UNIVERSIDAD de DEUSTO

Facultad de Informática

Diseño de un nivel lógico avanzado e integrador del factor seguridad para su aplicación en un Sistema de Gestión de Red Automatizado

Luis Miguel Garay Gallastegui

UNIVERSIDAD de DEUSTO

Facultad de Informática

Diseño de un nivel lógico avanzado e integrador del factor seguridad para su aplicación en un Sistema de Gestión de Red Automatizado

Tesis doctoral presentada por D. Luis Miguel Garay Gallastegui

Dirigida por el Dr. D. Javier Areitio Bertolín

El Director

El Doctorando

Bilbao, Septiembre de 1996

A Isabel y

especialmente a mis padres

Deseo expresar mi agradecimiento al Prof. Dr. D. Javier Areitio Bertolin, Profesor Titular de Redes de Computadores y Sistemas de Transmisión de Datos de la Facultad de Informática de la Universidad de Deusto, que con su constante colaboración y dirección técnica hizo posible el desarrollo de esta investigación. No puedo olvidar el apoyo prestado por el Prof. Dr. D. Máximo Llaguno Ellacuria, Jefe del Dpto. de Matemática Aplicada y Telemática, así como por el Prof. Dr. D. Evaristo Kahoraho Bukubiye, Catedrático de Automática y Responsable del Área de Ingeniería de Sistemas y Automática, y todas aquellas personas que han colaborado de alguna manera en este trabajo.

También quiero mencionar especialmente a B.T. Telecomunicaciones, por su impulso, colaboración y actitud siempre positiva hacia la Tesis

RESUMEN

El objeto de la Tesis que se presenta es el diseño de un nivel lógico avanzado e integrador del factor seguridad, para su aplicación en un Sistema de Gestión de Red Automatizado. Este diseño se logra satisfaciendo dos objetivos claves, como son por un lado estructurar y diseñar las relaciones y funcionalidades críticas para una integración positiva de las aplicaciones de Gestión de Fallos con las Plataformas de Gestión de Red, y por otro, aportando claves para mejorar la calidad del proceso de seguridad de una red y su integración en el rendimiento de las Plataformas de Gestión de Red.

ABSTRACT

The Thesis's purpose is the design of an advanced logical level that integrates the segurity factor, to be used by an Automate Network Management System. To satisfy these requirements, we structurate and design the relations and critical functional characters for a good integration of the Fault Management Applications with the Network Management Platforms, and we give keys for improving the Network security process and integrating it into the Network Management Platforms performance.

Índice

Índice de Algoritmos

Índice de Figuras

1. Introducción : Ámbito

La gestión de una red de telecomunicaciones implica monitorización casi en tiempo real y control de sus recursos con el fin de aportar una óptima y segura utilización de los equipos disponibles y maximizar la capacidad de transporte de los datos.

A principios de los 80 se produjo una fuerte expansión del tráfico de comunicaciones de datos. Las compañías se percataron de los beneficios y aumento de productividad obtenida gracias a sus redes corporativas y comenzaron a expandir sus redes rápidamente y en paralelo con la aparición de nuevos productos y el avance de la tecnología

Todo este crecimiento desbordado hizo que a mediados de los 80 se comenzaran a sentir las consecuencias dolorosas de tal empuje, especialmente en aquellas empresas que no se habían ajustado a unos planes estratégicos que contribuyeran a aliviar esta pesadilla y encauzaran ordenadamente sus infraestructuras locales, equipos de comunicaciones, servicios de comunicación remotas, servicios de acceso a computadores y gestión de red. Es decir, entornos y arquitecturas múltiples bajo una estructura común.

En el pasado, la función de gestión de redes era más sencilla y menos crítica que en las redes modernas de hoy. Tradicionalmente ha sido una operación manual, apoyándose en personal cualificado y experimentado. Sin embargo, las redes han crecido en complejidad y demandan menores tiempos de respuesta, por lo que ha llegado un momento en que la

propia función de red tiene como limitación el juicio humano, viéndose seriamente limitada por el número y nivel de capacidad del personal disponible para su control.

Una gran red de telecomunicaciones no puede gestionarse solamente con el esfuerzo humano. La complejidad de los sistemas exige automatizar su gestión y esta urgente necesidad crece de igual manera que la proliferación de cambios tecnológicos.

La introducción y empleo de las Plataformas de Gestión de Red en este entorno, como sistemas de supervisión y control que son, supone un adecuado soporte de aquellas aplicaciones especificamente adaptadas al entorno de red, y donde se requiere un comportamiento que satisfaga tanto las altas exigencias de seguridad como de tiempo existentes. Sin embargo, la relación entre éstas y las aplicaciones es aún deficiente, al igual que la seguridad de SNMP, mayoritariamente empleado en este entorno. Lo cierto es que la disponibilidad de entornos de gestión unificada y soluciones que combinen e integren aplicaciones eficaces e integradas, es actualmente una utopía

1. Introducción : Objetivo

Debido a esta incompleta relación entre las aplicaciones de gestión y el nivel de servicios propio de las Plataformas de Gestión de Red, su soporte, se pretende contribuir a la mejora de los Sistemas de Gestión de Red mediante el diseño de un nivel lógico avanzado que se implemente como intermediario entre las Aplicaciones de Gestión y las propias Plataformas de Gestión, a modo de valor añadido y con funciones de soporte a decisiones específicas de cierta complejidad a tomar por las primeras, integrando aquellos factores relativos a la seguridad.

Con esta finalidad, el primer objetivo es **estructurar y diseñar las relaciones y funcionalidades críticas para una integración positiva de las aplicaciones de Gestión de Fallos con las Plataformas de Gestión de Red**

En este sentido, se diseña la arquitectura ASSEF para la Gestión de Comunicaciones en un entorno WAN generalizado como plataforma en la que se desarrolla el software de gestión de fallos, abordando también la necesidad de mantener en ocasiones una gestión descentralizada

Es en este marco donde se estructura el desarrollo del NAAP (Nivel Avanzado de Apoyo a las Plataformas de Gestión). De igual manera, se sintetizan los criterios fundamentales para ajustar el NAAP con las Plataformas de Gestión de Red, y se adapta la funcionalidad aportada por el NAAP a la gestión de red en tiempo real, aportando claves para su representación e implementación algorítmica con un modelo concreto para la detección de problemas y su diagnóstico

Finalmente, para completar el valor añadido del NAAP y su contribución a las aplicaciones de gestión de red actuales, se aporta el método CNOD (Cuantificación de la Necesidad y su repercusión en los Objetivos basado en Lógica Difusa), que mejora el comportamiento humano a la hora de reaccionar ante los eventos de la red, pudiéndose implementar e integrar como un módulo software dentro del NAAP. Este método se elabora para ayudar por un lado al gestor de la red y por otro, para poder incorporar dentro de las Plataformas de Gestión la posibilidad de trabajar con objetivos, a través de una cuantificación de la necesidad y permitiendo así establecer una relación directa entre los recursos de la red, las prioridades de empresa y la probabilidad en los diagnósticos, automatizando la mecánica de operación

El segundo pilar importante es la **aportación de pautas para la mejora de la calidad del proceso de seguridad de una red y su integración en el rendimiento de las Plataformas de Gestión de Red a través del NAAP**

Con esta finalidad, se define y diseña un Modelo de Seguridad Avanzado integrable en el NAAP, tras realizar un estudio sobre la falta de seguridad en diferentes casos de accesos no autorizados, basados en un entorno real Este apartado se completa con la síntesis de factores claves complementarios con el MOSA, que condicionan la percepción de un sistema de seguridad, y su estructuración

También se evalúa la incidencia la incidencia del Protocolo de Gestión de Red en la seguridad y robustez de un Sistema de Gestión de Red, validando la factibilidad del uso masivo de SNMP v 1 en entornos seguros al razonar con datos incompletos

Se completa este segundo objetivo, con un diseño adaptativo de criterios para afrontar la variable "tiempo" del dominio propio de las plataformas, y sintetizando las facilidades y requerimientos relativos a dicho factor, que el NAAP orientado a la gestión de red aporta en un entorno integrado con las plataformas de gestión de red

2. Bases TEÓRICAS.

Dada la necesidad de interconexión creciente por parte de las empresas, y con unos niveles de calidad exigidos cada vez mayores, hay dos aspectos que se hacen más obvios:

1º La red, sus recursos y aplicaciones distribuidas son indispensables para la organización. De hecho se tienden a considerar como un sistema estratégico, global en las empresas, en lugar de un medio para resolver un problema concreto [BEAM93].

2º Desgraciadamente, también cada vez más, un mayor número de cosas pueden ir mal, llegando a degradar su operatividad a un nivel no aceptable, o incluso inhabilitar parcial o totalmente la red [KUBA92].

2.1. Estado del arte de las Plataformas de Gestión de Red.

Esta situación hace necesarias nuevas soluciones que soporten las actuales necesidades de servicio en las grandes redes y que den respuesta de forma automatizada al imperativo de gestión y administración que supone un colectivo de clientes que aumenta día a día y en constante proceso de cambio [AFEK96]. En este punto, la utilización de plataformas abiertas de gestión de red como *OpenView de HP, NetView de IBM, SunNet Manager o Spectrum de Cabletron*, constituyen la base sobre la que unos módulos software, trabajando con un cierto grado de integración a través de APIs, son capaces de recolectar y gestionar una gran variedad de datos de los distintos dispositivos,

poniéndolos después al servicio de las aplicaciones propietarias que estarán funcionando sobre estas bases.

Las plataformas, al ofrecer a los proveedores de equipos de red un grupo común de servicios, como un interface único para el operador, un mapa con la representación de todos los equipos conectados, etc , y la posibilidad de que funcionen todas las aplicaciones sobre un único terminal, recayendo la mayor parte del hardware y software necesario para la gestión de red sobre un mismo equipo de usuario [DEWA93], constituyen un aliciente para que los fabricantes hagan evolucionar sus aplicaciones propietarias a estas plataformas

Las aplicaciones de gestión, por su parte, examinan, relacionan y trabajan con la informacion recogida pudiendo complementar incluso los servicios de la plataforma con metodos nativos de obtención de información adicional de los dispositivos de la red y siendo capaces de incidir directamente sobre ellos en caso de un comportamiento atipico [FIL91] La amplia aceptación de SNMP es un factor importante de cara a que los desarrolladores coordinen sus aplicaciones en las plataformas comunes

2.1.1. Problemas existentes en las Plataformas de Gestión de Red.

Esta esperanza de unificación de servicios, independientemente de la plataforma empleada, arrastra aún alguna grieta que el mercado y el tiempo terminarán cerrando

a) En algunas áreas todavía no existen aplicaciones de soluciones complementarias, y en otras, aún se encuentran en un estado muy primario y poco elaborado [STAL95]

b) Muchos fabricantes de equipos de red están aún comenzando a migrar sus

aplicaciones de gestión a las plataformas dominantes [FREN90].

c) Gran parte de los equipos que hoy se utilizan en las redes fueron fabricados a mediados de la pasada década, y al no ser actualizados no se pueden utilizar con las plataformas de gestión [LAZA91].

2.1.2. Evolución de las Plataformas de Gestión de Red.

Sin embargo, esta migración hacia las plataformas de gestión tiene una importancia crítica porque parece ser la única esperanza real de unificar la gestión, y compatibilizar así, una gestión eficaz de las redes de empresa con un entorno empresarial hoy por hoy marcado por la reducción de costes y mejora de la productividad [STAN93].

Los Sistemas de Gestión de Red permiten garantizar unos niveles de servicios de red preestablecidos que demandan los usuarios para la conectividad e interoperatividad de sus recursos [AREI96b]

La evolución de estas plataformas vendrá impulsada por un lado por su demanda, y por otro por las posibilidades de mejora que presentan al ser un producto joven [VORU94].
El mercado se mueve y como entrante tenemos que un factor común en las futuras versiones es su orientación hacia una gestión descentralizada. Para mostrar esta tendencia que pretenden seguir los diversos fabricantes, tenemos que:
a) Spectrum de Cabletron introduce la noción de servidores distribuidos que recogerá por separado información de gestión proveniente de las diversas zonas de la red y los equipos a ellas asociadas

b) IBM entra en la gestión orientada a objetos - SystemView - para sistemas y redes. Las herramientas de gestión serán representadas como objetos, permitiendo ver los propios dispositivos supervisores desde un punto central.

c) SunSoft con Consoles Software permite bajo SunNet Manager intercambiar información de varias estaciones de trabajo, para formar una sóla base de datos lógica. No se podrá utilizar para la sincronización de bases de datos [COWO95].

2.2. Situación actual de la integración entre Plataformas de Gestión de Red y aplicaciones.

La integración de los productos con las plataformas sobre las que funcionan, y con otras aplicaciones que la comparten simultáneamente, no está todavía implementada al 100%. Esta falta de interoperatividad puede llevar al usuario a verse obligado a utilizar conjuntamente varias aplicaciones de modo que, al final, pueda obtener la funcionalidad requerida [NASS94]

La capacidad de acceder a una MIB común, de intercambiar comandos comunes para que una aplicación pueda invocar a otra que realice una tarea, de reducir procesos redundantes como las propias prestaciones de escrutinio, manejo de errores y su codificación particular con colores diferentes, de integrar datos, almacenar y facilitar su acceso en bases de datos con sistemas gestores de bases de datos comunes, etc., constituyen aspectos clave que deben normalizarse. Las especificaciones de SNMP

contienen una MIB estándar para que las herramientas de gestión puedan acceder a la información, pero no para que se pueda traducir estos datos de forma que pueda ser almacenada. Los fabricantes de plataformas tienen que agregar una capa de software que identifique y traduzca las diferencias.

Los fabricantes de productos dependen en gran medida de la plataforma bajo la que van a operar y esto obviamente conlleva un esfuerzo añadido a la hora de poner en el mercado una misma aplicación que sea compatible con distintas plataformas [CHAN91]. Por un lado los fabricantes de productos demandan una serie común de APIs, pero por otro lado los fabricantes de plataformas quieren diferenciar sus productos y no tienen ninguna intención de estandarizarlos [CLAR92]

Se debería tender a describir, por ejemplo, esquemas para poder almacenar información de sistemas DBMS en repositorios, desarrollar un API normalizado y sencillo con el que se pudiera acceder a datos comunes e integrar eventos multiprotocolo, etc. De esta forma se ayudaría a los usuarios a enmascarar las diferencias internas de los distintos fabricantes

Con este objetivo, en mayo del 94 un grupo de terceras empresas formó el Consorcio de Integración de Gestión (MIC), en un intento de discutir el control de las API. Pero ya en Julio del 95, ante las dificultades para llegar a acuerdos, cuatro grandes pilares como Digital Equipment, Hewlett Packard, IBM y SunSoft, que en un principio se comprometieron a soportar los resultados que MIC adoptara, han abandonado el consorcio

Los principales impulsores de esta iniciativa MIC eran las compañías que suministraban equipos de red (hubs, routers, ...) pero al parecer los fabricantes de plataformas prefieren seguir diferenciando sus productos. A pesar de todo, MIC seguirá con sus trabajos aunque realmente tendrán poco impacto si los fabricantes de plataformas no los implementan [COWO95].

2.3. Estudio de la arquitectura de una Plataforma de Gestión de Red.

La gestión integrada de herramientas de monitorización y control de red presenta una estructura básica (Figura 1) y conjunto de relaciones, que está presente en la mayoría de las arquitecturas de gestión de red. Las dispositivos gestionados disponen de un software (agente) que les permite enviar alarmas (traps) cuando detectan problemas. Con dichas alarmas recibidas, las entidades de gestión están programadas para reaccionar ejecutando diversas acciones: notificación al operador, actualización del histórico, intentos automáticos de recuperación y reconfiguración, aislamiento de averías, etc. [BOUL94]

Las entidades de gestión (gestor) también pueden interrogar a las estaciones finales para conocer el estado de sus variables. Este sondeo puede ser automático o iniciado por el operador. El agente de cada dispositivo gestionado responde al sondeo, valiéndose de un protocolo de gestión de red (SNMP, CMIP) y la información se almacena en una base de datos, denominada MIB.

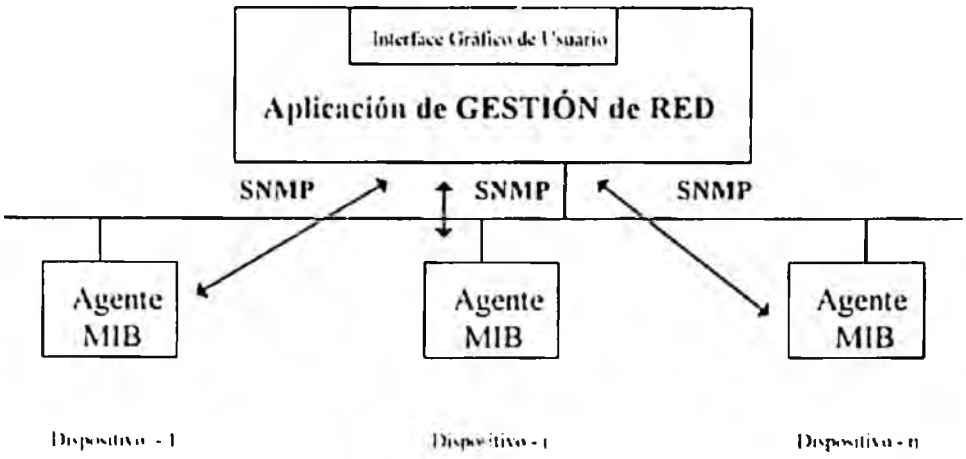

Fig. 1 Arquitectura de una Plataforma de Gestión moderna.

2.3.1. Profundización en una plataforma: SunNet Manager

Esta plataforma abierta de gestión de red consta de una serie de librerías y demonios, unas pocas aplicaciones de gestión, agentes para gestionar las estaciones SUN y unos pocos agentes apoderados para manejar otros sistemas, incluyendo aquellos manejados a través de SNMP

a) Agentes

Los agentes (Figura 2) son programas que permiten acceder a la configuración y datos de operaciones de sistemas y dispositivos. Suelen actuar por orden de los gestores aunque también pueden enviarles mensajes no solicitados. Se ejecutan dentro del dispositivo gestionado

b) Gestores

Los gestores (Figura 3) conocen las características de los agentes al proveer estos últimos esquemas que definen los datos manejados.

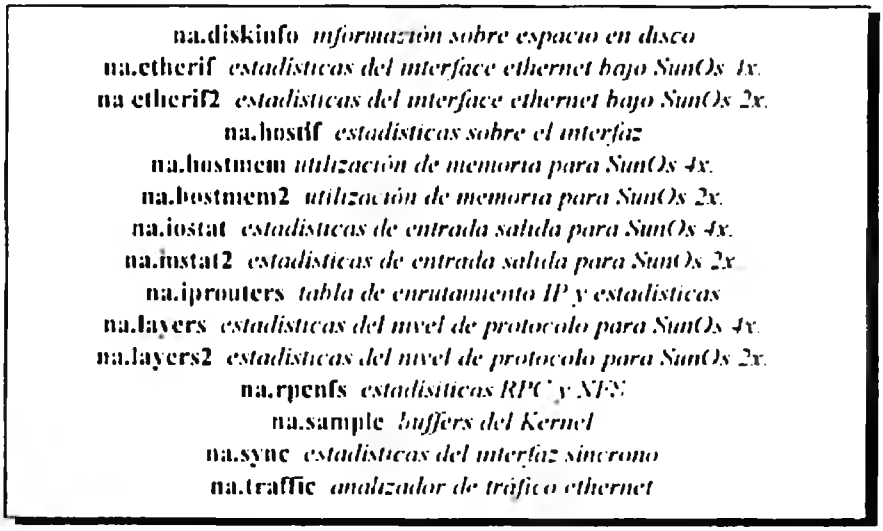

Fig. 2 Agentes de SunNet Manager

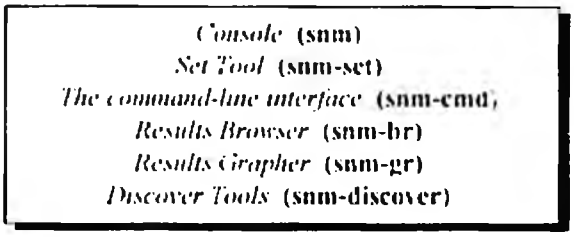

Fig. 3 Gestores de SunNet Manager.

c) Agentes apoderados.

