocolos estándar IP: SNMP, Telnet y ping, la ORCHID actúa como un proxy TCP /IP, pues es ella quien responde a estos protocolos en lugar de las propias unidades de red. La aplicación TMA utiliza el puerto UDP 1728 para encapsular paquetes CMS2 en paquetes UDP.

Constantemente están registrándose encuestas a los elementos de la red para ver si existen condiciones de alarma. Se remiten las condiciones de la alarma inmediatamente al sistema de dirección de red. Como mencionamos, la ORCHID soporta tipos diferentes de encapsulamiento IP: El encapsulamiento MAC sobre Ethernet y PPP, encapsulamiento X.25 y Frame Relay sobre líneas serie.

2.2.3.2 ENCAPSULAMIENTO DE PROTOCOLOS

2.2.3.2.1 ENCAPSULAMIENTO MAC

Si los sitios con la Orchid 1003 LANs ya están interconectados por una red IP, la Orchid puede enviar su tráfico al segmento Ethernet dónde se enruta hacia el sistema de gestión central:

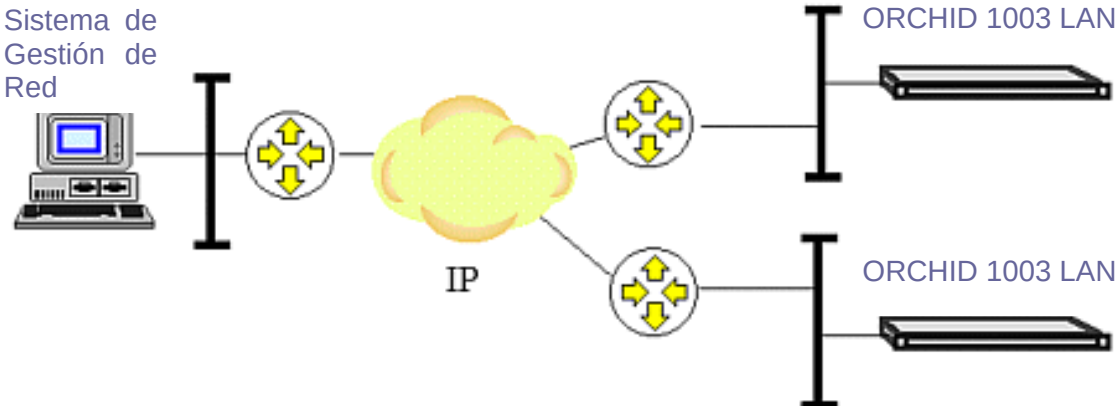


Figura 7. Gestión a través de una red IP.

2.2.3.2.2 ENCAPSULAMIENTO FRAME RELAY Y X.25

Si los sitios con la Orchid 1003 LAN son interconectados por una Red Frame Relay o X.25, la Orchid puede encapsular el tráfico IP en X.25 ó FR y enviarlo sobre el puerto serie A (V.24).

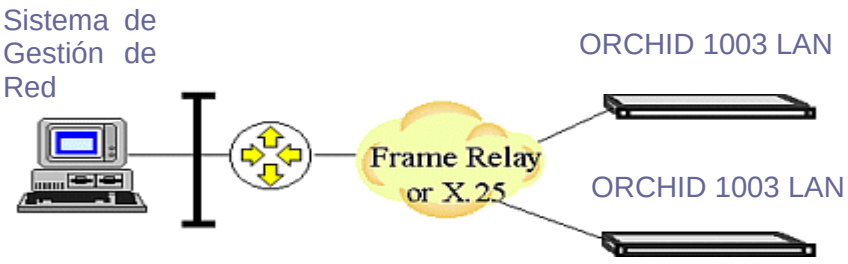


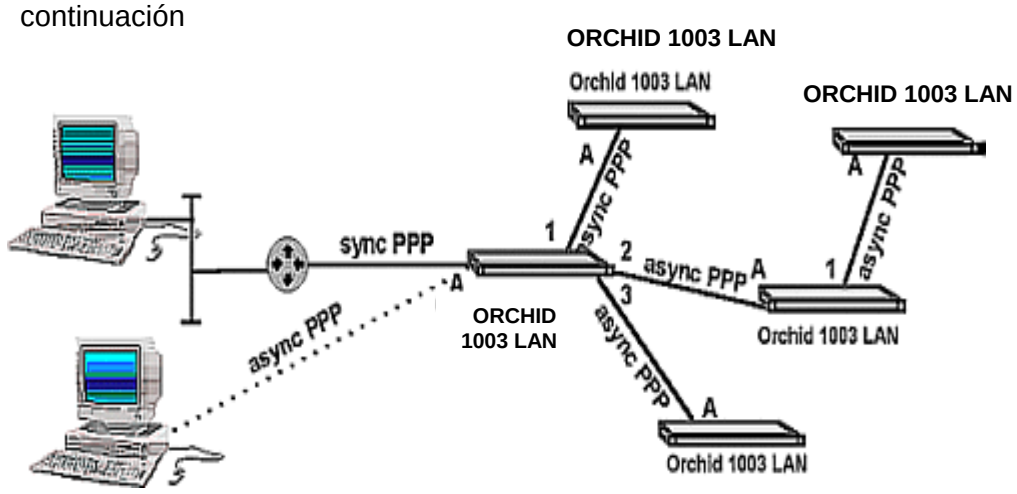
Figura 8. Gestión de modems a través de una red X.25/FR.

En este caso la propuesta de gestión es sobre una red IP: la de Infocom. Pero pudiera hacerse también sobre X.25 ó FR, protocolos manejados por CUBADATA.

En modo X.25, la ORCHID se conecta directamente a un nodo X.25 (los PSX) y utiliza canales virtuales de conmutación (SVCs) para enviar y recibir información desde la estación central de gestión de red. En el sitio central, se requiere un "router" WAN, en el segmento LAN próximo a la plataforma de gestión. Se encapsula el tráfico IP en X.25, usando la RFC 1356. En FR, la Orchid 1003 LAN se conecta directamente a un nodo FR local y usa canales virtuales permanentes (PVC) para enviar y recibir información desde la estación de dirección de red central. En el sitio donde se encuentra la gestión, un "router" WAN se instala en el segmento de LAN cerca de la plataforma de gestión. El tráfico IP se encapsula en FR, usando las técnicas descritas en la RFC 1490.

2.2.3.2.3 ENCAPSULAMIENTO PPP

Si los sitios con la Orchid 1003 LAN son interconectados por líneas serie, la Orchid 1003 LAN puede encapsular tráfico IP hacia el sistema de gestión central en PPP asíncrono ó síncrono. enviarlo sobre su puerto serie A (V.24) a uno de los 14 puertos serie de otro concentrador Orchid. La velocidad máxima es 9600bps. En la Orchid 1003 LAN, versión de tarjeta, están disponibles 2 puertos serie asíncronos, en la Orchid de buró están disponibles 14 puertos serie. Alternativamente la Orchid 1003 LAN puede conectarse a través de su puerto serie A, a un "router" IP con PPP asíncrono o síncrono o directamente al puerto serie de la estación de gestión de red (si este puerto soporta PPP asíncrono). En el modo de PPP síncrono, es el puerto A externamente, hasta 64 Kbit/s e internamente hasta 38400bps. En el modo asíncrono, la velocidad es de hasta 38400bps. La configuración se muestra a continuación



ORCHID 1003 LAN

ORCHID 1003 LAN

Figura 9 Gestión con encapsulamiento PPP.

En esta configuración, la Orchid 1003 LAN enruta trafico IP entre sus diferentes puertos serie usando “routers” estáticos.

2.2.3.2.4 TOPOLOGIAS MIXTAS

La conectividad IP y Frame Relay entre la estación NMS y la Orchid 1003 LAN también puede combinarse con conexiones serie como se muestra

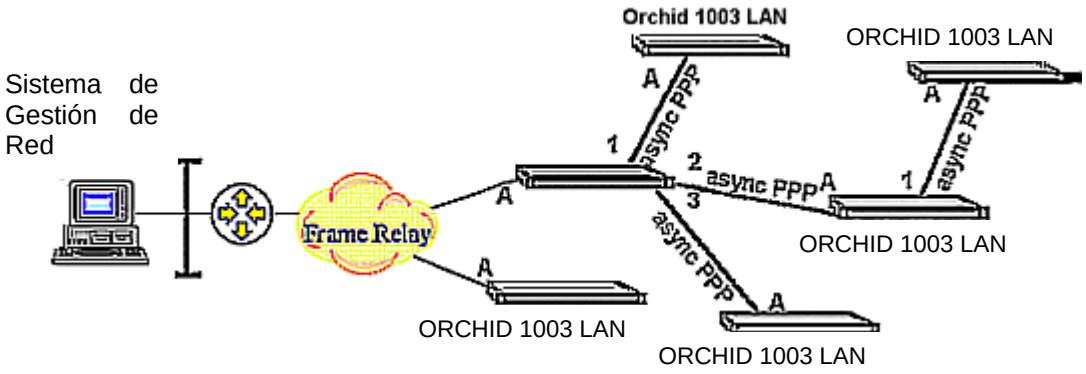


Figura 10. Topologías Mixtas.

2.2.4 ESPECIFICIDADES DEL SISTEMA DE GESTIÓN PARA MODEMS TELINDUS EN REDES DE TRANSMISIÓN DE DATOS DE ETECSA.

Ya con la teoría de todos los elementos necesarios para implementar el sistema de gestión, recordamos que el sistema propuesto se instalará en el MINCOM, el cual constará, como ya mencionamos, con computadora Pentium III, de 256 K de memoria RAM y 20 Gb de espacio en el disco duro, además de contar con Windows 2000 como Sistema Operativo.