Los agentes (Figura 4) son programas que se ejecutan dentro del dispositivo gestionado En algunas ocasiones esto no es posible, por la insuficiencia de recursos, o conveniente, debido a los elevados costos Los agentes que gestionan dispositivos diferentes de aquellos en los que se están ejecutando son agentes apoderados En cierto sentido los agentes apoderados son gestores y agentes al mismo tiempo.

SunNet Manager también provee unos cuantos agentes apoderados Estos agentes

siempre se ejecutaran en un sistema SUN suministrando información a otros fabricantes.

na.hostperf *datos sobre el rendimiento del host*
na.ippath *información de trazas de los paquetes IP*
na.lpstat *estado de la impresora*
na.ping *información sobre conectividad IP*
na.snmp *agente genérico SNMP v1*
na.snmpv2 *agente genérico SNMP v2*
na.snmp-trap *agente traps SNMP*

Fig. 4 Agentes apoderados de SunNet Manager.

d) Extensiones de la plataforma

En la plataforma SunNet Manager es posible añadir nuevas aplicaciones de gestión o nuevos agentes (Figura 5) El autor de la presente Tesis dentro de la compañía B.T. Telecomunicaciones, ha colaborado durante 1995 en la evaluación de la incorporación a su sistema de gestión de red del software 9000-SNM. **9000-SNM** es una serie de extensiones a SunNet Manager que permite la gestión de MODEMs y PADs bajo una estación SunSparc Ha sido diseñado para trabajar bajo el entorno Motif, aunque también funciona bajo un entorno OpenWindows, cubriendo las necesidades de redes virtuales privadas, que aporta los siguientes agentes

na.codex6500 *habla con el CTP del nodo 6500 a través de X.25*
codextrap *pseudo agente que escucha X.121 y redirecciona las alarmas a SunNet Manager*
na.codexcaple *habla con SunNet Manager y también habla SNMP con un proxy*
codexcapletrap *pseudo agente que escucha traps SNMP y los direcciona a SunNet Manager*

Fig. 5 Agentes de 9000-SNM.

Productos como 9000-SNM supondrían para las compañías operadoras de transmisión de datos un cambio cualitativo en su gestión de red, impulsado originariamente por una

migración en los módems empleados en los nodos, fruto de la evolución natural en los dispositivos empleados, y también por el deseo de elevar el rendimiento y control sobre una red en constante crecimiento.

Sin embargo no hay que olvidar que los sistemas de gestión de red deben orientarse y adecuarse a los procedimientos de trabajo empleados en la organización en que se encuadrarán. De igual forma que cada nueva implementación en una empresa pretende mejorar el funcionamiento de una parte del negocio, o implementar funcionalidades nuevas para aumentar la eficiencia, los sistemas de gestión también deben dar una solución satisfactoria a los problemas, puesto que si no serán algo inútil para el Centro de Control y para la propia compañía en general. En definitiva, hay que ajustar las soluciones a las necesidades y no al revés.

2.3.2. Consideraciones en torno al protocolo de gestión de red: SNMP.

La gestión llevada a cabo por las plataformas y las aplicaciones que sobre ellas funcionan, se sirve de un protocolo de gestión de red para el transporte de la información. SNMP (Simple Network Management Protocol) es un protocolo dentro del nivel de aplicación diseñado para facilitar el intercambio de información entre dispositivos de red, y con un grado de aceptación y uso en las plataformas de gestión sobresaliente. Por ello se ha convertido en un elemento integrador imprescindible y

realmente se puede decir que la gestión y administración de redes se encuentra actualmente bajo el imperio de SNMP [GOUD95].

En su origen SNMP era una especificación interina, y como tal fue diseñado e implementado: tenia que servir mientras el estándar OSI no fuera una realidad, pero no ocurrió asi. Lejos de ser una solución provisional, SNMP se ha convertido actualmente en el estándar de facto de la gestión de red [STAL94], evolucionando en su propia linea. Pero para saber algunas de las limitaciones y virtudes de SNMP hay que saber cuales son sus principios fundamentales de diseño.

2.3.2.1. Determinación de las carencias y ventajas actuales del diseño de SNMP.

La IETF (Internet Engineering Task Force) se propuso que sus trabajos fueran sencillos, lo que incluso afecta al nombre del protocolo, aunque sólo es "sencillo" en comparación con el modelo de gestión OSI.

Los criterios de diseño de SNMP tienen como primer axioma fundamental, que debido a que los dispositivos gestionados pueden tener una limitada habilidad para ejecutar software de gestión (pueden tener una CPU relativamente lenta, o memoria limitada), éste debe asumir el mínimo denominador común. En consecuencia, el impacto en los nodos gestionados es mínimo siendo los agentes muy simples. Casi toda la inteligencia reside en los gestores. No es que no se pudieran crear agentes mucho más inteligentes, pero al demandarles unos requisitos escasos, SNMP se puede meter en casi cualquier equipo, siendo fácil y barato.

El segundo criterio es que la gestión de red debe ser útil y debe llegar a la mayor cantidad de elementos posible. Este apartado puede ser posible satisfaciendo el primer criterio.

El tercer y cuarto criterio dicen que la gestión de red debe ser diseñada para trabajar aunque existan fallos en la red o esté parcialmente dañada o congestionada, y que la finalidad de una red y de sus elementos es transportar datos de la aplicación y no soportar las funciones de la gestión.

Estos criterios son ciertamente muy válidos y en muchos caso necesarios, pero el deseo de simplicidad y facilidad de implementación, ha chocado con la robustez deseable de un protocolo que gestiona elementos criticos y con requisitos de seguridad [STAL95]. Por ello SNMPv2 ha avanzado desarrollando nuevas caracteristicas. Sin embargo, muy pocos fabricantes han comercializado por ahora paquetes acordes con SNMPv2 [COWO95]

2.3.2.2. Comparación de SNMPv.1 vs SNMPv.2.

Un punto fuerte de la versión original era su prestación de descubrimiento automatico, que encontraba e identificaba nuevos dispositivos de red. Esto es incompatible con la seguridad de SNMPv2, que exige que un dispositivo suministre una declaración de seguridad para ser conectado a una red. La administración de seguridad es otro área problemática puesto que obliga a mantener y coordinar una serie de bases de datos distintas, recargando perceptiblemente el sistema informático. SNMP v 2 trata también de paliar las carencias de la norma original en lo que se refiere a seguridad, transparencia

de datos o privacidad y comunicaciones "gestor a gestor".

SNMPv.2 ha mejorado resumidamente en seguridad, privacidad , control de accesos y reducción de tráfico [STAL95].

a) Mejoras en cuanto a seguridad y privacidad.

La ausencia de autentificación es la deficiencia más seria de SNMPv.1, haciéndolo vulnerable a cambios no autorizados de la red. Por este motivo, muchos vendedores no han implementado la primitiva *'Set'*, reduciendo SNMP a las facilidades de monitorización y eliminando las de control. Los agujeros en la seguridad de SNMPv.1 son notorios

a.1) Una entidad no autorizada puede intentar realizar operaciones de gestión asumiendo la identidad de una entidad autorizada, modificando el mensaje incluso en operaciones de configuración y contabilidad.

a.2.) Debido a que SNMPv.1 está diseñado para operar en conexiones no orientadas a conexión, una entidad puede reordenar, borrar o copiar un mensaje para responderlo más tarde. Por ejemplo, se podría copiar y después repetir un mensaje para resetear un dispositivo.

a.3.) Una entidad puede aprender los valores de objetos gestionados y aprender eventos notificables, monitorizando los cambios entre un agente y un gestor.

SNMPv.2, (RFC 1446) a través de su procedimiento de autentificación permite verificar a un agente que el envío de un determinado comando ha sido efectuado por un gestor autorizado, y asegurar que los mensajes son recibidos como se enviaron, sin alteraciones

en su contenido Para ello los gestores y agentes sujetos de la comunicación han de compartir una clave secreta (algoritmo MD5). El gestor usa esta clave para obtener un código de autentificación que se añade al mensaje a transmitir. Cuando el agente recibe el mensaje, utiliza la misma clave para, a su vez, obtener de nuevo el código de autentificación. Si la versión del código del agente coincide con el valor añadido al mensaje entrante, el agente sabe que el mensaje sólo puede haber sido originado por el gestor autorizado y que su contenido no ha sido alterado durante su transmisión.

La privacidad permite a los gestores y agentes encriptar los mensajes para impedir que sus contenidos sean conocidos por terceros no autorizados También en este caso los agentes y gestores han de compartir una clave secreta, pero diferente a la usada para autentificación. Si ambos son configurados para utilizar esta función de privacidad, el gestor encripta el mensaje según el algoritmo DES (Data Encrytion Standard) y su clave secreta, y lo envía al agente, el cual realiza el proceso de descifrado también mediante DES y su clave correspondiente.

b) Mejoras en cuanto al Control de accesos.

SNMPv.2 hace posible configurar los agentes de modo que sean capaces de ofrecer diferentes niveles de acceso según el gestor de que se trate. Así, los accesos pueden ser limitados identificando tanto los comandos que el agente aceptará de un gestor determinado como la porción de MIB del agente al que ese gestor puede acceder.

c) Mejoras en cuanto a la Reducción de tráfico.

Otro de los puntos flacos de la norma SNMP original reside en el alto volumen de tráfico

generado entre los gestores y agentes [STAL95]. Como SNMPv.1 sólo permite intercambiar un número limitado de datos en cada transacción, frecuentemente las estaciones de gestión se ven forzadas a generar un elevado número de ellas.

Para eliminar este inconveniente, SNMPv.2 (RFC 1448) añade un nuevo comando GetBulk, introduciendo también una versión mejorada del comando Get de SNMPv.1.

En condiciones reales de utilización, el rendimiento de SNMP depende de la rapidez con la que los agentes puedan atender peticiones. El ancho de banda necesario para los mensajes SNMP es trivial, y la potencia del hardware acostumbra a ser más que suficiente para procesar los mensajes. Pero si se reducen las peticiones SNMP y los mensajes que los agentes necesitan generar, se aligera mucho el peso de los mismos en el sistema. Muchas de las peticiones tratan sobre bloques grandes de objetos MIB, por lo que la operación GetBulk representa una forma obvia de aumentar el rendimiento. Después de todo, un agente puede procesar una petición de diversas entradas de la tabla casi tan rápido como para una sola entrada. Por ejemplo, una típica MIB de datos estadísticos históricos RMON puede tener doscientas entradas. Para recuperar esta información sin una operación GetBulk, el software de gestión tendría que generar doscientas peticiones y doscientas respuestas. Con la operación GetBulk sólo hay una petición y una respuesta

d) Mejoras en cuanto a las comunicaciones gestor a gestor: cooperación entre gestores.

A medida que crece el número de dispositivos y redes gestionadas, se vuelve poco

práctico gestionar la totalidad del sistema desde la única estación de gestión. Por ello, lo que muchos usuarios querrían es poder disponer de una estrategia de gestión descentralizada, en la que uno o algunos gestores de alto nivel controlasen otros gestores de nivel inferior. Esto implica una cooperación gestor a gestor que SNMPv.1 no da puesto que no tiene ningún macanismo automático que permita a un gestor conocer información sobre la red que gestiona otro sistema de gestión [STAL95].

En una arquitectura distribuida, algunos sistemas operan tanto como gestor y agente. Cuando funcionan como agente, un sistema acepta comandos de un sistema de gestión superior y estos comandos pueden acceder a la información que está almacenada localmente o por el contrario pueden pedir al sistema que suministre información sobre agentes subordinados.

La comunicación gestor a gestor viene implementada por dos nuevas características:

d.1.) Comando Inform. Se utiliza por el gestor para enviar información no solicitada a otro gestor, como notificación de eventos inusuales. Tales notificaciones no solicitadas constituyen una herramienta ideal para configurar un esquema de gestión de red descentralizado, puesto que los gestores de mayor nivel no se ocupan por si mismos de ciertos detalles concernientes a las partes remotas de la red.

d.2.) MIB gestor a gestor (RFC 1451) : define tablas que pueden ser usadas para poner en marcha un esquema de informes de eventos. La MIB especifica qué eventos darán origen a una notificación, qué información va a ser incluida en ella y qué gestor o gestores la recibirán. La información es transmitida en un comando Inform.

2.3.2.2.1. Viabilidad de SNMPv.2 y su coexistencia con SNMPv.1.

A pesar de las lagunas de SNMPv.1 que afectan sin remedio a la gestión de red, se puede decir que SNMP goza de buena salud, y no solamente en el área de las WAN [STAL95]. SNMP también se emplea con muy buenos resultados en los sistemas operativos de red local [COWO95]. De hecho, los principales fabricantes están construyendo sus propios caminos. Novell, Microsoft y Banyan Systems cuentan ya con soluciones de gestión para sus respectivos entornos LAN desde una plataforma única. Pero aunque el objetivo es el mismo, cada una de estas firmas ofrece un enfoque diferente. Banyan y Novell buscan el soporte de una amplia variedad de niveles de SNMP que garantice el control de sus LAN desde la misma consola utilizada para gestionar los dispositivos de InterNetworking. Microsoft, sin embargo, pretende aportar herramientas basadas en Windows NT Advanced Server que gestionen los sistemas conectados a las LAN y ofrezcan la información así obtenida a plataformas de nivel superior.

A pesar de todo, la adopción de SNMPv.2 implica un coste adicional puesto que la seguridad dispara los gastos de desarrollo y de diseño en áreas como la depuración de problemas de red, exploración de topología y diseño de sistemas de gestión de red.

Por otro lado, la posibilidad de que los dispositivos soporten un SNMP bilingüe facilitaría a los usuarios la migración gradual a SNMPv2. RFC 1452 define una estrategia para la coexistencia SNMPv1 / v2. Esta estrategia define dos técnicas básicas un agente proxy y una estación de gestión de red (consola) bilingüe El agente proxy traduce los

mensajes entre SNMPv1 y SNMPv2, mientras que la consola bilingüe incorpora tanto la versión 1 como la 2, y por lo tanto puede comunicarse con los dos tipos de agentes.

3. Estructuración y diseño de las relaciones y funcionalidades críticas para una integración positiva de las aplicaciones de Gestión de Fallos con las Plataformas de Gestión de Red.

La gestión de una red de comunicaciones y transmisión de datos moderna presenta una doble vertiente para una operadora

Primero, como cualquier otro suministrador de servicios, vende un producto que no es mas que la capacidad para el transporte de tráfico de su red "global" y el uso de sus componentes a otras compañías. A partir de ahí, los clientes, con la posibilidad de combinar estos ingredientes de muy distintas formas, utilizarán este potencial para construir sus redes corporativas y de paso, cada vez más, demandar un mayor control y asistencia sobre ellas y los elementos que las forman. De hecho, esta gestionabilidad de los recursos, a ser posible trasparente, se esta convirtiendo en un requisito previo en la venta de servicios

En segundo lugar, una operadora puede ser por si misma un gran usuario de su propia red

Los sistemas de Gestión de Red obviamente se encuentran incluidos en este doble enfoque, y desempeñan un papel fundamental. Considero adecuado por lo tanto, antes de pasar a estudiar la integración de las aplicaciones software en las plataformas de Gestión

de Red, estructurar el marco en que estos sistemas de Gestión de Red se mueven (Figura 6) y en el que se encuadran todas las acciones, funciones e información que se emplea para planificar, organizar, ejecutar y controlar efectivamente una red de comunicaciones.

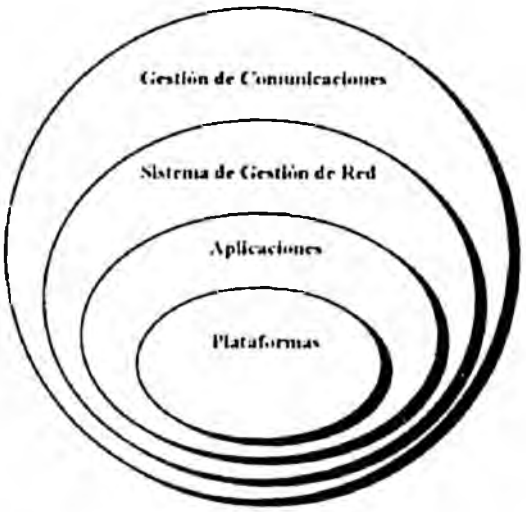

Fig. 6 Esquema de Capas de la Gestión de las Comunicaciones.

3.1 Definición y diseño de la arquitectura ASSEF para la Gestión de Comunicaciones en un entorno WAN generalizado.

Recogiendo los procesos fundamentales esparcidos por los distintos planteamientos reales utilizados hoy en dia que toda estructura de gestión posee, y tras integrarlos, interrelacionarlos y aplicarlos al mundo tecnológico de las redes de comunicaciones, aporto la arquitectura **ASSEF** (Arquitectura de Soporte al Software de Gestión de Fallos), formada por tres componentes primarios:

a) Componente funcional: Cuáles son las funciones propias de una gestión, donde se desarrollan y cómo interactúan entre si.

b) Componente estructural: Cómo encajan unos con otros los niveles y componentes del sistema de gestión y cómo se almacena y manipula la información.

c) Componente de interface: Cómo fluye la información dentro del sistema y cómo se le da forma, se intercambia y comunica.

3.1.1. Desarrollo funcional de una arquitectura de Gestión de Comunicaciones global.

Este apartado describe las funciones que se llevan a cabo en la estructura de gestión. Las agrupo en categorías funcionales según la Figura 7.

a) Gestión de eventos

Es la categoría encargada de gestionar ponderadamente los eventos que se dan en la red: alarmas, etc ... y formada también por todos los procesos de gestión necesarios para enfrentarse a esas ocurrencias: testeos, etc. Una vez obtenida la información, ayudará a los usuarios a comparar, contrastar y filtrar los datos, incorporando funciones de diagnóstico y de interpretación capaces de examinar información fragmentada, errónea o muy voluminosa.

b) Gestión de los recursos

Engloba las funciones que gestionan la construcción tanto física como lógica de la red: estado del software y hardware de la red, repuestos, chequeos de los equipos, etc.

c) Gestión de la configuración

A esta categoría le hago corresponder la gestión de recursos en cuanto a su configuración dentro una red activa, cambios, volcado de configuraciones predefinidas a los dispositivos en cualquier momento, etc.

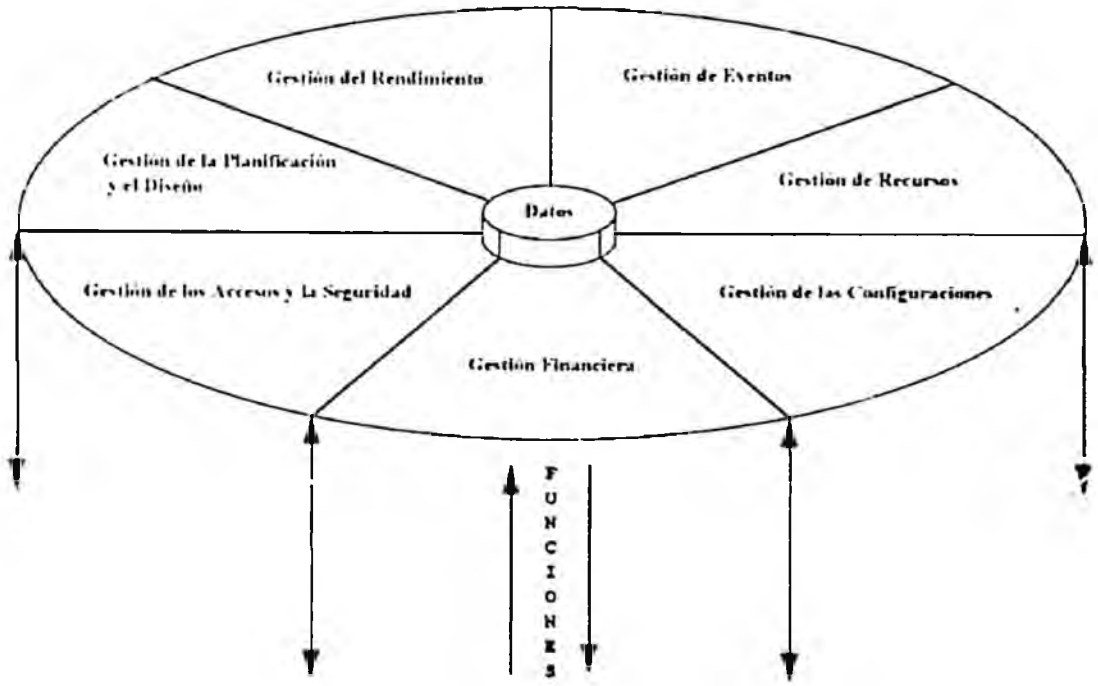

Fig. 7 Arquitectura funcional para la Gestión de Comunicaciones.

d) Gestión financiera

Se hace cargo de las funciones financieras relativas a la red como costes de

mantenimiento, facturación del tráfico generado a los correspondientes usuarios, etc. La recogida de datos respecto a los elementos de la red y su utilización es directa y automática.

e) Gestión de los accesos y de la seguridad

Monitoriza y controla la información obtenida sobre passwords, listas de control de acceso de clientes, registros de seguridad de elementos tales como puertos y su configuración de acceso disponibles para pruebas, facilidades de cifrado, etc.