En el capítulo 2 se muestran las arquitecturas de la redes CUBADATA e Infocom, que son las que utilizan los modems Telindus a gestionar. En cada sitio central existen gabinetes de propósito general, en los cuales se instalan los subrack CN4. Ver figura 1 del anexo, capitulo 3. En cada sitio se instalará una tarjeta ORCHID. En los centros

donde haya equipos de Infocom, la tarjeta se ubicará en el primer subrack que contenga modems de esta red. En caso de que solo existan modems de CUBADATA, la tarjeta se instalará en el primer subrack. La tabla 2 del anexo, capítulo 3, refleja los lugares donde se ubican los modems y la cantidad existente por sitio.

Se usará el protocolo IP para la gestión de los modems. En este caso se le asigna una dirección IP a cada tarjeta ORCHID y ella se configurará para gestionar las tarjetas de modems instaladas en su sitio. Cada tarjeta podrá administrar hasta 7 "subracks" CN4. Se usará el modo de direccionamiento NMS relativo, donde en este caso, el modem central, toma el valor 0 y el remoto, el 1. La comunicación entre el “proxy” y las tarjetas de modems se hará usando el protocolo CMS2, propietario de Telindus.

En cada sitio, si existe más de un CN4, estos deben conectarse ó “cascadearse”, lo cual se hace a través de uno de los conectores “high speed” (b) con los que cuenta el mismo, como vemos en la figura 4 del anexo, capítulo 3. La conexión con la tarjeta en el “subrack” correspondiente, también se muestra en la figura, lo cual se hará usando un cable de red directo.

Después que ya existen las conexiones internas del gabinete, se llevará, usando el conector TPI de la tarjeta ORCHID y cable RJ45 cruzado, la conexión al “router” de Infocom existente en el lugar, como se muestra en la figura 5 del anexo, capitulo 3.

En caso de que co-existan las redes de CUBADATA e Infocom y los “subracks” se encuentren en gabinetes diferentes, se hará la conexión de los mismos, de gabinete a gabinete. En todos los casos se encuentran lo suficientemente cerca.

Para una mejor gestión por parte del operador se debe usar la resolución de nombres en lugar de las direcciones IP, para esta configuración, ver [58].

Serán instaladas 38 tarjetas ORCHID en todo el país, lo cual representa un costo aproximado de 53664 dólares, incluyendo 10 tarjetas de repuesto, lo cual unido al costo del centro de gestión, 26076 dólares, hace aproximadamente un valor de 79740 dólares en total. Pero esta inversión se amortizará rápidamente, pues al existir este sistema de gestión, se reduce el personal destinado a la atención de estas fallas, lo cual disminuye los gastos en salarios, dietas y hospedaje de la empresa. De manera que podrá recuperarse lo invertido, en menos de dos años.

Esto sin mencionar la reputación que ganará la empresa en la calidad de sus servicios, pues al tener un monitoreo constante del desempeño del sistema, las fallas se detectarán a tiempo, además de saber con mucha precisión, cual es su origen y ubicación, lo que también disminuirá los tiempos fuera de servicio.

3. CONCLUSIONES

Concluyendo este capítulo, queremos reiterar la importancia técnica y económica que para ETECSA constituirá el implementar este sistema de gestión, aunque no debemos dejar de hacer énfasis en la necesidad de poner en marcha la gestión de los sistemas que hoy carecen de este servicio. Sería muy útil aprovechar la plataforma HP Openview para gestionar los equipos de Infocom, pudiera usarse por ejemplo, el Ciscowork, utilizado en los equipos del NAP y de una vez montar estos equipos sobre la misma plataforma de gestión.

Un poco más costosa sería la integración de la gestiones de las Redes de CUBADATA, lo cual necesitaría de una Asistencia Técnica de Alcatel.

CONCLUSIONES Y RECOMENDACIONES

El tema de la integración de las redes de gestión es todavía una novedad en las telecomunicaciones cubanas, pero ETECSA trabaja fuertemente en este sentido, buscando con ello mejorar la calidad de la supervisión y el control de su red de telecomunicaciones y garantizar un mejor servicio.

El objetivo fundamental de este proyecto consiste en analizar el estado actual de la gestión de las Redes de Transmisión de Datos de ETECSA, y como solución a la heterogeneidad de los mismos, provocada a su vez por la complejidad y diversidad del equipamiento instalado, proponer la implementación futura de un sistema de gestión centralizado de red para los modems Telindus, sobre una plataforma que sirva para centralizar las gestiones de redes de datos, en la medida de las posibilidades en el futuro. En este trabajo nos basamos en metas específicas como:

- El análisis del sistema de gestión centralizada
- La caracterización del estado de sistemas de gestión de Transmisión de Datos en Cuba
- El estudio de la aplicación de "Softwares" para implementar un sistema de gestión de modems Telindus.
- La propuesta de un sistema de gestión centralizada en base al equipamiento de los modems Telindus para emplear en ETECSA.

Como conclusiones de este trabajo, a partir de la propuesta de un sistema de gestión para los modems Telindus que se usan en la red de Transmisión de Datos de ETECSA, podemos decir que se ha dado un importante paso de avance en cuanto a la centralización de la gestión de redes, teniendo en cuenta que:

- Los sistemas de gestión de red son cada vez más necesarios para cualquier tipo de empresa que haga uso de redes informáticas por pequeñas que estas sean.
- Las tecnologías de la gestión de red establecidas evolucionan para adaptarse a las nuevas condiciones que ofrece el desarrollo del hardware y nuevas necesidades de gestión.

- Están surgiendo nuevas tecnologías de gestión para redes basadas en la arquitectura de redes TCP/IP donde se destacan la gestión distribuida, los agentes inteligentes y la gestión web con un futuro muy prometedor.

- La mayoría de las instituciones necesitan, para gestionar sus recursos informáticos en redes, una solución asequible y fácil de usar.

- Para el análisis de varios "softwares" de gestión se requiere de parámetros bien definidos que permitan evaluarlos y compararlos.

La propuesta de implementación de un sistema de gestión de red flexible para los modems Telindus de ETECSA se basó en la integración de dos softwares de gestión, el HP Openview y el TMA, este último propietario de Telindus.

Con la realización de este trabajo se ha dado un paso de avance en el diseño de sistemas de gestión de red enfocados a las características particulares de una red, haciendo énfasis en la necesidad de gestionar totalmente el equipamiento existente en nuestras redes.

Es de vital importancia ir hacia la integración de la gestión, tratando de basar la misma en una plataforma flexible y potente como la HP Openview.

Como primeros pasos que den continuidad a este trabajo se recomienda:

- Terminar de comprar, por parte de la Empresa, el equipamiento necesario para el sistema de gestión.

- Preparar al personal para la explotación del mismo.

- Establecer procedimientos de trabajo para la gestión de la red.

- Divulgar los resultados obtenidos a otras instituciones.

REFERENCIAS BIBLIOGRÁFICAS

[1]Bailey, A, “3Com Corp. Transcend” disponible en: http://163.18.14.55/datapro/50461-1.htm#start; Abril, 1998.

[2]Baldi, M.; Picco, G., “Evaluating the Tradeoffs of Mobile Code Design Paradigms in Network Management Applications”;1998.

[3]Bellavista, P.;Corradi A.; Stefanelli C., “An Integrated Management Environment for Network Resources and Services”, IEEE Journal on Selected Areas in Communcations, Volumen (18), No. 5; Mayo, 2000.

[4]Boutaba, R.;Polyrakis, A,”COPS-PR with Meta-Policy Support”, IETF Internet Draft; Mayo, 2001.

[5]Boutaba, R.; Polyrakis, A.,”Projecting Advanced Enterprise Network and Service Management to Active Networks”, IEEE Network; Febrero, 2002.

[6]Bredin, J. ;Kotz, D. ; Rus, D., “Economic Markets as a Means of Open Mobile-Agent Systems, In the workshop “Mobile Agents in the Context of Competition and Cooperation” at Autonomous Agents”; Mayo, 1999.

[7]Bredin, J.; Maheswaran, R.; Imer, C., “A Game-Theoretic Formulation of Multi-Agent Resource Allocation”; 2000.

[8]Brunner, M., “Active Networks and its Management”; Febrero, 2001.

[9]Casassa, M.; Baldwin, A.; Goh, C., “POWER Prototype: Towards Integrated Policy-Based Management”, IEEE/IFIP Network Operations and Management Symposium; 2000.

[10]Chan, K.; Durham, D.; Gai S., “COPS Usage for Policy Provisioning”, IETF Internet Draft, draft-ietf-rap-pr-05.txt; Octubre, 2000. [RFC 3084].

[11] Cheikhrouhou, M.;Conti, P., Labetoulle, J., “Intelligent Agents in Network Management: A State-of-the-art”; 1998.

[12] Dan, B., “Proactive Management With Workgroup SNMP Managers” disponible en:

http://www.networkcomputing.com/713/713revSNMP.html ; 2001.

[13] Displaying Cisco Devices Information with Show Commands, disponible en: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwfw/cw_5_0_1/use_501/cwwsc.htm; 2001.

[14] Dobson, J.E.; McDermid, J.A., "A Framework for Expressing Models of Security Policy", IEEE Symposium on Security & Privacy; Mayo, 1989.

[15] Documentación de CiscoWork, disponible en: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwfw/cw_5_0_1/index.htm; 2001.

[16] Goldszmidt, G.; Yemini, Y., "Distributed Management by Delegation, Proceedings of the 15 the International Conference on Distributed Computing Systems"; Junio, 1995.

[17] Hegering, H.; Abeck, S.; Neumair, B., "Integrated Management of Network Systems"; 1999; pp.6.

[18] Hegering, H.; Abeck, S., Neumair, B., "Integrated Management of Network Systems"; 1999; pp.82-94.

[19] Hegering, H., Abeck, S., Neumair, B., "Integrated Management of Network Systems"; 1999; pp.121-152.

[20] Hegering, H.; Abeck, S.; Neumair, B., "Integrated Management of Network Systems"; 1999; pp.279-287.