Esta categoría regula a quién se le permite hacer qué cosas con la red y cuándo. No es necesario que ella misma aporte las funciones de seguridad pero si gestionará su implementación, siendo necesario que se complemente con una gestión apropiada de la seguridad incorporada en los recursos.

f) Gestión de la planificación y diseño

Es la serie de funciones necesarias para planificar el crecimiento de la red, con la posibilidad de estructurar adecuadamente los recursos, satisfaciendo requisitos combinados de costes y diseño. Opcionalmente también agrupa las funciones relacionadas con rutas alternativas de los datos, carga de la red, estrategias alternativas en caso de caídas de nodos, etc.

g) Gestión del rendimiento

Las funciones de esta categoría aseguran que la red es capaz de responder en un tiempo óptimo, factores de utilización, etc

Ayuda a identificar posibles "cuellos de botella" en las operaciones de red y a evaluar la carga de trabajo que soportan los elementos en un momento dado, así como a predecir cómo responderá la red en condiciones de cargas más elevadas, con el objeto de mantener el rendimiento de la misma con un nivel aceptable. Esto se consigue principalmente monitorizando el tráfico que se transfiere entre los elementos de la red y comparando las tasas de utilización reales con los límites definidos por el usuario.

La dificultad reside en la codificación de medidas de rendimiento en los protocolos de gestión, puesto que el rendimiento viene determinado por una serie de factores interrelacionados, como la velocidad de los enlaces de red, el tipo de hardware utilizado para el funcionamiento de redes, el tipo de servidores y sistema operativo empleados, así como el tipo de aplicaciones que se están ejecutando

3.1.2. Síntesis del componente estructural en una red WAN.

En términos generales se puede decir que la gestión de cualquier tipo de sistemas tiende a ser jerárquica por naturaleza. Puede tener más o menos niveles, y un mayor o menor número de divisiones dentro de cada nivel, pero lo que sí se mantiene como norma es que en cada nivel se deben llevar a cabo tareas de naturaleza diferente

A medida que nos acercamos a la cúspide de la pirámide, las percepciones deben transformarse y evolucionar hacia un mayor nivel de dirección y una menor participación en calidad de gestor. En la Figura 8 se resumen dichas diferencias

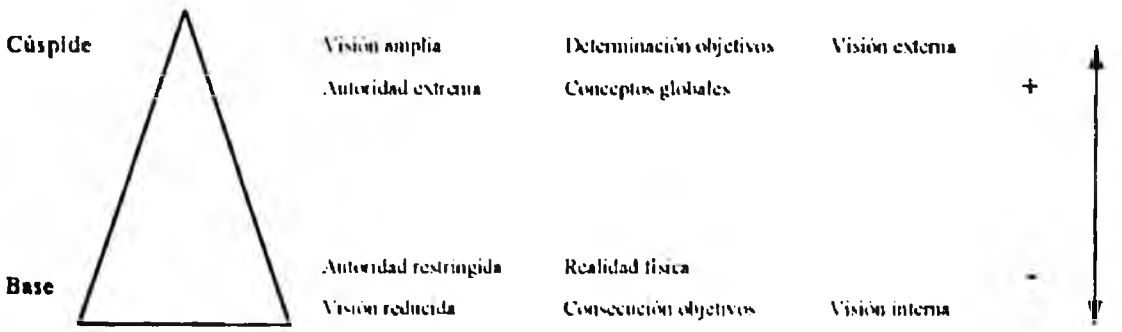

Fig. 8 Nivel de desarrollo de las percepciones y capacidades en una estructura jerárquica.

En este modelo, se mantiene dicha constante. Siguiendo por lo tanto esta linea, establezco cuatro niveles diferentes (Figura 9) atendiendo a los siguientes criterios:

a) Elementos de red

Son los dispositivos que necesitan gestión dentro de la Red de Comunicaciones. No solamente hago referencia o incluyo elementos fisicos sino también lógicos, como por ejemplo servicios de conmutación de paquetes, etc., que aún pudiendo estar formados por muchos elementos fisicos, constituyen desde el punto de vista del usuario un sólo elemento gestionable.

Las redes pueden en ocasiones ser recursivas. Esto vendria dado por la definición que he empleado para designar el concepto de elemento de red, recogiendo su consideración lógica Un ejemplo seria las recursiones que se desencadenarían estructuralmente, y con sucesivas pirámides, en un servicio de mensajeria X.400: servicios de funciones superiores son progresivamente construidos partiendo de otros más simples.

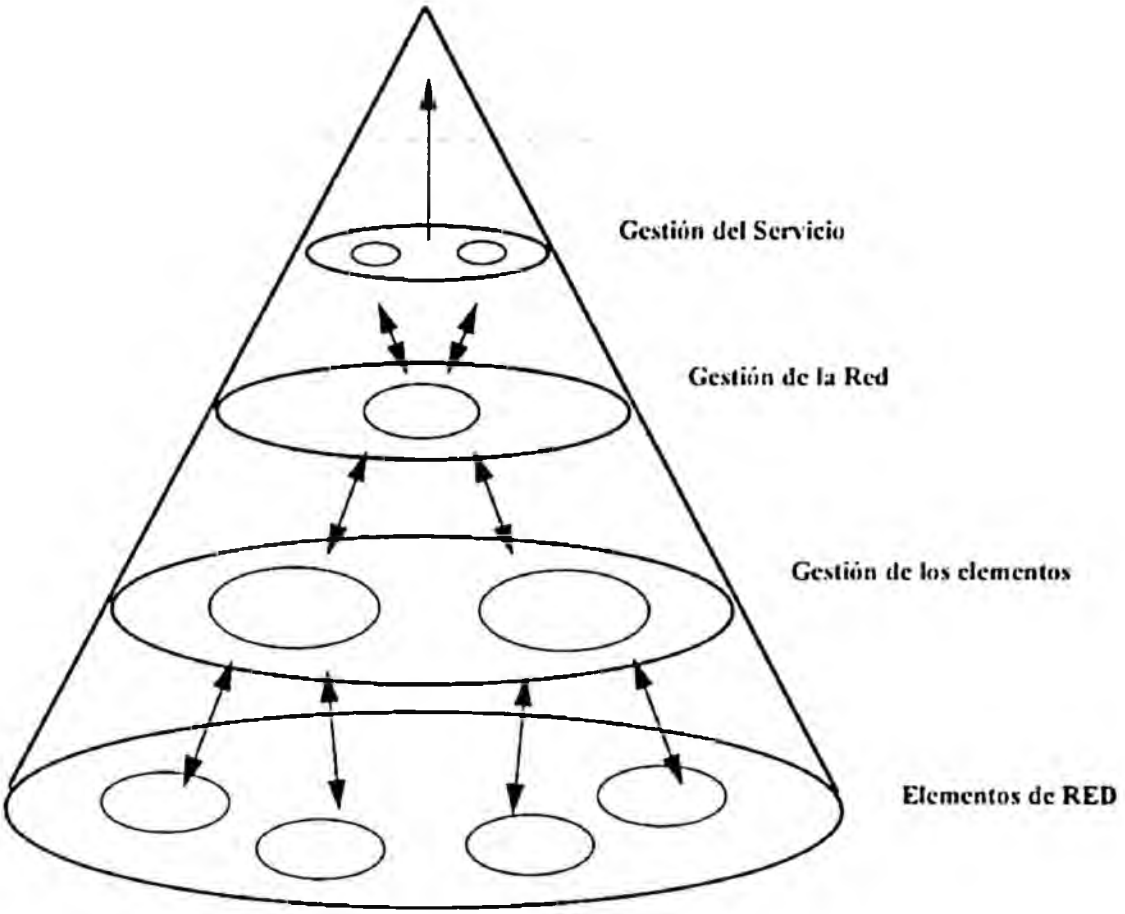

Fig. 9 Niveles dentro de la Gestión de Comunicaciones.

b) Gestión de elementos

Este nivel se encarga precisamente de gestionar los elementos del nivel inferior. Su complejidad puede ir desde un simple circuito impreso o programa software dentro del dispositivo, hasta en el caso más extremo, comprometer toda una estación de trabajo por completo, o una red local

c) Gestión de red

Este nivel controla e integra a un número indeterminado de gestores Es el primer nivel en el que se gestionan las relaciones entre elementos Aunque los gestores sólo se hacen

cargo de su especialidad concreta, existe un gestor global que controla cómo se está trabajando a lo largo de toda la red.

d) Gestión del servicio

Esta nivel de la jerarquía gestiona los servicios soportados por la red. Las aplicaciones que se sirven de la red, bien sea con transmisión de voz, datos, imagen o sonido, esperan que el sistema de comunicaciones les prevea de una serie de servicios. Este nivel lo aislo de los detalles concretos de la red y lo asocio más bien con sus funciones generales. Un gestor principal delega en sus gestores de nivel inferior para que cuiden de los detalles del dia a dia, mientras que él es responsable de asegurar la calidad en sus productos, en la forma apropiada Este nivel por lo tanto, también se relaciona fuertemente con otros sistemas fuera de la red

3.1.2.1. Estructuración jerárquica de la gestión de red.

Según el componente estructural de la arquitectura que he desarrollado en el apartado anterior, el crecimiento de las redes puede enmarcarse adecuadamente siguiendo unas relaciones jerárquicas Sin embargo, el tamaño creciente de las redes hace que su gestión también sea cada vez más difícil. A pesar de ello, los sistemas de gestión de red actuales continúan en su gran mayoría con una arquitectura plana agente-gestor, en un enfoque totalmente centralizado donde la mayor parte de la carga la soporta la estación de gestión central

Las redes evolucionan y las tareas de gestión adquieren mayor complejidad,

convirtiéndose en necesaria la distribución de esta carga. De hecho, SNMPv2 ha pretendido evolucionar también en este sentido, incluyendo la posibilidad de comunicación entre gestores.

Estas dos formas diferentes de entender la gestión de un sistema, que difieren básicamente en la distribución o no del control y de la inteligencia entre las distintas entidades de gestión, no son excluyentes. Por el contrario, deben coexistir adecuadamente hasta lograr el nivel apropiado de colaboración mutua

En un sistema centralizado de gestión, una única entidad recolecta y procesa ella sola todos los datos procedentes de la red. A intervalos regulares suele comprobar mediante sondeo el estado de los dispositivos, solicita estadísticas que le llegan en forma de enormes tablas para su posterior proceso, etc. Y también suele ocurrir que en periodos donde confluyen varios problemas a la vez (caídas de enlaces...), la gestión centralizada debe incrementar sus peticiones de información, precisamente en un momento en el que el sistema en general está menos capacitado para poder hacerlo. Esto conlleva pérdidas de información y una no definición exacta del estado de la red, justo cuando más se necesita una respuesta rápida y fiable. Las aplicaciones de gestión se comportan así peor, cuando mejor lo deberían hacer, degradándose el nivel de calidad.

Esta forma centralizada de incorporar los sistemas de gestión se deriva de los entornos de red tradicionales, donde los dispositivos solamente disponían de recursos para ejecutar programas más o menos sencillos, desarrollar funciones simples y donde las organizaciones podían disponer relativamente de todos los recursos humanos necesarios

Sin embargo, el entorno de las comunicaciones se ha ido trasformando con sistemas complejos, heterogéneos y distribuidos, con elementos que incorporan una significativa capacidad de proceso propio, y con una tendencia general en las empresas de contención en politicas de personal.

Este incremento en la inteligencia de los dispositivos se empleará para incluir agentes distribuidos con posibilidades de cálculo autónomo, y de esta forma, poder preprocesar y elaborar la información realizando su propia gestión local, con anterioridad a la transferencia de información a la estación de gestión central

La gestión descentralizada no elimina responsabilidades sino que las reparte. Consiste en delegar para beneficiarse de un mayor nivel de seguridad y un descenso de la presión del centro de control central, persiguiendo en última instancia, una mayor eficiencia y calidad global

3.1.2.2. Elaboración de una métrica para determinar el grado de gestión descentralizada adecuado.

La distribución en la gestión se expandirá tanto en el espacio como en el tiempo. En el espacio por distribuirse diferentes dispositivos o productos de red, y en el tiempo por poder abarcar franjas horarias diferentes. Esta visión bien entendida no es excluyente sino complementaria No pretende competir sino sumar esfuerzos.

Para determinar por lo tanto, si las aplicaciones de gestión de red en un entorno concreto deberian distribuirse, hay que estudiar qué parámetros son los esenciales a pesar de ser

implícitos, invisibles y de difícil extracción. Dejando de lado aspectos obvios relativos a la seguridad, como puntos clave se han podido identificar:

a) Necesidad de inteligencia, control y proceso distribuido.

Si esta característica la ubicamos dentro de una escala, iría desde una baja necesidad a una alta descentralización. Un aplicación que requiera decisiones rápidas basándose en información local, necesitará un control e inteligencia descentralizados. Aplicaciones que emplean una gran cantidad de datos también pueden encontrarlo ventajoso, aunque no siempre sea necesario.

b) Frecuencia en el muestreo.

La necesidad de proximidad a la fuente de información y la frecuencia en su muestreo pueden aconsejar acciones locales.

c) Equilibrio entre el caudal de la red y la cantidad de información de gestión.

En un extremo de la escala, la red dispone de suficiente capacidad como para no preocuparse del ancho de banda que consume su gestión. En el otro extremo estarán aquellas aplicaciones que podrían llegar a saturar enlaces de un caudal escaso.

d) Necesidad de un diálogo frecuente y semánticamente rico, entre agentes y gestores.

Los volcados de diagnósticos, el acceso constante a las MIB, etc., son factores que también condicionan el irse o no hacia un extremo de esta escala que mide la necesidad de descentralización.

Con este apartado he pretendido introducir otro elemento a considerar dentro del componente estructural de la arquitectura para la Gestion de Comunicaciones: la propia vertebración del software de las aplicaciones de gestión de la red. De igual forma que no siempre es necesario descentralizar la gestión de red, tampoco es menos cierto que a veces se tiene que considerar seriamente esta posibilidad siguiendo una estructura jerárquica en diferentes niveles de distribución.

3.1.3. Diseño del componente interface en la Gestión de Comunicaciones.

Todas las funciones, niveles y criterios que he estructurado tanto en el diseño de la arquitectura funcional como en el del componente estructural de una red de gestión, necesitan intercomunicarse de una forma también estructurada. Esta estructuración en niveles o jerarquías, se completará con métodos estructurados para compartir la información e interactuar entre si. Además, una red no se puede mantener aislada de otras funciones y niveles propios de aquellas actividades diferentes a la Gestión de la Red de Comunicaciones, por lo que el flujo de información y relaciones se expande en horizontal hacia otras pirámides.

El componente interface de la arquitectura está integrado por dos partes, dependiendo de que su naturaleza sea técnica o que por el contrario, encontrándose alejado de este plano, se considere de naturaleza más abstracta.

La parte técnica que hace de interface en la arquitectura, no es más que una familia de protocolos de comunicación, primitivas entre niveles para usarse tanto dentro de la propia arquitectura como con otras arquitecturas, APIs, etc. Los protocolos no necesitan mayor explicación al ser algo estándar en el área de la Telecomunicaciones. Mencionar si cabe el auge y desarrollo que está teniendo SNMP, a pesar de sus limitaciones.

En cuanto a la parte intangible que forma los interfaces internos de la propia arquitectura, y que sirve para relacionarse con otras externas, son pautas de actuación y comportamiento ante las relaciones que se dan entre los procesos incluidos en la Gestión de Red, y englobados dentro del flujo de información de la empresa

Como caso práctico, cuando hay que afrontar una ampliación en una red WAN, se ven involucrados tanto el componente funcional como el estructural de la arquitectura diseñada, pero también es necesario establecer una serie de relaciones interdepartamentales y seguir unas pautas de comportamiento que conlleva una forma de hacer las cosas, etc., teniendo como objetivo el llevar a buen término dicha modificación en la red global, con unos criterios de calidad.

Estas relaciones entre los elementos con responsabilidades y funciones diferentes dentro de la empresa, para conseguir un objetivo es la segunda parte del componente interface. Hoy por hoy, en muchas compañías de Telecomunicaciones sería preciso una labor de reingeniería considerable para determinar estos procesos y su relación dentro de su propio ciclo empresarial.

3.1.3.1. Aproximación a los procesos de red.

En una aproximación sencilla a estos procesos de red se identifican las siguientes variables dentro de la arquitectura: Planificación, Implantación y Operación de Red.

a) Planificación de Red.

Afecta al nivel de Elementos de Red, Gestión de los elementos y Gestión de la Red dentro de la Gestión de Comunicaciones (Figura 9).

Permite elaborar un marco estable para la realización de cambios sobre la red al prever la asignación de recursos y generar planes de trabajo, que se utilizarán en el proceso de implantación. Es un proceso que tiene por objetivo adecuar la capacidad ofrecida por la red a la que demandan los clientes, concretándose en las siguientes actividades:

a.1.) Planificación de la Topología de la Red.

Tomando como entradas el Plan de Negocio, las previsiones de Marketing, la topología actual y sin olvidar factores económicos, se busca la optimización de la Topología de forma que el coste esté dentro del presupuesto del Plan de Negocio , al mismo tiempo que cumple los requisitos de disponibilidad y capacidad ofrecida.

a.2.) Planes estratégicos de la Red.

Planifica los cambios a introducir en la red, a partir de la estrategia de la empresa reflejada en el Plan de Negocio y en los nuevos Servicios acordados en el Plan de Lanzamiento. Dentro de estas actividades se estiman los recursos necesarios a utilizar, convirtiendo las previsiones en la cantidad de equipo que se va a instalar, el espacio y

necesidades de equipamiento de locales técnicos, fechas previstas de implantación y duración de los proyectos

a.3.) Supervisión de la adecuación de la Red.

Lleva a cabo una supervisión de la red actual vigilando la definición y el grado de utilización de los diferentes equipos a partir de los datos de las mediciones reales. Se trata de confrontar los recursos libres con los que se cuenta en cada nodo, con la demanda real que existe

b) Implantación.

Dentro de la Gestión de Comunicaciones, afecta a los niveles de Elementos de Red y Gestión de los elementos (Figura 9)

Este proceso tiene como entrada la planificación de actividades a realizar sobre la red, y es responsable de su correcta ejecución.

c) Operación de Red.

Dentro de la Gestión de Comunicaciones afecta a los 4 niveles Elementos de Red, Gestión de los elementos, Gestión de la Red y Gestión del Servicio (Figura 9)

Los procesos dentro de la Operación de Red podrán también relacionarse directamente con las áreas de funcionalidad definidas en la arquitectura: Gestión de Fallos, Gestión de Recursos, Gestión de Eventos, Gestión de Prestaciones o Rendimiento, Gestión de Configuración y Gestión de los Accesos y Seguridad.

Con este componente de la arquitectura se abren futuros trabajos de investigación que sirvan para sintetizar procesos y aporten modelos de relación basados en la presente arquitectura para la Gestión de Comunicaciones en un entorno WAN generalizado. Una vez establecidos los procedimientos básicos, el formalizar sus relaciones y dependencias sería sin duda una vía de investigación con una importancia y aceptación positiva en este dominio, máxime cuando un número cada vez mayor de clientes plantea la exigencia de tener la Certificación ISO 9001 que afecta a todos los procesos y actividad de una empresa.

3.2. Síntesis de criterios fundamentales para ajustar el NAAP con las Plataformas de Gestión de Red.

Muchas veces al examinar un Centro de Control de una Red de Telecomunicaciones de cierto tamaño, visualmente se recibe un fuerte impacto al observar el gran número de computadores en funcionamiento y orientados expresamente a gestionar la red.

Este espectáculo, que en ocasiones arropa un gran componente de marketing nada despreciable, también manifiesta la dificultad y complejidad extrema en el control de un sistema activo y dinámico que pide ser controlado.