[21] Hein, M.;Griffiths, D.,"SNMP Versions 1 & 2 Simple Network Management Protocol, Theory and Practice", International THOMSON computer press; 1995; ISBN 1850321396.

[22] HP OpenView, disponible en: http://ipesa.centroamerica.com/servicios/redes.htm; 2001

[23] Hu, C., Chen, W. E., "A Mobile Agent-Based Active Network Architecture", ICPADS 2000.

[24] IETF Internet Draft: "Policy Framework, draft-ietf-policy-framework-00.txt, work in progress"; Septiembre, 1999.

[25] IETF Internet Draft: “Policy Terminology, draft-ietf-policy-terminology-00.txt, work in progress”, Julio, 2000.

[26] IETF RFC 2748: “The COPS (Common Open Policy Service) Protocol”, IETF RFC 2748; Enero, 2000.

[27] Jay, W., CiscoWorks; disponible en: www.cisco.com; 2000.

[28] Ju, H.; Choi M.; Hong J., “EWS-Based Management Application Interface and Integration Mechanisms for Web-Based Element Management”, Journal of Network and Systems Management, Volumen (9), No.1; 2001.

[29] Knight, G.; Hazemi, R., “Mobile Agent-Based Management in the INSERT Project”, Journal on Network and Systems Management, Volumen (7); 1999.

[30] Koch, T.; Kramer, B.; Rohde, G., “On a Rule Based Management Architecture, The 2 nd International Workshop on Services in Distributed and Networked Environments”, IEEE Computer Society. Canada, 1995.

[31] Koch, F. L.; Westphall, C. B., “Decentralized Network Management Using Distributed Artificial Intelligence”, Journal of Network and Systems Management, Volumen (9), No.4, Diciembre,2001.

[32] Lange, D., “Java Aglets Application Programming Interface (J-AAPI)”, IBM white paper, disponibl en: www.trl.ibm.com/aglets/JAAPI-whitepaper.htm; Febrero, 1997.

[33] Liotta, A.; Pavlou, G.; Knight, G., “A Self-Adaptable Agent System for Efficient Information Gathering”; 2001.

[34] Lupu, E.; Sloman, M., “Conflicts in Policy-Based Distributed Systems Management”, IEEE Transactions on Software Engineering, Volumen (25), No. 6; Noviembre, 1999.

[35] Managing Cisco Devices with CiscoView, disponible en: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwfw/cw_5_0_1/use_501/cwwcv.htm; 2001.

[36] Manual de gestión de Red Alcatel 1100, Alcatel; 1999 .

[37] Manual del usuario de Telindus, Telindus; 2003.

[38] Manual de Gestión de Equipos Newbridge 5620, Newbridge; 2001 .

[39] Martin-Flatin, J.; “Push vs. Pull in Web-Based Network Management”, Technical Report SSC/1998/002, Swiss Federal Institute of Technology. Lausanne; 1998.

[40] Martin-Flatin, J.; Znaty, S.; Hubaux, J. P., “A Survey of Distributed Enterprise Network and Systems Management Pradigms”, Journal of Network and Systems Management, Volumen (7), No.1; 1999.

[41] Microsoft Corporation (Edt), et al: “Optimizing Network Traffic (Notes from the Field)”; 1999.

[42] Miller, M.A., “Managing Internetworks with SNMP”, M&T Books; 1993; ISBN 1558513043.

[43] Moffett, J.; Sloman, M., “Policy Hierarchies for Distributed Systems Management”, IEEE Journal on Selected Areas in Communication, Volumen (11), No. 9; Diciembre, 1993.

[44] Monitoring Cisco Devices with Threshold Manager, disponible en: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwfw/cw_5_0_1/use_501/cwwtm.htm. ; 2001;

[45] Moussa, K., “Tesis de Maestría “Plataformas de Gestión de Redes de Telecomunicaciones”, 2000.

[46] Murphy, S.; Lewis, E.; Puga, R.,”Strong Security for Active Networks”, IEEE OPENARCH; 2001.

[47] Network Node Manager (NNM); 2001; http://www.managementsoftware.hp.com/print.asp?catid=510&level=products.

[48] Network World Fusion, disponible en: http://www.nwfusion.com/reviews/0823rfpipswitch.html; Agosto,1999.

[49] Ou,M.G, “The Common Object Request Broker: Architecture and Specification”;Junio, 1999.

[50] Parnell and Null. “Network Administrator´s Reference”, McGraw-Hill; 1999; ISBN 0078825881.

[51] Prozeller, P., “TINA and the Software Infrastructure of the Telecom Network of the Future”, Journal on Network and System Management, Volumen (5); Diciembre, 1997.

[52] RMON Overview, disponible en: http://www.suport.baynetwork.com/library/tpubs/html/router/soft1101/114070B/N_24.htm.; 2001.

[53] Rogerson, D., “Inside COM, Redmond, WA”; 1997.

[54] Stallings, W.,”Local & Metropolitan Area Networks”, Prentice Hall, Edición:5; 1997; ISBN: 0131907379.

[55] Stallings, W., “SNMP, SNMPv2, CMIP. The Practical Guide to Network-Management Standards”; 2000l.

[56] Straber, M.; Baumann, J.; Fohl, F., “A Java Based Mobile Agent System”, 10 th European Conference on Object-Oriented Programming ECOOP’96; Julio, 1996.

[57] Tennenhouse, D. L.; Smith, J. M.; Sincoskie, W. D, “A Survey of Active Network Research”, IEEE Communications Magazine, Volumen (35), No. 1; Enero,1997.

[58] Thompson, J., “Web-based Enterprise Management Architecture”, IEEE Communications Magazine; Marzo, 1998.

[59] Waldbusser, S., “Remote Network Monitoring Management Information Base”. RFC 1757; Febrero, 1995.

[60]What Is Network Management?, disponible en: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/nmbasics.htm; 2001.

[61] WhatsUp Gold User Guide, disponible en: ftp://ftp.ipswitch.com/ipswitch/manuals/whatsupg.pdf; 2000.

[62] Wooldridge, M.; Jennings, N. R., “Intelligent Agents: Theory and Practice, The Knowledge Engineering Review”. Volumen (10), No.2; 1995.

GLOSARIO DE TÉRMINOS

ADSL	Linea de Abonado Digital Asimétrica (Asymetrical Digital Subscriber Line)
AIM	Módulo de Análisis e Inventario (Analysis Inventory Module)
AMC	Centro de Gestión ACX (ACX Management Center)
API	Interfaz para el Programador de Aplicaciones (Application Program Interface)
AS	Supervisión de Alarmas (Alarm Supervision)
ASCII	Código Estándar Americano de Intercambio de Información (American Standard Code for Information Interchange)
ATM	Modo de Transferencia Asincrónico (Asynchronous Transfer Mode)
BBC	Centro de Facturación (Billing Collection Center)
CAC	Control de Admisión de Conexión (Conection Admission Control)
CCO	Centro de Configuración (Configuration Center)
CGI	Interfaz de Acceso Común (Common Gateway Interface)
CLI	Interfaz de Linea de Comando (Command Line Interface)
CMES	Centro de Mediciones Sistemáticas (Systematic Measurement Center)
CMIP	Protocolo Común de Información de Gestión (Common Management Information Protocol)
COD	Código en Demanda (Code On Demand)
COPS	Servicios de Políticas de Apertura Común (Common Open Policy Services)
CORBA	Arquitectura de Negociación de Petición de Objetos Comunes (Common Object Request Broker Architecture)
CPSS	Sistema de Conmutación de Paquetes de Control (Control Packet Switching System)
CPU	Unidad de Procesamiento Central (Central Processing Unit)
CTAX	Centro de Información (Charging Center)
CTEC	Centro Técnico (Tecnical Center)
CWSI	Ciscoworks para Interconexión de Ruteo (CiscoWorks for Switched Internetworks)

C++	Lenguaje C Orientado a Objetos
DCOM	Modelo de Objeto Distribuido (Distributed Component Object Model)
DOC	Sistemas de Gestión Distribuidos (Distributed Object Computing)
DSL	Linea de Abonado Digital (Digital Subscriber Line)
DTE	Equipo Terminal de Datos (Data Terminal Equipment)
ETECSA	Empresa de Telecomunicaciones de Cuba
GUI	Interfaz Gráfica de Usuario (Graphical User Interface)
HDD	Torre de Disco Duro (Hard Disk Drive)
HDSL	Linea de Abonado Digital de Alta Velocidad (High bit rate Digital Subscriber Line)
HP	Hewlett Packard
HS	Alta velocidad (High speed)
HTTP	Protocolo de Transferencia de Texto (HyperText Transfer Protocol)
IETF	Fuerza de Tareas de Proyectos de Internet (Internet Engineering Task Force)
IP	Protocolo de Internet (Internet Protocol)
IPM	Monitor de Rendimiento (Performance Monitor)
ISDN	Red Digital de Servicios Integrados (Integrated Services Digital network)
ISP	Proveedor de Servicios de Internet (Internet Service Provider)
JIDM	Gestión de Conexión Interdominio (Joint Inter Domain Management)
JMAPI	Interfaz de Gestión Java para el Programador de Aplicaciones (Java Management API)
JVM	Máquina Virtual Java (Java Virtual Machine)
KQML	Lenguaje de Tratamiento de Encuestas (Knowledge Query Manipulation Language)
LAN	Red de Area Local (Local Area Network)
LSP	Ruta Conmutada (Label Switched Path)
MA	Agente Móvil (Mobile Agent)
MAC	Control de Acceso al Medio (Media Access Control)