Las redes de comunicaciones sean grandes o pequeñas, de voz o de datos, con servicios básicos o de valor añadido, todas comparten características comunes: deben ser

planificadas, diseñadas, implementadas y mantenidas. Cada vez más se pretende automatizar estos procesos, a pesar de que la automatización de tareas aplicables a la gestión de una red ofrece solamente una solución parcial, puesto que el rendimiento de la gestión vendrá generalmente impuesto por los límites en el rendimiento de sus gestores, que son personas humanas. Es innegable que la mecanización aporta una enorme ayuda y elimina por supuesto, tiempos de ejecución sobre todo en tareas de mantenimiento, pero no elimina la demanda de una ayuda extra, de cierto nivel, en momentos críticos.

El conjunto formado por una plataforma de gestión junto con sus aplicaciones, aún constituyendo un muy adecuado cimiento sobre el que construir toda una gestión integrada, adolece de herramientas y principios de actuación elaborados que tengan en cuenta elementos y situaciones específicas propias de un entorno caracterizado principalmente por desarrollarse en tiempo real y con imperativos muy elevados de seguridad, rigor y exactitud en las actuaciones que en él se desencadenan.

De la simbiosis entre los programas y técnicas que hoy en día se emplean para dar soporte a los operadores de un Centro de Gestión, y las características especiales que aportaría este nivel específico y adaptado al entorno concreto en el que se tendría que desenvolver, nace el concepto ilustrado en la Figura 10.

Según este enfoque las tareas recogidas en dicha figura se agrupan en dos grandes campos:

a) Monitorización del estado de la red.

Son las aplicaciones de gestión estándar.

Implica recogida adecuada de información y capacidad para relacionarla, detectando y mostrando las anomalías existentes o previsibles.

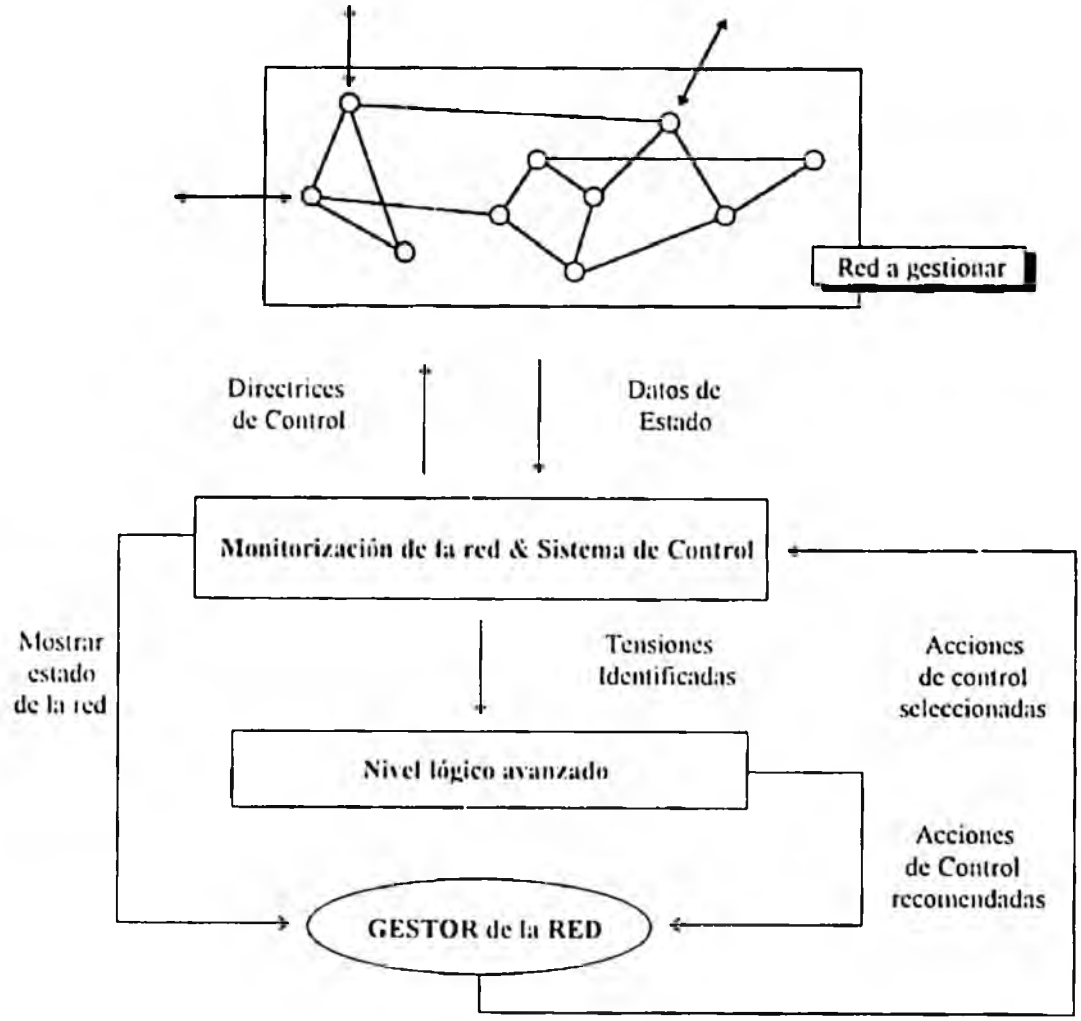

Fig. 10 Integración de un nivel lógico de apoyo a la toma de decisión en un esquema de Gestión de Red.

b) Selección de las acciones de control de red más apropiadas según sea el caso.

Este nivel a añadir a las aplicaciones de gestión, se ha sintetizado en esta Tesis y su denominación es **NAAP** (Nivel Avanzado de Apoyo a Plataformas de Gestión).

Se basa en métodos heuristicos combinados con la experiencia acumulada tras muchos años de experimentación y algoritmos procedurales. Este nivel añadido de apoyo a decisiones específicas de cierta complejidad, que complementa la arquitectura básica de un Sistema de Gestión de Red (Figura 1), aconseja y presenta al operador un grupo de acciones en vez de una gran cantidad de datos de alarma en bruto, sin elaboración ni proceso previo, guardando un compromiso adecuado dentro de un sistema altamente dinámico. Aunque los fallos en grandes redes de comunicaciones son inevitables, una rápida detección y la identificación de sus causas por el NAAP puede hacer que los sistemas de comunicaciones sean más robustos, y su funcionamiento también más fiable, incrementando asi el nivel de confianza en los servicios que proveen.

3.3. Adaptación de la funcionalidad aportada por el NAAP a la gestión de red en tiempo real.

Muchas veces las aplicaciones tipicas no contemplan el dominio en su conjunto sino que intentan solucionar problemas muy específicos sin valorar la totalidad de los estímulos que debe manejar. Así por ejemplo, en todo sistema de gestión de red existe un cuello de botella añadido que es el reconocimiento y diagnóstico de problemas en tiempo real, al que el NAAP puede poner ciertas cotas con el fin de limitar su impacto sobre el gestor de la red.

Los procesos de cálculo en sistemas de tiempo real deben satisfacer correctamente tanto

los criterios habituales de lógica en cuanto a su programación, como los aspectos específicos impuestos por su restricción en el tiempo. Cualquier deficiencia en satisfacer uno de ellos produciría un resultado inaceptable. Además, aparte del imperativo de una integración pacífica del NAAP con la plataforma y el resto de aplicaciones de gestión de red que corren sobre ella, satisface otra serie de funciones, como son:

a) Mantenerse en equilibrio con el flujo de alarmas asíncronas.

La supervisión de una red de telecomunicaciones se lleva generalmente desde un centro de control. Los eventos de excepción que ocurren en la red se reportan al centro de control a través de la propia red como intermediaria. Estos eventos deben ser interpretados por operadores humanos para detectar y diagnosticar problemas. En este contexto, un problema es cualquier situación anormal lo suficientemente seria como para incomodar, impedir la comunicación entre los componentes de la red. Según esta apreciación, el NAAP gestiona y relaciona eventos de todo tipo.

a.1.) Correlación de eventos.

Un simple evento no es significativo. Una situación anormal siempre genera un gran número de eventos, conteniendo cada uno una pequeña pieza de información. El análisis de la situación se hará por un proceso de razonamiento integrando diversos eventos. A primera vista, la correlación de eventos es directa: los eventos reportados solamente necesitan ser divididos o clasificados en grupos de componentes, la secuencia de eventos se comparará con la secuencia estándar del problema y esto nos llevará a concluir el problema.

Sin embargo, este enfoque no se puede considerar del todo completo porque también

hay que considerar la correlación tanto en el tiempo como en el espacio, así como los eventos redundantes.

a.1.1.) Correlación en el tiempo.

Los eventos relacionados con una situación dada pueden estar dispersos en un intervalo de tiempo que puede ser grande: horas e incluso días para algunos problemas de degradación.

También, el ritmo o la secuencia en que los eventos aparecen puede tener importancia y es que por ejemplo, la fluctuación de un módem durante una hora no es seria, pero 10 veces en un minuto sí.

a.1.2.) Correlación en el espacio.

Una situación anormal puede inducir eventos en varios componentes de la red: en el propio componente, en componentes jerárquicos y en los componentes interconexionados a través de la red. Un problema puede ser detectado indirectamente, por eventos reportados por otros.

Para cubrir todo esto, sobre todo la correlación en el espacio, el NAAP aporta un conocimiento estructural sobre la red, incluyendo sus componentes y relaciones entre ellos, y sobre los eventos que pueden deducirse de estos componentes.

a.2.) Eventos redundantes.

Muchos eventos son consecuencia directa de otros y no dan información adicional. Los eventos pueden ser reportados (a través de la red) después de que el problema ha sido arreglado. Estos eventos solamente distraen al operador y deben ser enmascarados.

El NAAP es capaz de procesar mensajes de alarmas más rápidamente que la media a la que son generados por los elementos de la red. Además se recuperará rápidamente de periodos cortos e intensos de un gran volumen de alarmas asociados a caídas enteras de un nodo, enlace, o situaciones catastróficas.

b) Mantener un modelo exacto de la configuración de la red.

El conocimiento de la topología de la red a todos los niveles, también de configuraciones específicas de dispositivos, es crítica para el diagnóstico. Debido a que el almacenamiento de datos y su los requisitos de su actualización pueden ser prohibitivos para redes complejas, el compromiso entre el refresco de datos y el tiempo de acceso es considerado cuidadosamente por el NAAP.

c) Razonamiento con datos incompletos.

Los problemas de red siempre comienzan y se desarrollan con datos incompletos. La información se va recopilando progresivamente a medida que se van produciendo más eventos. Muchas veces solamente se sacan hipótesis sobre una situación cuando llegan nuevos eventos dando más información teniendo que reconsiderar o redefinir nuestras hipótesis anteriores. Otras, la ausencia de eventos puede ser tan significativa como la llegada de ellos, y debe ser interpretada como tal. Por ejemplo, nos llegan eventos que nos pueden hacer sospechar la degradación de un componente. Poco después, nos llegarán otra serie de eventos confirmando dicha funcionamiento anómalo. Si no se reportara ningún evento adicional, el NAAP decide si es adecuado descartar o no la presunción de degradación anterior.

Existe una relación entre los tipos de problemas y los patrones de las alarmas que se generan en la red. Las alarmas normalmente asociadas con un problema, se pueden perder por diferentes razones. En estos casos el NAAP es capaz de reconocer que los datos se pueden haber perdido y buscar evidencias que lo corroboren.

d) Solucionar los problemas a tiempo.

Normalmente existen unos factores que por su importancia, ante cualquier defecto en su funcionamiento u operatoria, inciden negativamente en las estadísticas de rendimiento global de una red. Por ejemplo, la pérdida de un circuito crítico puede causar serios daños al producto o a la reputación de una empresa. Así pues, el NAAP se enfrenta con la detección de fallos, mantenimiento, diagnóstico y restauración del servicio

A primera vista, la solución de problemas de red es bastante similar a otras aplicaciones en el entorno industrial. Sin embargo, en este dominio estimo que presenta algunas características que hacen algo especial su diseño, como son: la integración de conocimiento estructural y heurístico, los mecanismos de inferencia eficientes bajo tiempo real, la revisión de las conclusiones con el tiempo, y la coexistencia de varios problemas de diferente naturaleza simultáneamente

En estos sistemas aplicados a grandes redes, el factor tiempo juega un papel importante en varios frentes que no puede ser ignorado.

De hecho, la apariencia y severidad de los problemas pueden cambiar por muchas causas. Problemas que aparentemente parecen difíciles, espontáneamente desaparecen.

Problemas intermitentes pasan a ser severos. Problemas que están ahi desde hace mucho tiempo, crónicos, pueden emerger. El NAAP reconoce estos cambios y les asigna prioridades.

e) Arreglar los problemas según su severidad.

Los problemas se deben tratar dependiendo de su severidad para centrar la atención en aquellos que más afecten al servicio. El NAAP es capaz de trabajar guiado por objetivos.

Una red generalmente suele tener varios problemas pendientes y la correspondencia de eventos generados por cada uno de ellos se mezclan. Algunas situaciones anormales son más criticas, y tienen que pasar a un primer plano. Al estar llegando la información continuamente, el razonamiento sobre un problema alcanza diversas etapas, discontinuas en el tiempo e interrumpidas por los eventos generados por la red, teniendo que cambiar frecuentemente el foco del razonamiento.

En este punto, el mecanismo de razonamiento almacena todas las deducciones hechas hasta ahora para permitir que luego continúe el razonamiento apropiadamente.

f) Filtrar efectos colaterales.

Algunas topologías complicadas manifiestan problemas con muchos efectos colaterales, ninguno de los cuales existiría por si mismo. El NAAP no pierde el tiempo arreglando el problema erróneo, sino que tiene capacidad de discernimiento para buscar el origen de tales efectos secundarios

g) Suspender o resumir el diagnóstico de los problemas cuando sea apropiado.

Debido a que el proceso de diagnóstico tiene pausas ocasionales mientras está esperando resultados, en cada pausa de éstas, el NAAP puede reemplazar el problema actual con otro nuevo más importante.

h) Considerar cambiante la sospecha de un fallo según probabilidades.

Los expertos son capaces de expresar y razonar, empleando alguna medida de probabilidad, que un componente dado puede haber causado un problema observado. Ellos actualizan las medidas y probabilidades con las que trabajan según está disponible nueva información proveniente de alarmas y tests de resultados Aunque no siempre se aplica formalmente, el concepto de probabilidad se emplea en el NAAP para guiar la búsqueda de problemas.

i) Seleccionar el test más barato y que más información aporte.

Después de discernir cuál es el problema más grave a solucionar en un momento dado, la habilidad más importante a desarrollar por el NAAP es la de seleccionar el test o acción a desarrollar para recabar más información o dar una solución al problema: duración, alcance, posibilidad de interrumpir el servicio, costes y posibilidad de reconfiguración...

j) Automatizar lo más posible los test de diagnóstico.

Es mucho más valioso un sistema que puede realizar un diagnóstico sin la intervención humana, que otro que necesite que un operador esté disponible.

k) Interpretar los resultados del test para establecer el diagnóstico.

El NAAP hace un uso óptimo de la información. El requisito más restrictivo de un sistema basado en tiempo real es que está orientado a los datos. Responderá ráp ida y apropiadamente a los cambios en los procesos que está monitorizando, o bien a los datos que otros mismos procesos le hacen llegar. El sistema está guiado por interrupciones para procesar cada nueva alarma según la recibe.

3.4. Claves para la representación e implementación algorítmica para la gestión de fallos del NAAP.

Para realizar un acercamiento a una representación exacta del conocimiento, hay que considerar en primer lugar, precisamente los tipos de conocimiento con los que trabaja el NAAP Los clasifico de la siguiente manera:

a) **Conocimiento estructural:** topologia de red.

b) **Deducciones:** tipos de datos creados y manipulados durante el razonamiento.

c) **Conocimiento sobre la detección de problemas:** cómo interpretar los eventos de la red, cómo reconocer los problemas y cómo enfrentarse a ellos.

3.4.1. Conocimiento estructural.

En este parte, se emplea una forma de representación siguiendo el formalismo de objetos

estructurados, por ser un método de diseño de software de mucho más fácil mantenimiento que otros, y porque para añadir requisitos o funcionalidades simplemente basta con incluir nuevos objetos y establecer sus relaciones con los ya existentes, resultando al final que el impacto en el trabajo ya realizado es mínimo.

Cada tipo de objeto de la red y cada evento se representa por una clase y por una jerarquía de instancias de esa clase. Una clase hija se considera como una especialización de la del padre, heredando sus características, pudiendo cambiarlas o añadir más si así fuera necesario

En su implementación, existe una cierta tensión entre el deseo de expresar el conocimiento sobre el modelo de red de una forma general y declarativa, y por otra la necesidad de representar la heurística, típicamente expresada en reglas, empleada para el diagnóstico

Se debe adquirir un compromiso equilibrado en el uso de paradigmas de programación orientados a objetos para asociar código procedural a estructuras de datos, y programación basada en reglas para el conocimiento heurístico sobre la gestión de redes en tiempo real

Las estructuras de datos siempre describen objetos del mundo real en términos de sus atributos, valores de esos atributos y el comportamiento de estos objetos en respuesta a diferentes estímulos. Estas estructuras definidas para clase de objetos sirven de plantillas para construir instancias específicas de estos objetos durante la ejecución del programa

Además, una instancia de un objeto puede heredar valores de atributos y código procedural de su clase, por lo que este mecanismo de herencia permite especificar un modelo general de red que pueda ser instanciado con una configuración particular de red, dotándolo de un potencial especial para simulaciones y estudio del comportamiento.

Todo esto, unido a que el imperativo de la modularidad en su programación hace que el trabajo de mantener un modelo de red consistente sea más fácil, lo convierte en una opción excelente para construir un modelo de red

Así, el proceso para modelar una red es el siguiente:

a) Seleccionar el modelo a aplicar.

El paradigma de representación es el Modelo Orientado a Objetos. Los objetos son organizados en una jerarquía de clases.

b) Identificar los recursos que necesitan convertirse a objetos, para su posterior gestión.

Normalmente suele ser fácil la elección de qué debe constituirse como un objeto, pero otras veces no está tan claro. Se modela como objeto, tanto cada recurso que se emplee en la comunicación, y que o bien tiene que ser descrito para monitorización directa o bien ejerce cierta influencia sobre otro objeto monitorizable, así como los eventos de red.

Por lo tanto, dentro del conocimiento estructural existen dos tipos de objetos: componentes de red y eventos de red.

c) Identificar los atributos de los objetos gestionados.

Solamente se incluyen aquellas características que son útiles y relevantes para la actividad de gestión. El color de un módem forma parte de la descripción completa del recurso, pero no es necesaria para su gestión.

d) Identificar las relaciones entre los objetos gestionados.

Relaciones de herencia, pertenencia, conectividad...

Las propiedades de los componentes de la red pueden representar relaciones entre objetos, como la relación componente/subcomponente o componentes físicamente interconectados, o bien representan situaciones de los objetos, como el estado de un dispositivo.

Las propiedades de los eventos sirven por un lado para situarlos en el tiempo y en el espacio, como por ejemplo momento de recepción o enviado por, y por otro lado para definir las características de su tratamiento: intervalos, límites...

e) Describir el comportamiento del objeto: operaciones que se pueden hacer sobre él y sus entradas y salidas de datos.

La especificación de un objeto incluye la descripción de los métodos que pueden interactuar con él. En el modelo de un objeto, los métodos podrán por ejemplo sondear (un módem...), reiniciar (una tarjeta de alta velocidad en nodo comunicaciones...), etc.

f) Formalizar toda la información anterior.

Toda la información sobre la modelización del objeto se debe presentar formalmente.

3.4.2. Deducciones.

Las deducciones las agrupo en 3 tipos básicos: síntomas, hipótesis o resultados.

a) Síntomas.

Representa un evento o conjunto de eventos que pueden ser requeridos para el manejo de acciones futuras. Los síntomas y eventos difieren en su utilización y en su interpretación temporal. Un evento ocurre en un momento específico y luego desaparece. Un síntoma se graba para su utilización posterior en el proceso de razonamiento. Los síntomas se dan a lo largo del tiempo y por ello tienen un comienzo y un final. Esto permite a los síntomas representar una secuencia de eventos de un mismo tipo ocurridos durante un intervalo de tiempo.

b) Hipótesis o resultados

Esta distinción se da por su representación lógica. Una hipótesis es una afirmación sobre un objeto de la red que puede ser verdadera o no, mientras que un resultado es una afirmación. Las hipótesis las introduzco para manejar razonamientos posibles.

De todas formas, un evento y su síntoma correspondiente pueden ser interpretados como diferentes vistas de un mismo concepto. Lo mismo sirve para las hipótesis y los resultados. pueden compartir propiedades idénticas. Esto nos lleva a que la utilización de jerarquías puras produce una posible duplicación del conocimiento, inconveniente no deseado y que se soluciona fundiendo en una sólo objeto las diferentes vistas del concepto.