MbD	Gestión por Delegación
MIB	Base de Información de Gestión (Management Information Base)
MPLS	Conmutación Etiqueteada Multiprotocolo (Multi Protocol Label Switching)
MSD	Dispositivo para compartimiento de Modems (Modem Sharing Device)
MSP	Plataforma Multishelf (Multishelf Plattaform)
NAP	Punto de Acceso de Red (Network Access Point)
NM	Gestor de Nodo (Node Manager)
NMC	Centro de Gestión de Red (Network Management Center)
NMTI	Interfaz de Terminal de Gestión de Nodo (Node Management Terminal Interface)
NMU	Unidad de Gestión de Red (Network Management Unit)
ODBC	Conectividad de Base de Datos Abierta (Open Database Connectivity)
OO	Orientación a Objecto (Object Orientation)
ORB	Negociación de Petición de Objetos (Object Request Broker)
OSS	Sistema de Soporte de Operación (Operation Support System)
OAM	Operaciones, Administración y Mantenimiento (Operations, Administration and Maintenance)
OSI	Interconexión de Sistemas Abiertos (Open Systems Interconnection)
PCRET	Terminal de Usuario final (PC Relational End-user Terminal)
PC-STAT	Centro de Análisis Estadístico (Statics Análysis Centre)
PDP	Puntos de Decisión de Políticas (Policy Decisión Points)
PEP	Puntos de Ejecución de Políticas (Policy Enforcement Points)
PNNI	Interfaces privadas (Private network to network Interface)
PSTN	Red Telefónica Pública de Conmutación (Public Switching Telephone Network)
PVC	Circuito Virtual Permanente (Permanent Virtual Circuit)
QoS	Calidad de Servicio (Quality Of Service)
RAP	Protocolo de Asignación de Recursos (Resource Allocation Protocol)
REV	Evaluación Remota (Remote Evaluation)

RFC	Petición de Comentarios (Request For Comment)
RME	Administrador de Recursos Esenciales de Cisco (Cisco Resource Manager Essentials)
RMI	Invocación de Métodos Remotos (Remote Method Invocation)
RMON	Monitoreo Remoto (Remote Monitoring)
RPC	Llamadas de Procesamiento Remoto (Remote Procedure Call)
RSP	Plataforma de Conmutación de Ruteo (Routing Switch Plattaform)
RTR	Request Time Reporter (Reportero de Tiempos de Respuesta)
SDH	Jerarquía Digital Síncrona (Synchronous Digital Hierarchy)
SDSL	Linea de Abonado Digital Simétrica (Symetrical Digital Subscriber Line)
SLA	Acuerdos de Nivel de Servicio (Service Level Agreement)
SMTP	Protocolo de Transferencia de Mensajes Simple (Simple Mail Transfer Protocol)
SMART	Escalabilidad, Multiprioridad, Ubicación de Recursos y Tráfico (Scalability, Multipriority, Allocation of Resources and Traffic)
SNMP	Protocolo Simple de Gestión de Red (Simple Network Management Protocol)
SONET	Red Optica Estándar (Stándar Optical Network)
SQL	Lenguaje de Programación Estructurado (Structured Query Language)
SPVC	CircuitoVirtual Permanente Conmutado (Switching Permanent Virtual Circuit)
STM	Módulo de Transporte Sincrónico (Synchronous Transport Module)
SVC	Circuito virtual Conmutado (Switching Virtual Circuit)
TCP/IP	Protocolo de Control de Transmisión/Protocolo de Internet (Transmission Control Protocol/Internet Protocol)
TFTP	Protocolo de Transferencia de Ficheros Trivial (Trivial File Transfer Protocol)
TINA-C	Consorcio de Arquitectura de Red de Información de Telecomunicaciones (Telecommunication Information Network Architecture Consortium)
TMA	Aplicación de Gestión de Telindus (Telindus Maintenance Application)
TMN	Gestión de Red de Telecomunicaciones (Telecommunication Management Network)

TSOM	Módulo de Optimización de Tráfico y Servicio (Traffic and Service Optimization Module)
UDP	Protocolo de Datagramas (User Datagram Protocol)
UPC	Control de Parámetro de Uso (Usage Parameter Control)
VAN	Red Activa Virtual (Virtual Active Network)
VFST	Herramienta de Transferencia de Fichero (File Transfer Tool)
VGS	Estación Gráfica VPN (Virtual Private Network Grafic Station)
VIP	Punto de Validación de Información (Validation Information Point)
VLAN	LAN Virtual (Virtual LAN)
VPN	Redes Privadas Virtuales (Virtual Private Network)
WBEM	Gestión de Red Basada en Web (Web-Based Enterprise Management)

ANEXOS

Puerto	**Velocidad Máxima (bps)**	**Número de puertos**	
		Stand alone (TT)	Versión de tarjeta(CV)
Puerto Asíncronico RJ45	9600	14	1
Puerto Asíncronico subD-9	9600	0	1
Puerto RJ45 (A/B)	64000	2	2
Puerto síncronico RJ45 (high speed)	80000	2	2
Puerto de control RJ45	9600	1	1
Puerto Ethernet TPI	10000000	1	1
Puerto Ethernet AUI	10000000	1	0

Función de cada Puerto:

Puerto Asíncronico:

- Conexión de los modems “stand alone”
- Conexión serie del TMA.