Las deducciones están unidas por relaciones N a M (deducciones empleadas en/deducidas de). Las deducciones relativas a una situación anormal forman una red que representa nuestro conocimiento sobre la situación.

3.4.3. Conocimiento sobre la detección de problemas y diagnóstico.

En este apartado se podria haber utilizado el concepto de razonamiento en profundidad: el sistema está representado por un modelo profundo que integra la representación de la estructura del sistema con sus componentes y relaciones entre ellos, y por la descripción funcional de cada dispositivo. El razonamiento se llevaría a cabo simulando el funcionamiento del sistema a partir de este modelo. Sin embargo, puesto que el conocimiento sobre las redes es más heuristico y está muy fragmentado entre los diferentes expertos de cada área especifica, la simulación es ineficiente , por ser incompleta El razonamiento basado en modelos sólo podrá ser utilizado a un nivel muy elemental, como por ejemplo: "*si un nodo conmutador se cae, todos los terminales conectados a él no estarán disponibles*". Esta naturaleza heuristica podria llevarnos de una manera natural a la representación basada en reglas La reglas deben estar bien integradas en la estructura de objetos para acceder fácilmente a ellos, y su selección y aplicación tiene que ser eficiente para enfrentarse a la limitación del trabajo en tiempo real.

Una alternativa a la simulación es representar el conocimiento del diagnóstico y detección empleando técnicas procedurales unidas a los objetos. Las condiciones o

disparadores de cada evento se producirían según el tipo de objeto al que pertenecieran. Sin embargo, esta técnica no resulta lo suficientemente flexible.

La técnica de representación que aporto combina las ventajas de las reglas y los *"demonios"* Por un lado, existe un mapa heuristico de patrones de alarmas (Figura 11) relacionado con problemas, para efectuar un primer análisis y clasificación del síntoma.

Si se ha producido un evento relacionado con un MÓDEM que pertenece a un enlace Punto-a-Punto, y además ha sido reportado por el módem vecino-B, clasifico en primera instancia el problema como una incidencia del enlace.

```
Objeto MODEM.
    Posición: Nodo red.Armario.Chásis.Posición.

    Objeto Punto-a-Punto.
        if ?evento es reportado por el módem vecino-B then ?Conexión.
```

Fig. 11 Pseudo-código de un mapa parcial de patrones de alarmas

Una regla de diagnóstico (Figura 12) está definida dentro de una clase de objeto. La definición de reglas tiene las siguientes propiedades:

a) Clase: la clase con la que está asociada la regla (Conexión).

b) Nombre: nombre de la regla (Regla_1).

c) Disparador: Especifica el concepto entero, los eventos de la red o las deducciones del sistema que pueden causar la aplicación de la regla (en el ejemplo, es el evento cambio del estado del enlace), además de las consecuencias intrínsecas al evento recibido, independientemente del disparo de las reglas (cambio en la representación física del enlace).

d) Entorno: Permite la declaración de variables locales a la regla, generalmente expresando las propiedades de los componentes de la red y las propiedades de los eventos.

e) Cuerpo: Generalmente tiene la forma de IF condición THEN acción

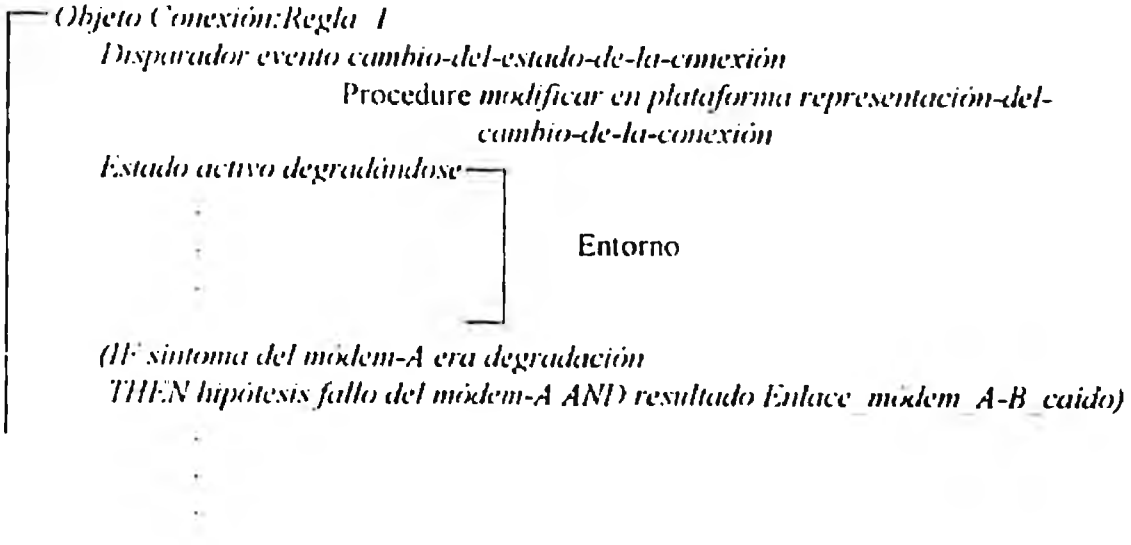

Fig. 12 Pseudo-código de una regla de diagnóstico

La regla R1 pertenece a la clase CONEXIÓN, se dispara por haberse reportado un evento de modificación en el estado de la conexión, y en la regla ya existía una variable

local que nos advertia del sintoma de degradación que se habia detectado en el módem-A, a pesar de estar aún activo. Se ejecuta la primera regla y obtenemos como resultado que el enlace entre el módem A-B está caído y como hipótesis a trabajar posteriormente que el módem-A tiene algún problema.

Todos los eventos que ocurren en la red se transforman al formalismo interno, orientado a objetos, determinando qué objetos de la red guardan relación con este nuevo objeto por la información asociada al evento. A los objetos seleccionados se les pasa un mensaje reportando el evento ocurrido, y en su recepción, cada objeto selecciona de sus reglas aquellas cuyo disparador y estado encaje con el evento recibido. Este mecanismo de inferencia restringe las actividades de solución a los objetos de la red que tienen que ver con el problema, manejando en consecuencia únicamente información relevante.

En este proceso final de inferencia también se implementa la posibilidad de revisión de la validez de las deducciones, debido a la acción del paso del tiempo. Estimar si una deducción puede ser revisada o no, y consecuentemente poder ser eliminada es un proceso que se podria implementar en la base de las reglas, pero esto creo que la inundaria con conocimiento de control y no conocimiento experto del dominio. Pienso que ambos tipos de conocimiento se deben separar para ganar en transparencia, por lo que una solución válida a este problema está en añadir estados a los disparadores como por ejemplo TIMEOUT estaria TIMEOUT si para un cierto intervalo no se ha empleado para derivar nuevas deducciones y ninguna deducción nacida de ella está todavia EN USO

Este mecanismo nos permite enfrentarnos con el problema del tiempo en el NAAP sin incrementar el tiempo requerido en la selección de reglas. Tiempo que si bien se va a ganar en su mayor parte con técnicas de implementación en codigo, también se puede limar a nuestro favor evitando el acceso a disco y a memoria virtual, guardando el conocimiento estructural, por naturaleza estático, en un área no dinámica, ubicando las deducciones en áreas donde no existan esperas debidas a "recogida de basura" del software...

3.5. Validación de la importancia de los objetivos en el NAAP.

Dada la limitación impuesta por la variable tiempo, se deben buscar algoritmos computacionalmente eficientes que logren respuestas óptimas en el mínimo tiempo posible, y este factor lo debe contemplar el NAAP

Esta circunstancia se complica enormemente en los sistemas de gestión de red por el flujo continuo y afluencia de nuevos datos que pueden provocar que el foco de atención se traslade a otro problema de mayor envergadura y repercusión Esto significa que se debe implementar algún mecanismo que determine qué inferencias son importantes y cuáles pueden ser pospuestas

Esta importancia se podría establecer de antemano o bien, dictaminarse dinámicamente según sean los problemas. Por ejemplo, *"mi interés o necesidad puede ser mayor en intentar saber qué sucede con los módem defectuosos que en analizar el nivel de ruido de los enlaces, a no ser que el enlace sea una línea de transmisión de 2M. (backbone) importante"*.

Para dar respuesta a esta situación cambiante en la búsqueda de metas, he desarrollado el método **CNOD** (Cuantificación de la Necesidad y su repercusión en los Objetivos basado en Lógica Difusa), para calcular la influencia de las necesidades sobre los recursos disponibles mediante Lógica Difusa.

El objetivo es aportar un medio de cuantificación de la necesidad que nos permita establecer una relación directa entre dichos requisitos o 'necesidades' y la idoneidad de unos posibles recursos disponibles, valorando cuantitativamente la influencia que ejercen las variables de entrada para realizar un refuerzo positivo (o negativo) sobre las variables de control

Sin embargo nada más intentar afrontar el problema, nos encontramos con la 1ª dificultad parametrizar algo tan intangible y vago como es la NECESIDAD que se tiene de algo. Seguidamente, nos toparíamos con un 2º problema: la relación entre nuestra NECESIDAD (ya convertida en un ente matemático con el que se puede operar) y el efecto proporcional ocasionado por ella en los recursos de los que disponemos.

3.5.1. Acotación del concepto de necesidad con referencia a los objetivos.

Para tratar con la necesidad emplearemos las 'variables lingüísticas', un artificio que intenta acercar la inferencia artificial a la humana y cuyo uso se debe a la lógica Difusa. Variables lingüísticas pueden ser 'casi alta', 'muy pequeño'... Son términos que los operadores humanos emplean habitualmente en los procesos de control.

Un operador de red habitualmente emplea expresiones como "Si la tasa de errores en un enlace es MUY ALTA, entonces disminuir en grado MÁXIMO la disponibilidad de dicho circuito", haciendo una descripción cualitativa del proceso empleando un lenguaje que incluye términos imprecisos.

"Tasa de errores MUY ALTA" y "disminución MÁXIMA" son sentencias lingüísticas representables mediante subconjuntos difusos, dentro de universos previamente definidos. Estos subconjuntos se usan para representar la NECESIDAD

La mayor dificultad en el diseño de un controlador basado en Lógica Difusa (CLF) se encuentra en la definición adecuada de las reglas de control y de los valores difusos asociados a las sentencias lingüísticas. El número de terminos o variables lingüísticas dependerá de la aplicación y de la "finura" de las reglas de control

3.5.2. Diseño de un método para cuantificar la necesidad y su repercusión en los objetivos: CNOD

A continuación se estructura la necesidad en gestionar la red, a través de una cuantificación de la necesidad.

3.5.2.1. Pautas y fundamentos del método CNOD

1º - Existe una característica denominada A de la cual se tiene necesidad, unida a un diagnóstico que afecta probabilísticamente a su disponibilidad. Esa característica A puede ser por ejemplo módem en funcionamiento, bajo nivel de ruido, baja tasa de errores, alta y constante velocidad en la transmisión o cualquier otra propiedad (ANTECEDENTE).

2º - Dependiendo de la necesidad de A y en la proporción generada por la probabilidad, efectuaremos un refuerzo positivo o negativo sobre la idoneidad del elemento Z para tal característica (CONSECUENTE).

Estos 2 principios constituyen la base para crear las reglas de control.

Además de estos principios se da que:

a) El grado de probabilidad del diagnóstico (realizado previamente por el NAAP) que afecta a la característica A que se desea, se va a acotar entre 0 y 10, siendo el valor 0 la probabilidad mínima posible o nula probabilidad, y el 10 la probabilidad máxima.

b) Por otro lado, se diseñan unas curvas de probabilidad comprendidas entre los valores 0 y 10 (son subconjuntos difusos) , que nos indican o dividen en diferentes zonas (etiquetas lingüísticas) la certeza en el diagnóstico. Estas zonas serán 7:

TOTALMENTE PRESCINDIBLE
NADA IMPORTANTE
POCO IMPORTANTE
IMPORTANTE
MUY IMPORTANTE
MÁXIMA IMPORTANCIA
IMPRESCINDIBLE

Estos términos lingüísticos vienen definidos por las siguientes ecuaciones

x: grado de probabilidad
y: grado de pertenencia

TOTALMENTE PRESCINDIBLE

$y = 1$, si $x = 0$
$y = 0$, si $x \neq 0$

NADA IMPORTANTE

x	0	1	2	3
y	1	0,9	0,3	0

POCO IMPORTANTE

x	0	1	2	3	4	5	6
y	0	0,1	0,5	1	0,5	0,1	0

IMPORTANTE

x	1	2	3	4	5	6	7	8	9
y	0	0,1	0,4	0,8	1	0,8	0,4	0,1	0

MUY IMPORTANTE

x	4	5	6	7	8	9	10
y	0	0,1	0,5	1	0,5	0,1	0

MÁXIMA IMPORTANCIA

x	7	8	9	10
y	0	0,3	0,9	1

IMPRESCINDIBLE

$y = 1$, si $x = 10$
$y = 0$, si $x \neq 10$

Las curvas asociadas a estos términos lingüísticos pueden ser representadas de la forma que se indica en la Figura 13.

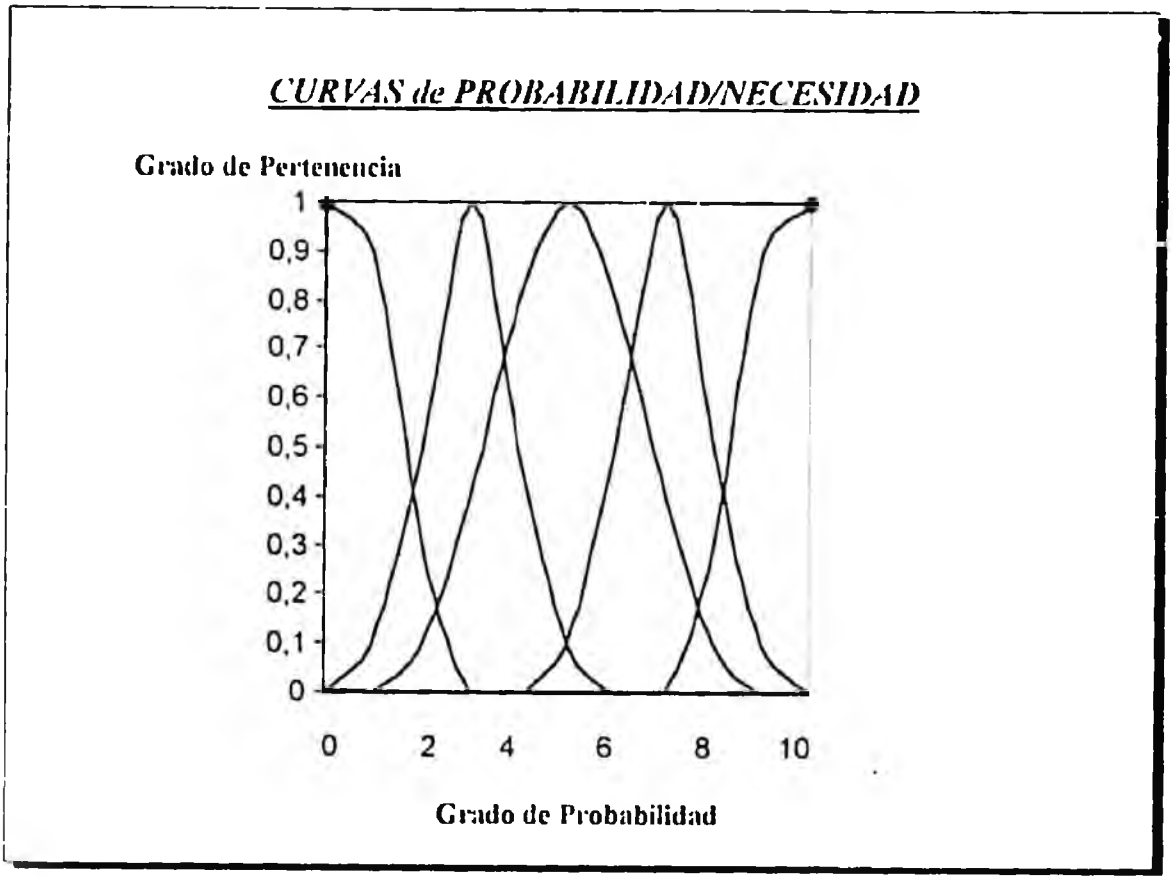

Fig. 13 Gráficas de las Curvas de Probabilidad

c) También se elaboran 7 términos lingüísticos para el refuerzo.

MÁXIMO
MUY ALTO
ALTO
MEDIO
NEGATIVO BAJO
NEGATIVO MUY BAJO
MÁXIMO NEGATIVO

MÁXIMO

y = 1, si x = 10

MUY ALTO

x	8	8,5	9	9,5	10
y	0,1	0,9	1	0,3	0

ALTO

x	6	6,5	7	7,5	8	8,5	9	9,5	10
y	0	0,1	0,2	0,5	1	0,5	0,2	0,1	0

MEDIO

x	5	5,5	6	6,5	7	7,5	8	8,5	9
y	0	0,1	0,2	0,5	1	0,5	0,2	0,1	0

Los términos negativo bajo, negativo muy bajo y máximo negativo son iguales que los términos alto, muy alto y máximo, pero con una influencia o refuerzo negativo.

Las funciones asociadas a los diferentes niveles de refuerzo, tienen de igual manera que en el caso de la probabilidad, su propia representación gráfica (Figura 14)

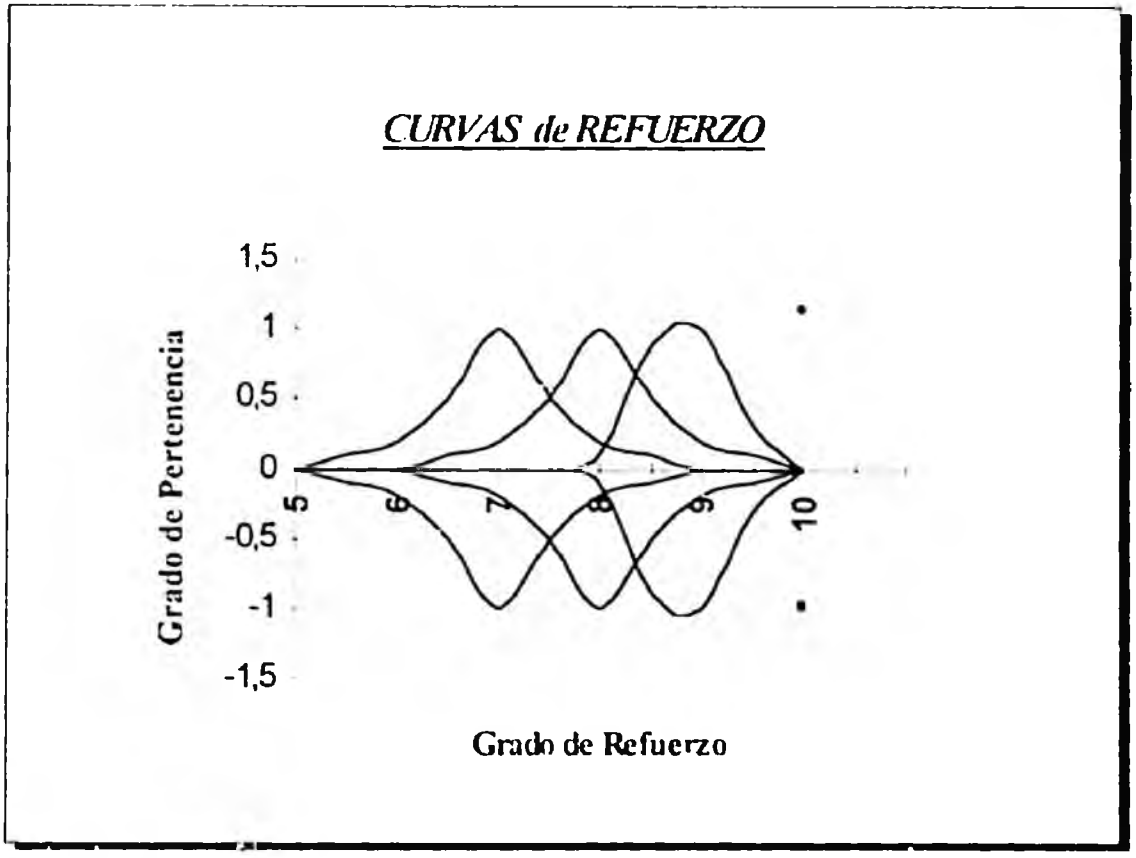

Fig. 14 Gráficas de las Curvas de Refuerzo.

Para ajustar la implementación del método, la distancia entre los elementos de cada subconjunto la divido por 2 con respecto a los de la necesidad, para que la forma de la curva no quede indefinida al ser los intervalos más pequeños.

3.5.2.2. Validación del método CNOD.

*a)**Premisa:** El CENTRO de OPERACIONES de RED dictamina que dentro de sus prioridades, el mantener los enlaces activos tiene una prioridad MUY IMPORTANTE.*

*b) **Datos de ENTRADA:** En un momento dado, entre la variedad de alarmas y datos de entrada que llegan dinámicamente a la consola del operador, aparece una "alarma" que el NAAP dictamina que es indicativa de un problema en un enlace, con una probabilidad IMPORTANTE (40%).*

*c) **Reglas de control: dada la premisa establecida en el punto a), se incorporan las siguientes reglas de control:***

Si existe un problema en un enlace con una probabilidad MÁXIMA,

hacer un refuerzo MÁXIMO sobre el recurso Z

Si existe un problema en un enlace con una probabilidad MUY IMPORTANTE,

hacer un refuerzo MUY ALTO sobre el recurso Z

Si existe un problema en un enlace con una probabilidad IMPORTANTE,

hacer un refuerzo MUY ALTO sobre el recurso Z

Si existe un problema en un enlace con una probabilidad POCO IMPORTANTE,

hacer un refuerzo ALTO sobre el recurso Z

En este caso las reglas realizan un refuerzo positivo sobre un recurso por ser adecuado su empleo para conseguir el objetivo; por el contrario, si no fuera apropiado, el refuerzo sería negativo.

d) Desarrollo.

La alarma que indica la existencia de *problemas o fallo en un enlace*, además de ser por sí mismo un dato de entrada a analizar, también debe considerarse como un elemento que influye activamente sobre la prioridad en el reparto o asignación de recursos que se haga para solventar los problemas, al considerar que el tener disponibles los enlaces es un elemento MUY IMPORTANTE dentro de las prioridades establecidas

Si al finalizar el diagnóstico se estuviera resolviendo otro problema con unos recursos cuyo refuerzo global calculado, bien directamente o como suma de refuerzos indirectos, fuera menor, se priorizará la búsqueda de una solución o al menos, el tratamiento, de la alarma de *fallo de enlace* en primer lugar, para posteriormente seguir con el siguiente problema de mayor importancia.

Ajuste sobre las curvas

El grado de pertenencia de la probabilidad de un problema en un enlace x activo (40%),

es de un 0,5 para la curva POCO IMPORTANTE y de un 0,8 para la IMPORTANTE, siendo 0 para el resto de las curvas.

Efecto proporcional

En la medida que el recurso z (siendo z cualquier medida, recurso, solución, etc.) es apropiado para mantener un enlace x activo, y teniendo en cuenta la probabilidad del diagnóstico, le aplico mi grado de necesidad sobre la característica "mantener un enlace x activo" recogidas en las reglas de control, obteniendo un valor final de refuerzo x sobre la idoneidad de z

En este punto por lo tanto, aplico el proceso de defuzzyficación mediante la expresión del Centro de Gravedad (Figura 15), consistente en la conversión de información difusa en concreta, puesto que una vez que tenemos un resultado final fruto de aplicar unas reglas de control, es necesario transformar los subconjuntos difusos obtenidos en valores o rangos de valores reales.

$$CDG = \frac{\sum_{j=1}^{n} u_A(x_j)\, x_j}{\sum_{j=1}^{n} u_A(x_j)}$$

Fig. 15 Expresión para el cálculo del Centro de Gravedad

Grado de necesidad: 9 (MUY IMPORTANTE)

*CDG (0,5 * (6*0 + 6,5*0,1 + 7*0,2 + 7,5*0,5 + 8*1 + 8,5*0,5 + ...*0,2 + 9,5*0,1 +*

*10 * 0) (0 · 0,1 · 0,2 · 0,5 · 1 · 0,5 · 0,2 · 0,1 · 0)) ·*

*· (0,8 * (8 *0,1 · 8,5*0,9 · 9*1 · 9,5*0,3 · 10*0) (0,1 · 0,9 · 1 · 0,3 · 0) =*

= 0,5 * 20,8 / 2,6 + 0,8 * 20,3 / 2,3 = 4 + 7,06 = 11,06

e) Conclusiones.

Efectúo un refuerzo de 11,06 sobre la idoneidad del recurso z para solventar el problema diagnosticado en un enlace con un 40% de probabilidad, teniendo en cuenta que se ha asignado una prioridad MUY IMPORTANTE a la necesidad de mantener los enlaces activos.

Esta característica es la primera ventaja respecto al comportamiento humano.

e.1) Es un mecanismo automático para la resolución de problemas, no viéndose influenciado por las habilidades ni inclinaciones humanas como pueden ser la tendencia a terminar el trabajo comenzado, el no percatarse de situaciones a veces no evidentes pero si deducibles, etc.. Es decir, el método trabaja con probabilidades en la certeza del diagnóstico y con baremos de importancia a través de las reglas de control, calculando y sumando todas las influencias inducidas previamente por el NAAP

Las influencias se pueden dar por eventos que afectan directamente a estas características que necesitamos, o bien a través de situaciones que indirectamente podrían influir sobre ellas. Sin embargo, al operador humano le cuesta bastante más actuar análogamente, tanto en tiempo como en esfuerzo y eficacia

e.2) Otra ventaja del método, es que al emplear subconjuntos difusos, es capaz de **automatizar y simular expresiones imprecisas del lenguaje humano** como MUY IMPORTANTE o probabilidad ALTA, mediante una asignación de valores concretos y transformándolas así en entes matemáticos con los que operar. Permite al sistema enfrentarse con sentencias o variables lingüísticas típicas empleadas por los operadores.

e.3) Siguiendo con las mejoras del método CNOD frente al diagnóstico no automatizado, **es capaz de manejar situaciones compuestas**. Se podría decir que basta con saber la escala de prioridades que se asignan y enfrentarla con los datos de entrada: *por ejemplo, si el tener un enlace activo tiene el mayor peso en mis prioridades, más que el arreglo de un pad, concentro en mayor medida los recursos disponibles para solucionar los efectos de las alarmas concernientes a problemas en los enlaces.*

En este caso se ha especificado una prioridad y una categoría de alarma simple asignada a un solo síntoma. Pero esta situación se torna bastante más compleja si la lista de prioridades es mucho mayor e interrelacionada *(es lo más importante si... y si..., mientras no ocurra...)*. El diagnóstico que realiza el NAAP, en ocasiones será unívoco al establecer una reacción directa causa-efecto entre el síntoma y sus efectos con una probabilidad del 100%, y en consecuencia, los refuerzos a generar sobre la necesidad de los recursos dependiendo siempre de las prioridades asignadas. Pero puede ocurrir que por la complejidad de los diagnósticos y de la realidad de una red de telecomunicaciones, el NAAP a través de este método, se ve obligado a realizar refuerzos paralelos de distinta intensidad según la probabilidad del diagnóstico, influyendo simultáneamente sobre distintas necesidades.

Este hecho puede provocar finalmente que ante problemas concurrentes y según la valoración establecida en las reglas de control sobre la necesidad de las características, la proporción e incidencia de la suma de las prioridades parciales supere la prioridad del problema que a simple vista pudiera tener más urgencia en ser resuelto.

e.4) Cabe también destacar la facilidad que el método CNOD proporciona para influir dinámicamente, tanto **sobre la importancia que se le quiere dar a las probabilidades** que el NAAP asigna a sus diagnósticos, como sobre las **prioridades** que en cada momento el **Centro de Operaciones de Red** pueda establecer internamente. Esta sencillez y efectividad que demuestra el método CNOD para modificar su comportamiento, no encuentra su analogía en el comportamiento humano

En cuanto a la posibilidad de **incidir sobre las probabilidades**, en lugar de realizar refuerzos proporcionales según su grado de pertenencia, un Operador de Red puede llegar a establecer franjas de certeza en los diagnósticos, desechando aquellos que se sitúen por debajo de un nivel preestablecido Para ello bastará con ajustar la definición de las curvas de probabilidad de la Figura 13. Este caso se dará cuando el NAAP carezca de suficientes datos como para asignar al diagnóstico una certeza apreciable, o cuando se vea forzado, por una limitación temporal excesiva sin posibilidad de disponer del mínimo tiempo necesario, a efectuar un diagnóstico El Operador puede querer observar estos diagnósticos pero no tenerlos en cuenta para que el sistema automáticamente tome decisiones

Las **prioridades en la resolución de problemas** se pueden también cambiar mediante un sencillo procedimiento, modificando la base de reglas de control De esta forma se

puede reorientar las directrices internas del Sistema de Gestión de Fallos, sin tener que detener el funcionamiento del NAAP.

Estos cambios en la base de reglas podrán ser temporales, por la introducción de un nuevo producto o elemento que requiere gestión, prioridades en los recursos asignados a diferentes clientes, etc., o bien semipermanentes debido a cambios en la política de gestión a desarrollar.

```
/*****************************************************/
/*          Núcleo principal del algoritmo CNOD      */
/*****************************************************/

#include <stdio.h>
#include <stdlib.h>

main()
{
  /* La necesidad dividida en 7 zonas */
        double curva_necesidad[7][11] = {1,0,0,0,0,0,0,0,0,0,0,
                                         1,.9,.3,0,0,0,0,0,0,0,0,
                                         0,.1,.5,1,.5,.1,0,0,0,0,0,
                                         0,0,.1,.4,.8,1,.8,.4,.1,0,0,
                                         0,0,0,0,0,.1,.5,1,.5,.1,0,
                                         0,0,0,0,0,0,0,0,.3,.9,1,
                                         0,0,0,0,0,0,0,0,0,0,1};

  /* El refuerzo dividido en 8 zonas */
        double curva_refuerzo[8][11] = {0,0,0,0,0,0,0,0,0,0,1,
                                        0,0,0,0,0,0,.1,.9,1,.3,0,
                                        0,0,0,.1,.2,.5,1,.5,.2,.1,0,
                                        0,.1,.2,.5,1,.5,.2,.1,0,0,0,
                                        0,-.1,-.2,-.5,-1,-.5,-.2,-.1,0,0,0,
                                        0,0,0,-.1,-.2,-.5,-1,-.5,-.2,-.1,0,
                                        0,0,0,0,0,0,-.1,-.9,-1,-.3,0,
                                        0,0,0,0,0,0,0,0,0,0,-1};


 int prioridad,importancia,positivo,refuerzo,t;
double grado_pertenencia,coef_refuerzo,denominador,x,CDG;

 /* Grado de prioridad que tiene una característica */
printf("\nPrioridad: ");
scanf("%d",&prioridad);


 /*****************************************************/
 /*  Definición de una REGLA de CONTROL               */
 /*****************************************************/

 /* ANTECEDENTE de la REGLA de CONTROL */
 /* Importancia que tiene la característica */

printf("\n\n1 - Totalmente prescindible");
printf("\n2 - Nada importante");
printf("\n3 - Poco importante");
printf("\n4 - Importante");
printf("\n5 - Muy importante");
printf("\n6 - Máxima importancia");
printf("\n7 - Imprescindible");
printf("\n\nImportancia: ");
```

```
 scanf("%d",&importancia).
 * CONSECUENTE de la REGLA de CONTROL. *
 * Refuerzo a efectuar sobre un recurso para mantener la caracteristica *
printf(" \n\nRefuerzo positivo(1) o negativo(2) ").
scanf("%d",&positivo).
printf(" \n1 - Maximo").
printf(" \n2 - Muy alto").
printf(" \n3 - Alto").
printf(" \n4 - Medio").
printf(" \n\nRefuerzo ").
scanf("%d",&refuerzo).
if (positivo != 1) positivo = -1.

*************************************************************************
* El grado de pertenencia indica la medida en que la prioridad
  satisface la curva de necesidad                              *

  grado_pertenencia = curva_necesidad[importancia-1][prioridad].

for (t=0.0; t<5; cost_refuerzo=0,denominador=0,t<11.0; t=t+0.5) {
  cost_refuerzo = t * curva_refuerzo[refuerzo-1][t].
  denominador = curva_refuerzo[refuerzo-1][t].
}
*****************
* Resultado *
*****************
CDG= grado_pertenencia*cost_refuerzo*positivo/denominador.
printf(" \n\nCDG: %d",CDG).
}
```

Algoritmo 1 Especificación del núcleo principal del algoritmo CNOD.

Esta validacion del metodo CNOD refleja la posibilidad de su aplicación como una simulación mejorada del comportamiento del operador humano, formulandose como un modulo software a integrar en el NAAP, dando soporte a las aplicaciones dentro del area de la gestión de red

4. Nueva metodología para mejorar la calidad del proceso de seguridad de una red y su integración en el rendimiento de las Plataformas de Gestión de Red a través del NAAP.

Para gestionar eficazmente un entorno de telecomunicaciones, debe existir un compromiso adecuado entre costes, seguridad, riesgo, rendimiento y conectividad, ademas de ser capaces de conjugar y aplicar todos estos factores con un nivel alto de calidad

El mantener la seguridad de red, en su más amplio concepto, debe incorporarse como elemento imprescindible de los sistemas de gestión de red, y no como valor añadido a implementar de una forma complementaria y sin ninguna integración con las plataformas o con las aplicaciones que sobre ellas funcionan

El concepto de red segura que incorpora el NAAP, implica una red fiable, estable y protegida, y no sólo un valor añadido al modo en que se accede y utilizan los datos

En un primer enfoque a la finalidad de la gestión de la seguridad del NAAP, se puede decir que su funcion es asegurar que los usuarios solamente podrán realizar aquellas tareas para las que están autorizados, que solamente podrán obtener información que están autorizados a tener y que no podrán causar daño a los datos, aplicaciones o incluso al sistema de red globalmente

4.1. Validación de amenazas y acotación de la falta de seguridad en una arquitectura para la Gestión de Comunicaciones WAN, tras una evaluación de datos experimentales.

Toda mecanismo de seguridad es susceptible de mejora en la medida que no existe nada totalmente seguro Este proceso comienza con la documentación de la configuración de la red y sus componentes, comprometiéndose a desarrollarla, a hacerla accesible convenientemente y a mantenerla al dia Hay que saber la "materia prima" con la que se va a trabajar y sus caracteristicas para que los gestores de una red puedan conocer quiénes son los usuarios de la red, a qué recursos acceden, cuándo y dónde, de una manera fiable

Pero sin duda, el punto que identifico como más débil de un sistema de red seguro, y que por lo tanto, las caracteristicas del NAAP lo consideran, es el de poder controlar o al menos detectar y gestionar los accesos a los dispositivos de red

4.1.1. Acceso autorizado a los recursos.

Los controles se tienen que colocar de manera que se verifique la identificación correcta en el momento de solicitar el acceso al recurso, teniendo la posibilidad de asignar diferentes perfiles de usuario según la clave que se emplee para acceder al dispositivo

Para evaluar el acceso no autorizado a un dispositivo, y documentar la grave incidencia que tiene, estudiaremos un caso práctico extraído de un elemento empleado habitualmente en redes de comunicaciones: un PAD.

4.1.1.1. Necesidad de un discriminador de amenazas basado en un estudio empírico en un entorno real dentro de una arquitectura para la Gestión de Comunicaciones WAN: PAD/FRAD/IFRAD.

La compañía B T Telecomunicaciones, incorpora estos elementos en sus nodos de telecomunicaciones con el objeto de gestionar los servicios X 28, X 32, Multiprotocolo, y permitir la gestion de los diversos chasis de módems que se encuentran instalados

Estos equipos de comunicación tienen varias formas de acceso, entre las cuales figura el acceso vía RTC para configuracion remota Es indudable, que al ser ésta una puerta de entrada cuanto menos "sensible", aunque por otro lado típica de estos sistemas, debe presentar una protección añadida para impedir que sea una puerta falsa No servirían de nada unas grandes protecciones en los locales donde están ubicados estos dispositivos, si con una simple llamada de teléfono se nos brinda un acceso muchísimo más cómodo y menos arriesgado Por todo ello, es imprescindible al menos un password de acceso

Como se aprecia por la opciones y posibilidades del menú principal reflejado en la Figura 16, el acceso al PAD no puede dejarse al azar de un número de teléfono más o menos privado Veamos una sesión estándar de entrada al PAD

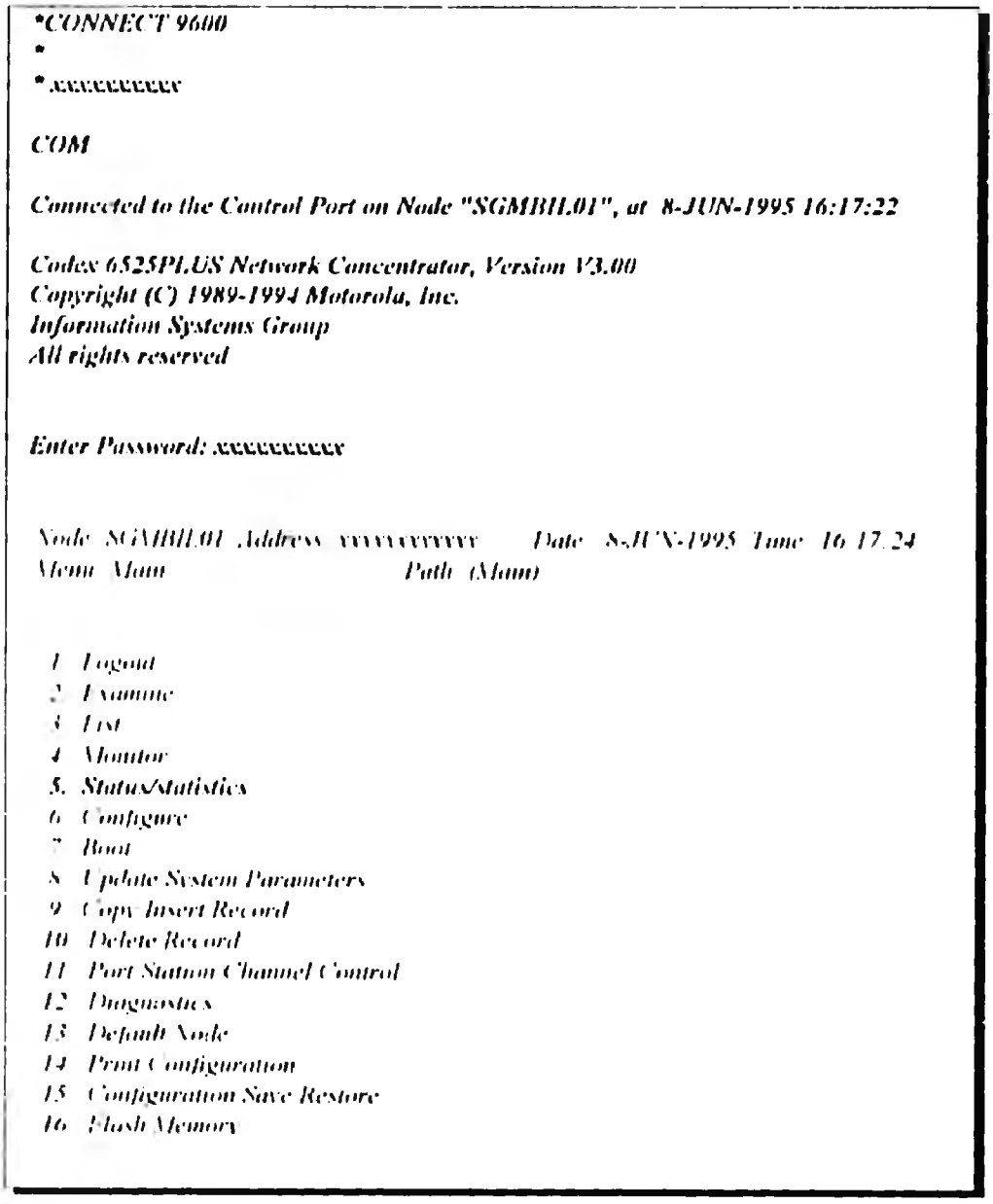

Fig. 16 Sesión estándar de entrada a un PAD.