Puerto (A,B) master/esclavo:

- Conexión a una red IP con encapsulamiento FR,X.25 y PPP.
- Conexión a otra ORCHID 1003 LAN sobre PPP.
- Conexión serie del TMA (puerto A solamente).

Puerto de alta velocidad: Conexión de la ORCHID 1003 LAN a un subrack CN4. Hasta 7 subracks pueden ser conectados en cascada a una misma ORCHID.

Puerto de control: Gestión local de la ORCHID, usando terminal VT100 ó TMA.

Puerto Ethernet AUI y TPI:Conexión a una red LAN IP

Tabla 3.2.2.3.1. Puertos de la tarjeta ORCHID, velocidades y usos.

Sitio	Cantidad de subracks de modems Telindus
MINCOM	4
Aguila	2
Buenavista	4
Vedado	3
Cubanacán	2
Fontanar	1
Guanabo	1
Luz	1
Lonja	1
Artemisa	1
San José	1
Santa Cruz	1
Mariel	1
Bauta	1
San Antonio	1
Caimito	1
Guanajay	1
Isla de la Juventud	2
Pinar del Río C.T	2
Matanzas	2
Varadero	2
Cienfuegos C.T	2
Santa Clara	2
Caibarién	1
Sancti Spiritus	2
Trinidad	1
Camaguey	2
Santa Lucia	1
Ciego de Avila	2
Cayo Coco	1
Las Tunas	2
Holguín	2
Nuevitas	1
Moa	1
Manzanillo	1
Bayamo	2
Santiago de Cuba	2
Sitio	**Cantidad de subracks de modems Telindus**

Guantánamo.	2
Total	38

Tabla 3.2.2.3.2 Cantidad de subracks de modems Crocus por sitio

Figura 1. Subrack CN4 para instalación de modems (CV) Telindus

Figura 2. Modem de tarjeta y modem stand alone

Figura 3. Subrack de modems SDSL, versión de buró.

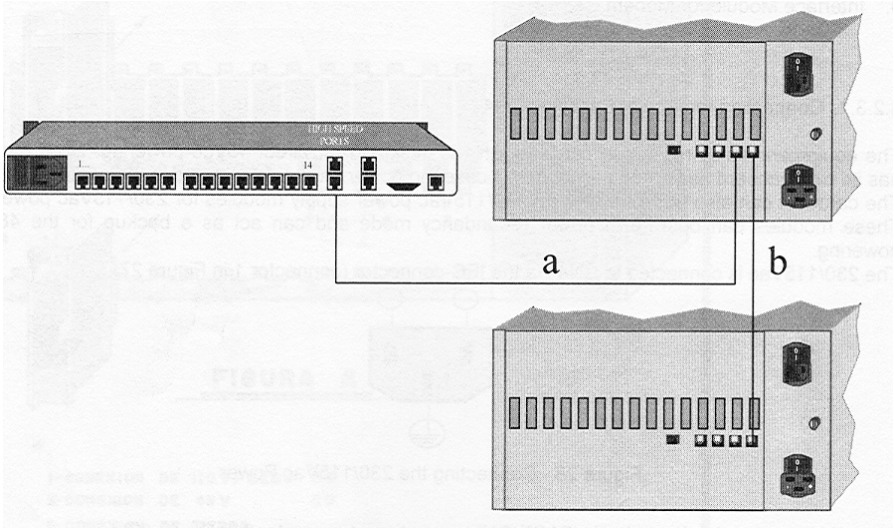


Figura 4 Interconexión entre subracks CN4 y entre el subrack y la red.

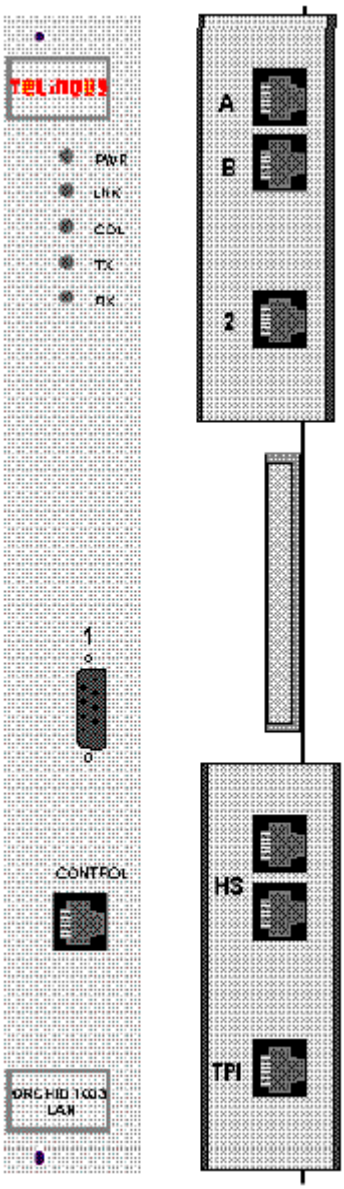


Figura 5. Frente y back panel de tarjeta ORCHID 1003 LAN, de tarjeta.