Este modelo de PAD permite saber cuándo ha sido la última vez que se ha accedido a cada uno de sus puertos. Es quizás un dato interesante, pero que no deja de ser un mero indicativo de una situación anómala. No es una protección activa.

```
Node: SGMBIL01  Address: xxxxxxxxxxx      Date: 8-JUN-1995  Time: 16:17:58
Menu: Status statistics                   Path: (Main.5)

 1.  Node Stat                          19.  Reset XDLC Station Stats
 2.  Detailed Port Stat                 20.  NCCP Pad Stats
 3.  Flash to Flash Transfer Stat       21.  Lan Connection Statistics
 4.  Detailed Link Stat                 22.  FRA Station Statistics
 5.  Detailed SDLC Station Stats        23.  TFTP Stats
 6.  Detailed Pad Stat                  24.  Router Stats
 7.  Call Summary Stat                  25.  LLC to SDLC Statistics
 8.  Hardware Stats                     26.  (reserved)
 9.  Reset SDLC Station Stats           27.  (reserved)
10.  Reset Port Stats                   28.  (reserved)
11.  Reset All Stats                    29.  (reserved)
12.  Software Option Statistics         30.  SNMP Statistics
13.  FRI Station Statistics
14.  DCP Statistics
15.  Internal DSD Stat
16.  Reset Internal DSD Stats
17.  LBU Table Stat

Enter Selection: 7
```

```
Node: SGMBIL01  Address: xxxxxxxxxxx      Date: 8-JUN-1995  Time: 16:18:03
Menu: Call Summary Stat                   Path: (Main.5.7)

 1.  SVC Call Summary
 2.  PVC Connection Summary

Enter Selection: 1
```

```
Node: SGMBIL01  Address: xxxxxxxxxxx      Date: 8-JUN-1995  Time: 16:18:05
Detailed Call Summary                     Page: 1 of 1

Calling Channel    Called Channel     R F N C     Connection Time
-----------------  -----------------  ---------   ---------------------
DPAD-1             PAD-2              0 0 0 0     5-JUN-1995 20:54:15
DPAD-1             X25-1(16)          0 0 0 0     5-JUN-1995 20:54:15
DPAD-2             PAD-3              0 0 0 0     5-JUN-1995 20:54:19
DPAD-2             X25-1(15)          0 0 0 0     5-JUN-1995 20:54:19
DPAD-3             PAD-4              0 0 0 0     5-JUN-1995 20:54:23
DPAD-3             X25-1(14)          0 0 0 0     5-JUN-1995 20:54:23
PAD-6              ControlPort        0 0 0 0     8-JUN-1995 16:17:22
```

Fig. 17 Último acceso a un PAD.

También podemos extraer estadísticas basadas en el tráfico que cursan los diferentes puertos que componen el nodo, canales que se están empleando, utilización de la CPU en diferentes momentos del día, etc.

```
Detailed Node Statistics

Node number: 0
Product Type: Codex 6525PLUS Network Concentrator
Software source: RAM
Software PROM revision: V3.00 (Sat Dec 5 13:28:58 EST 1992)

Download code source:  FLASH      Size: 3497524 Bytes

Last power on event:          07-MAY-1996 22:49:02
Last reset button event:      07-MAY-1996 20:30:10
Last node boot:               07-MAY-1996 22:56:47
Last configuration change:    07-MAY-1996 16:55:20

Power Supply Status: Running
Compressed config. memory (CMEM):   32214 bytes avail.,  3048 bytes (9%) used
Uncompressed config. memory (DRAM): 65536 bytes avail.,  7276 bytes (11%) used

Routing statistics
                  Current   Maximum
Calls in place:       25        31
Calls per second:      0         0
PVC connections:       0         0

Buffers available: 29586, used 488 (1%), maximum used 1001 (3%)

Node Throughput
                  Current   Maximum
Characters sec:      2429      7403
Packets sec:           46        85

Board 1:  Board Type: CPU4  Number of ports: 6  Status: Running

Memory Configuration
  EPROM: 2.0 MBytes        DRAM: 1.0 MBytes

Port Configuration
  Port 1 DMI:  V.35          DCE
  Port 2 DMI:  EIA-232-D     DCE

CPU Throughput:  CPU utilization: 16%
                  Current   Maximum
  Characters sec:     51       193
  Packets sec:        10        11
```

Fig. 18 Estadísticas diversas proporcionadas por el PAD.

Si nos centramos en otro tipo de protocolos como puede ser Frame Relay, la ausencia o deficiencia de las formas de protección en el acceso a los dispositivos puede provocar efectos aún más negativos. Tipicamente los equipos FRAD (Frame Relay Access Device) han soportado protocolos orientados a datos. Sin embargo algunos fabricantes de esta clase de equipos empiezan a comercializar los llamados IFRADs (Integrated Frame Relay Access Devices) que permiten combinar tráfico de voz , fax y datos para su transmisión sobre redes públicas o privadas Frame Relay.

Este nuevo producto obedece a la demanda de un servicio integrado de voz + datos que permita rentabilizar al máximo la linea de acceso de alta velocidad, integrando las llamadas telefónicas y las transmisiones de fax con el tráfico LAN y el de otros protocolos soportados por los routers.

Esta solucion Frame Relay se aplica en B T Telecomunicaciones siguiendo el siguiente esquema

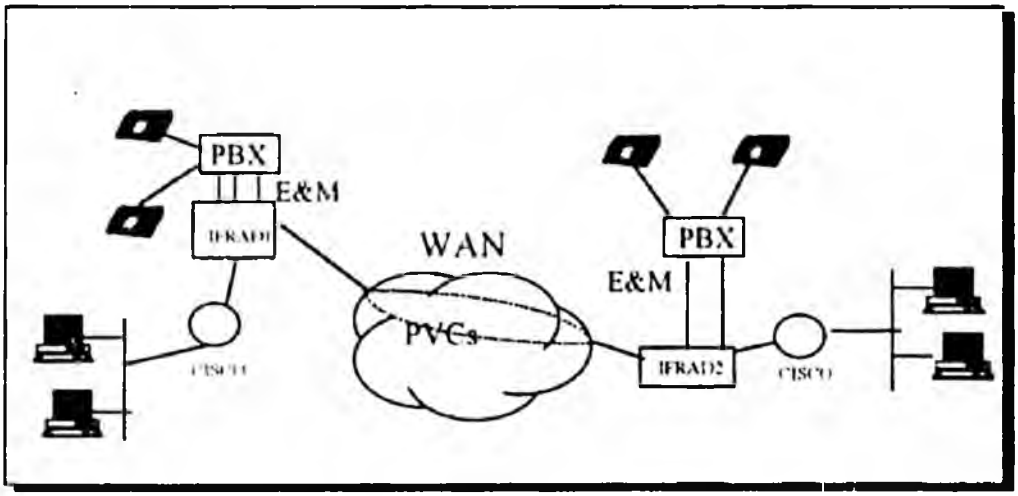

Fig. 19 Integración Voz + datos sobre Frame Relay

El IFRAD es el elemento que se enfrenta directamente con la WAN (Figura 19), existiendo la posibilidad de su acceso remoto a través de una dirección normalizada X.121 de gestión, asociada al puerto del IFRAD que está conectado al módem. Esto supone un posible acceso a través del servicio X 28 público de la propia WAN, o bien a través de cualquier acceso asincrono a los diferentes PAD de gestión ubicados en los diferentes nodos

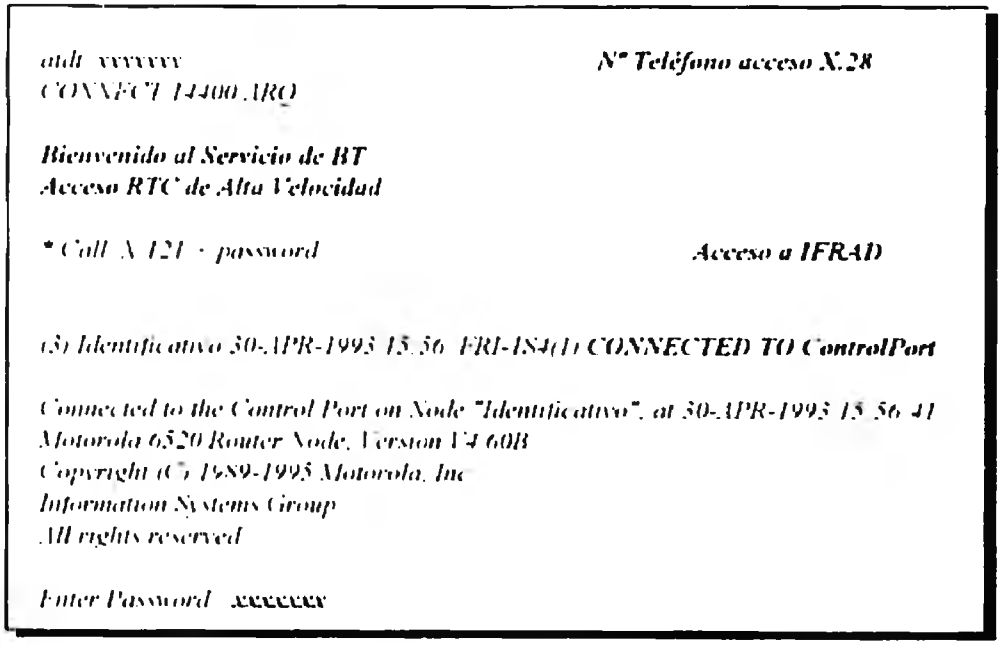

Fig. 20 Acceso a IFRAD vía servicio X.28

De nuevo tenemos un acceso total al dispositivo. En este caso podemos ver la cantidad de tráfico global de datos que esta organización genera, y observar incluso el número, la duración y destino de las llamadas telefónicas realizadas

Detailed Link Statistics — Page: 1 of 1

Type entity	Type subtype	State state	State speed	date	CRC errors	Link down	Data frames out
p1	FRI	up	64000	21-APR-1993	4	0	807058
p1s1	FRI	up	0	21-APR-1993	0	0	126052
p1s2	FRI	-	0	29-APR-1993	0	6	380174
p1s3	FRI	up	0	21-APR-1993	0	0	0
p1s4	FRI	up	0	30-APR-1993	0	10	299425
p1s5	FRI	up	0	21-APR-1993	0	9	1407
p2	FRA	up	64000	21-APR-1993	3	0	204650

Fig. 21 Tráfico generado en un IFRAD

Detailed VOICE Port Statistics: Port 13 — *Page: 1 of 5*

Time Of Last Statistics Reset: 21-APR-1993 13:24:52

Board Level
DSPM Board State: Running
Interface Type: FXS 4SA Present
HW Part Number: 72182G01

Port Level
Port State: Enabled — ***Voice Call Duration : 00:00:29***
Circuit State: Disconnected — ***Total Voice Calls Duration: 00:18:36***
Port Utilization: 0% — ***Number of Voice Calls : 6***

Packet Level
Tx Packets: 22080 — *Rx Packets: 1929*
Tx Packets sec: 0 — *Rx Packets sec: 0*
Tx Packets Dropped: 0 — *Rx Packets Dropped: 0*

DSP Level
Current Mode: VOICE — *DSP Efficiency: 100%*
Current Rate: 8K — *Reconstructed Pkts: 6*
FAX Transmissions: 0 — *Input Power: -66*

Call Summary
Last clear cause code: 0 (Cleared by other end)
Last clear diagnostic code: 186 (Unknown diagnostic code)

Last Inbound Call
Called Address: 2149450000 7013
Calling Address: 2149450000 95120
Facilities: C802014081 08C8010087010086040026001E
CUD: 11000153010000

Last Outbound Call
Called Address: 2149450000 95120
Calling Address: 2149450000 7013
Facilities: C1098701008604002600 1E
CUD: 11000128010000

Fig. 22 Llamadas telefónicas realizadas a través de un IFRAD.

4.1.1.1.1. Análisis de riesgos como métrica de evaluación de la gravedad de accesos no autorizados.

Supongamos que este IFRAD proporciona servicios de VOZ CORPORATIVA *(CIR = 36k)* y DATOS *(CIR = 16k)*, según esquema representado en la Figura 19. Los DATOS son encapsulados sobre F.R. tanto tráfico de LAN (TCP/IP) como tráfico X.25 nativo de un Gateway.

Para ver el uso que se hacen de los diferentes servicios en momentos concretos, se podrían elaborar, por ejemplo, estadísticas detalladas sobre el peso que cada protocolo, incluida la VOZ, tiene sobre el tráfico FR.

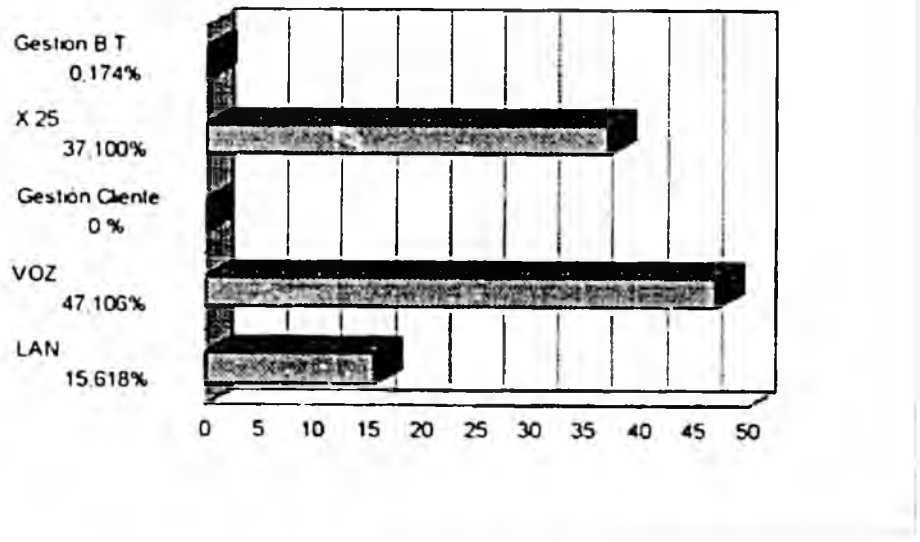

Fig. 23 Estadísticas por tipo de tráfico sobre Frame Relay

Incluso considerando también la hora del día en la que hace el muestreo (Anexo 1), se puede deducir qué uso y aplicaciones predominan a diferentes horas del día: primera hora

de la mañana, última hora de la tarde, etc., qué franjas horarias registran una mayor actividad, detalles de la gestión via SNMP...

En esta instalación el Puerto 1 está conectado al módem, saliendo por él todo el tráfico que procede del resto de los puertos y a su vez, por donde entra el tráfico procedente de la WAN; el puerto 2 se encuentra conectado al router, que enruta tráfico LAN y tráfico del Gateway X 25, y los puertos 13 y 14, son de la PBX o centralita de teléfonos.

Del tráfico que pasa por el PUERTO 1, se extraen las siguientes conclusiones:

a) La mayor parte del volumen de tráfico generado en esta organización recae en 2 franjas horarias a primera hora de la mañana (30%) y al mediodia (35%), disminuyendo bastante por la tarde (13%)

b) Observando el sentido en que fluye el tráfico (IN-OUT), a media mañana (10 00h - 12 00h) predominan las aplicaciones que generan tráfico saliente (26,88%) como son E-Mail, transacciones de entrada de datos, etc , frente a las que consultan información (17,679%), mientras que al mediodia se invierten las proporciones IN = 38,419% y OUT = 29,863%. En el resto del dia la balanza está equilibrada

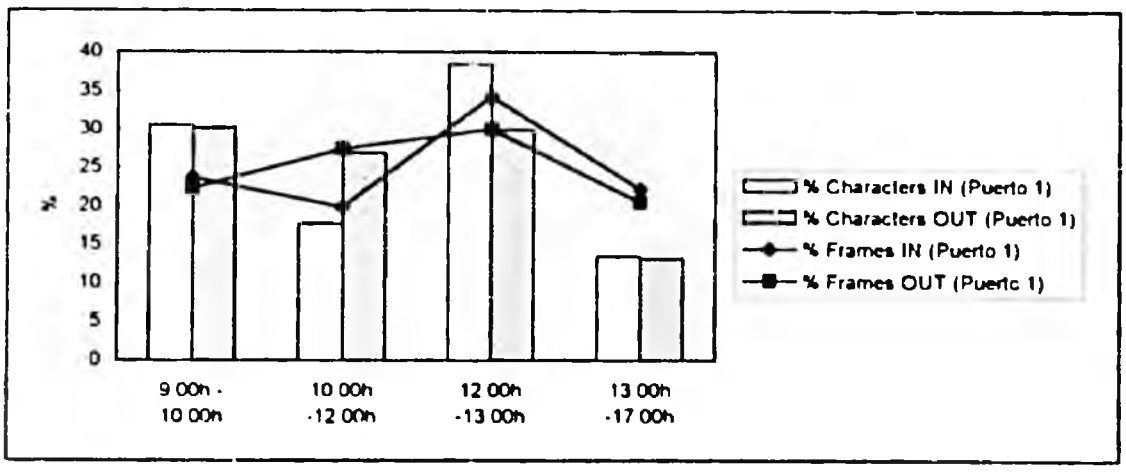

Fig. 24 Estadísticas del volumen de tráfico distribuido en franjas horarias del puerto WAN de un IFRID.

En cuanto al PUERTO 2 - conectado al router -, se puede decir que

a) La mayor parte del tráfico también se sitúa en las mismas franjas horarias que en el PUERTO 1 a primera hora de la mañana (34%) y al mediodía (33%), reduciéndose bastante durante el resto del dia

b) En todo momento, las consultas han generado un tráfico equivalente a la entrada de datos

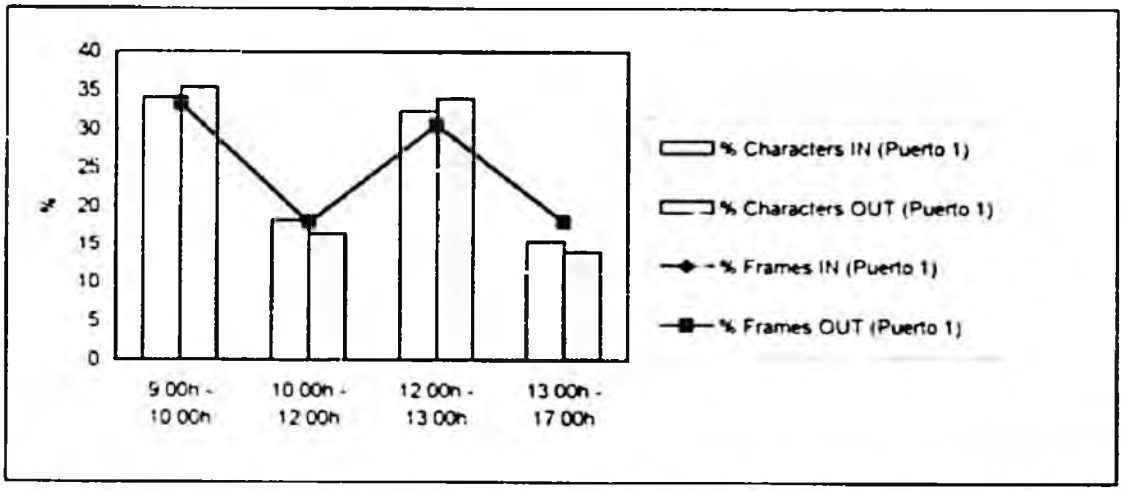

Fig. 25 Estadísticas del volumen de tráfico distribuido en franjas horarias del puerto LAN de un IFRAD.

Como aspecto chocante en el tráfico X 25 recogido en el Anexo 1, destacar que mientras a Nivel 2, el número de FRAMES conteniendo datos de entrada - IN -, es similar al de salida - OUT -, en el Nivel 3 de Enlace, los PAQUETES de datos de salida son casi 4 veces superiores a los de entrada Esto es asi porque en la configuración del IFRAD se ha especificado que cuando existan paquetes de voz, se trabaje con segmentación de datos y su tamaño sea como máximo de 128 bytes Esto normalmente generará un mayor

tráfico de salida que de entrada. Esta opción se ha activado porque la voz es sensible a los retardos, y a pesar de contar con prioridad, no es compatible con una conmutación de paquetes de datos excesivamente grandes.

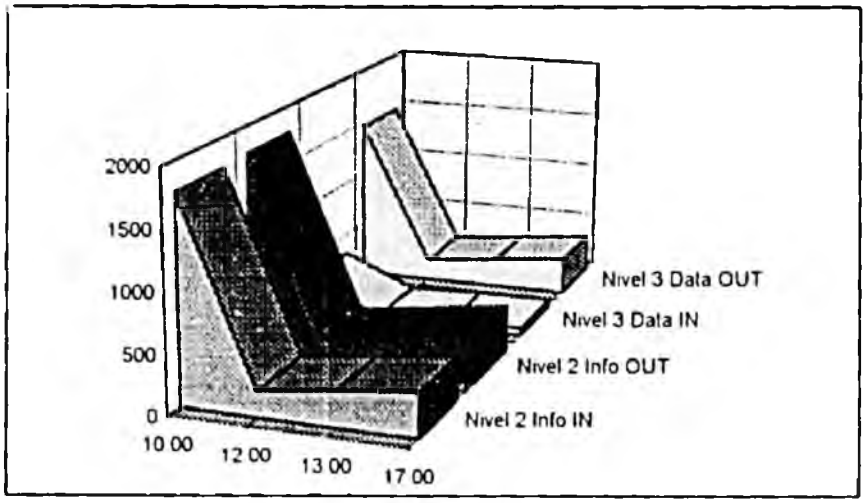

Fig. 26 Estadísticas del volumen de tráfico X.25 distribuido en franjas horarias a través de un IFRAD.

En cuanto al tráfico de VOZ, de las datos recogidos en el Anexo 1 se observa que la utilización de los puertos 13 y 14 se distribuye según la siguiente gráfica:

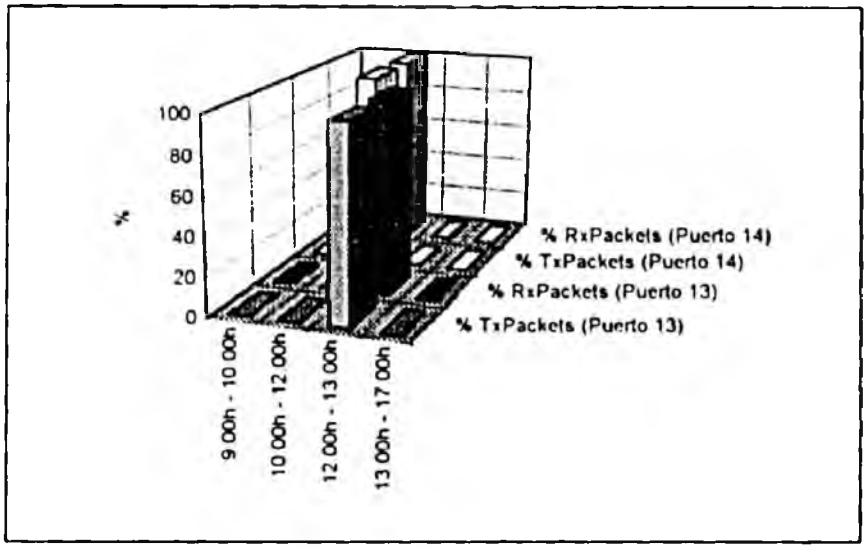

Fig. 27 Estadísticas del volumen de tráfico de VOZ distribuido en franjas horarias a través de un IFRAD.

La última estadística que quisiera valorar, hace referencia a la gestión SNMP del dispositivo. Según los datos del Anexo 1, durante el día no se ha producido ninguna alarma y además, la gestión remota se lleva a cabo a última hora del día.

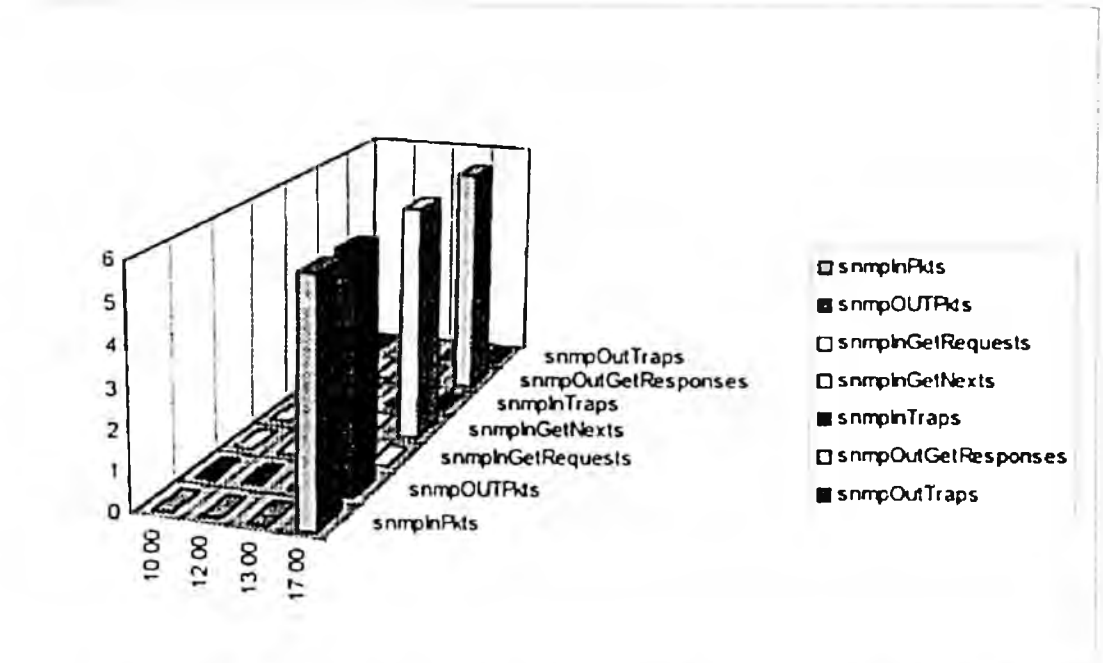

Fig. 28 Estadísticas del volumen de tráfico de Gestión SNMP distribuido en franjas horarias a través de un IFRAD.

Como se pone de manifiesto en este estudio basado en el tráfico de VOZ y DATOS que gestiona el IFRAD de esta organización, el acceso no autorizado a un dispositivo puede llegar a proporcionar, con una interpretación adecuada de los datos, información delicada sobre el funcionamiento y carga de trabajo de una empresa Además, únicamente hemos actuado como espectadores pasivos, sin intentar monitorizar tráfico ni incidir activamente sobre las comunicaciones

Con estas estadísticas y casos refuerzo la imperiosa necesidad de protección, y sobre

todo, la gran importancia que tiene el acceso autorizado a los recursos. Es por ello que el NAAP, no como funcionalidad de valor añadido, sino como funcionalidad necesaria, se percata de aquellos accesos de dudosa autorización (por el número de reintentos en el acceso, por notificación de los dispositivos, por verificación periódica y automática de los accesos, etc.), convirtiéndose en una valiosa ayuda al operador de la red.

4.2. Definición y diseño del modelo de seguridad MOSA en el NAAP.

El NAAP implementa una política de seguridad basada en las siguientes premisas:

a) Una persona, o máquina, puede no ser autorizada a acceder a datos clasificados, a menos que posea el nivel de seguridad suficiente y la necesidad de conocer la información

b) Existen normas para manejar aquellas restricciones especiales añadidas a los datos, que se cumplirán siempre que se acceda a la información.

Toda la información se transmite en formato de paquete de datos, incluyendo en su cabecera las direcciones y cualquier otro elemento incluido por el nivel de seguridad. En este contexto, el modelo de seguridad propuesto protege tanto el envío como la recepción de los paquetes de datos.

El MOSA (Modelo de Seguridad Avanzado) aportado establece 5 reglas básicas:

Regla 1: *Los paquetes de datos deben incluir una cabecera correcta, reflejando el nivel de seguridad.*

Regla 2: *La UIR (Unidad de Interface con la Red) no debe transmitir un paquete de datos si no está autorizado para hacerlo.*

Regla 3: *La UIR no debe distribuir un paquete de datos al computador central si no está autorizado para hacerlo.*

Regla 4: *Los paquetes entregados al computador central no se deben modificar o alterar.*

Regla 5: *Todos los eventos relativos a la seguridad se auditarán para tener constancia de cualquier violación que pudiera ocurrir.*

La Regla 1 establece que los paquetes deben incluir en su cabecera un campo necesario y obligatorio, para reflejar el tipo de paquete y cualquier restricción en cuanto a la seguridad que se le pudiera aplicar en su manejo

Las encargadas de cumplir la Regla 1 son las propias UIR, que siempre deben conocer el nivel de seguridad tanto de sus conexiones como el que les imponen los computadores centrales a los que están conectadas

Cuando una UIR recibe un paquete del computador central, primero comprobará el nivel de seguridad del computador central para utilizarlo en su comunicación Si no es así, aplicará el nivel relativo a la conexión que mantiene

La Regla 2 impide a la UIR transmitir información desde un computador central cuyo nivel de seguridad es, o bien demasiado alto, o demasiado bajo. Su cumplimiento asegura que los paquetes de un computador central solamente puedan ser enviados a aquellos otros computadores centrales que realmente necesiten recibirlos.

La Regla 3 impide a la UIR entregar paquetes a los computadores a los que está conectada, si éstos no están libres o necesitan recibirlos. Esta regla permite a los computadores tener un nivel mínimo de seguridad asignado a la recepción de paquetes y sin embargo garantizar la entrega correcta de los paquetes de datos

Para cumplir las reglas 2 y 3, una UIR debe ser capaz de tomar decisiones sobre el envio o no de paquetes y sobre su recepción procedente de otras UIR, basándose en la direccion origen incluida en el paquete, el nivel de seguridad y el nivel de ocupación y necesidad de cada UIR Para ello se utilizan tablas de control de accesos.

El NAAP es capaz de consultar estas tablas de control de accesos, cuyo mantenimiento y configuracion le corresponde al Centro de Operaciones de Red, único autorizado a entrar en el Modulo de Control de Accesos (MCA) y responsable de que cada entrada en la tabla de los diferentes destinos o computadores existentes, refleje los niveles de seguridad, restricciones en el manejo y acceso a datos, y los niveles a los que puede franquear su información y con los que puede comunicarse.

Para comenzar una comunicación, el computador A (H_A) envía una petición al computador B (H_B) especificando el nivel de seguridad y tipo de conexión que quiere

emplear. La UIR de H_A interpreta este proceso como una petición de conexión y la dirige al MCA, que basándose en sus tablas de control de accesos aprueba o no esta petición Si no es aceptada, se informa a H_A que no puede comunicarse con H_B Por el contrario, si valida positivamente la solicitud de H_A, el MCA envía una petición a H_B para que la apruebe, y éste intenta dirigir su aceptación o rechazo de conexión a H_A Sin embargo la UIR de H_B redirige esta respuesta de H_B al MCA Si la respuesta es positiva, el MCA registra esta situación en sus tablas, lo notifica a H_A, y también pide a las dos UIR que cambien el estado del enlace para que reflejen los computadores y los niveles de seguridad empleados

A partir de ahora las UIR se encargarán de la seguridad de la conexión activada No se volverá a hablar con el MCA hasta que se termine la conexión o se produzca algún evento de seguridad relevante y por otro lado, cualquier paquete que le llegue a la UIR, tanto de los computadores centrales como de la LAN, se aceptará o no de acuerdo a los niveles de la conexión que se han impuesto por el MCA

Las Reglas 2 y 3 no pueden cumplirse sin la Regla 4, y dependiendo ambas de la comunicación con el computador central Es muy importante que estos paquetes no puedan ser alterados o falsificados ya que de lo contrario podrían producirse conexiones no autorizadas

El cumplimiento de la Regla 4 puede reforzarse con el uso de las técnicas adecuadas de autentificación y encriptación

La Regla 5 no incrementa estrictamente la seguridad del sistema, pero se incluye para reforzar su confianza y tener certeza de que cualquier brecha en la seguridad pueda ser detectada y perseguida.

Esta auditoría de bajo nivel se produce tanto en las UIR como en el MCA. Las UIR comunican las incidencias relativas a la seguridad al MCA y allí se almacenan para su posterior estudio por el Centro de Control.

4.2.1. Desarrollo de un álgebra para el MOSA.

El MOSA introduce los conceptos y funciones necesarias para fundamentar matemáticamente las 5 reglas básicas de la política de seguridad.

Tiene en cuenta 3 elementos distintos: la UIR, el MCA y la comunicación entre las UIR y el MCA.

4.2.1.1. Fundamentos matemáticos de las reglas de seguridad.

Antes de formular las reglas matemáticamente, introduzco algunas consideraciones. Los niveles de seguridad de la Regla 1 tienen que ser formalmente definidos. Para describir las Reglas 2 y 3 se necesitan 4 funciones, que son: *enviar-paquete*, *recibir-paquete*,

iniciar-conexión, *terminar-conexión*. Finalmente, para completar la definición de las Reglas 4 y 5 establezco las funciones *no-alterar* y *auditar*.

Dado un conjunto, P, de paquetes. La Regla 1 dice que se debe asignar una etiqueta que clasifique a cada elemento p, de P, para identificar su nivel de seguridad. Su definición es es:

$$Etiqueta = (S, C, H)$$

donde

S *nivel de seguridad*

C *conjunto de información encasillado*

H *conjunto de restricciones*

El nivel de seguridad, S, indica la clasificación de los datos. El rango de posibles valores para S viene del conjunto ES, existiendo una función, R, que ordena definitivamente los elementos de ES. Los posibles niveles de seguridad, ordenados de menor a mayor por R, son: sin clasificar (SC), encriptado para transmitir (EPT), restringido (R), confidencial (C), secreto (S), alto secreto (AS), programación y control (PROC)

El conjunto de información encasillada, C, se utiliza para controlar los accesos y contiene la necesidad de acceder a la información. El rango de posibles valores para C viene del conjunto EC. A diferencia de ES, este conjunto no obedece a una estructura jerárquica. Cada elemento, Ci, representa una casilla donde se puede ubicar una unidad de datos

El conjunto H, también mantiene un orden no jerárquico dentro de su conjunto EH. Un valor nulo de H implica que no existe ninguna restricción en el manejo de datos.

Todos los niveles de seguridad posibles vienen dados por el espacio de seguridad, Espacio-C. Espacio-C se deriva de los 3 conjuntos: ES, EC y EH. Se define como el producto Cartesiano,

Espacio-C ES x P(EC) x P(EH)

donde P() es el conjunto de todos los posibles subconjuntos de los correspondientes conjuntos

Se puede lograr ordenar parcialmente el Espacio-C introduciendo el concepto de dominio en la seguridad. Dadas 2 cabeceras de seguridad CAx y CAy, tal que

CAx (Sx, Cx, Hx) y *CAy (Sy, Cy, Hy)*

se dice que CAx es dominado por CAy si y solo si

R(Sx) R(Sy),

Cx es un subconjunto de Cy, y

Hx es un subconjunto de Hy.

La función *dominar(CAx, CAy)*, donde CAx y CAy son elementos del Espacio-C, devuelve verdadero si y solo si CAx domina a CAy.

Existen también 2 funciones, *etiquetar (p)* y *s-etiquetar (p,l)* donde p es un elemento de P y l es un elemento del Espacio-C, que leen una cabecera, o escriben en una cabecera de un paquete de datos.

Antes de definir las funciones *enviar-paquete*, *recibir-paquete*, *iniciar-conexión y terminar-conexión*, es necesario también definir algunos conceptos y funciones más.

Existe un conjunto B definido como:

$$B = (b : b \text{ es una UIR}).$$

b es necesariamente no vacio. Debe tener al menos un elemento, B-MCA, que representa la UIR del MCA.

Existe una función, *identidad()*, que devuelve un elemento b, de B, que es la UIR que ejecutó la función. Esta función permite a la UIR determinar su propia identidad.

Existen otras dos funciones, *modo* y *establecer-modo*, que se definen de la siguiente manera.

modo(b) - devuelve el modo de funcionamiento del elemento b, de B.

0 si se puede confiar en las cabeceras de los paquetes del computador central al que está conectado.

1 si no se puede confiar en las cabeceras de los paquetes de datos del computador central al que está conectado.

establecer-modo(b,m) - establece el modo operativo

b *UIR a establecer - un elemento de B*

m *0 o 1*

0 si se puede confiar en las cabeceras de los paquetes de los computadores

1 si no se puede confiar en las cabeceras de los paquetes de datos de los computadores

Para describir el control de accesos realizado por el MCA para una UIR, se establecen otras dos funcionas más. Estas funciones, *acceso-obligatorio* y *acceso-opcional*, son:

acceso-obligatorio (b1, tipo, sia, iia) y

acceso-opcional(b1, b2, tipo),

donde

b1 – la UIR para la que se está haciendo la comprobación - un elemento de B,

tipo – el tipo de conexión - un elemento de T,

sia – el límite superior del intervalo de la conexión - un elemento de Al, y

iia – el límite inferior del intervalo de acceso de la conexión - un elemento de Al.

Mandatoy-access (b, tipo, sia, iia) devuelve verdadero si y solo si existe un elemento del CCA de b,

a (t, (min1, max1), (min2, max2)),

tal que

t = tipo,

dominar(min(sia),min1),

dominar(max1,max(sia)),

dominar(min(iia),min2),

dominar(max2,max(iia)).

Acceso-opcional(b1,b2,tipo) devuelve verdadero si y solo si existe un elemento en la UIR de b1,

a (b,t),

tal que

b = b2 y

t = tipo.

Empleando *acceso-obligatorio* y *acceso-opcional*, es posible describir más completamente lo que significa una conexión autorizada. Una conexión de un tipo determinado puede ser autorizada entre dos UIR en unos intervalos de acceso si los accesos obligatorio y opcional son verdaderos para cada computador. Una nueva función *abrir-ok*, devuelve verdadero si es posible autorizar la conexión. Se define como:

abrir-ok(b1, b2, t, ia1, ia2).

donde

(b1, b2) es un subconjunto de B,

t es un elemento de T, y

(ia1, ia2) es un subconjunto de IA,

devuelve verdadero si y solo si

acceso-obligatorio(b1,t,ia1,ia2).

acceso-opcional(b1, b2, t).

acceso-obligatorio(b2, t, ia2, ia1). y

acceso-opcional(b2, b1, t).

Es importante señalar que el que se devuelva un valor verdadero no implica que la conexión se establezca entre b1 y b2 sino que dicha conexión no viola las reglas de seguridad

Un paquete solo existirá en la red si se ha transmitido a través de una conexión autorizada Para manejar todas las conexiones de su computador central, la UIR asigna un número de conexión libre a cada conexión que establece con su computador central Es importante recalcar que dos UIR involucradas en una conexión pueden referirse a dicha conexión con un número diferente Estos números de conexión son elementos de un conjunto, *Conexiones*, CN Cada conexión de una UIR se identifica por un par ordenado (b, cn), donde b es un elemento de B y cn es un elemento de CN La función *nuevo-cn(b)*, donde b es un elemento de B, asigna un número de conexión libre a la UIR, b Esta función se utiliza para abrir las conexiones

En cada UIR hay información residente para cada posible conexión Esto incluye el tipo de conexion, la otra UIR involucrada, y los intervalos de acceso Para suministrar esta informacion, se definen las siguientes funciones

tc(b, cn) - devuelve el tipo de la presente conexión

t: un elemento de T, si la conexión existe

NULL: si no hay conexión

bc(b, cn) - devuelve la UI conectada

bI: un elemento de B si la conexión existe

NULL: si no hay conexión

ncc(c, cn) - devuelve el identificativo de la conexión usado por la otra UIR

cnI: un elemento de CN si existe la conexión

NULL: si no hay conexión

siac(b, cn) - devuelve el límite superior del presente intervalo

ia: un elemento de IA si hay conexión

NULL: si no hay conexión

nac(b, cn) - devuelve el límite inferior del presente intervalo

ia: un elemento de IA si hay conexión

NULL: si no hay conexión

donde

b la UIR implicada - un elemento de B y

cn el identificativo de la conexión - un elemento de CN.

Existen cinco funciones para escribir en la UIR información sobre el estado de la conexión Cada una de estas funciones tiene tres argumentos: la UIR, el identificativo de la conexion, y la información a grabar Se ejecutan exclusivamente a petición del MCA y devuelven verdadero si y solo si la información ha sido grabada adecuadamente Las cinco funciones se definen de la siguiente manera:

s-tc(b, cn, t) - pone el tipo de la presente conexión

b la UIR a poner - un elemento de B

cn el identificativo de la conexión a poner en la UIR - un elemento de CN

t el nuevo identificativo de la conexión - un elemento de T o NULL

s-bc(b1, cn, b2) - pone la UIR a la que está conectado

b la UIR a poner - un elemento de B

cn el identificativo de la conexión a poner en la UIR - un elemento de CN

b2 otra UIR - un elemento de B o NULL

s-ncc(b, cn1, cn2) - pone el número de la conexión en la otra UIR

b la UIR a poner - un elemento de B

cn1 el número de la conexión a poner en la UIR - un elemento de CN

cn2 el número de conexión en la otra UIR - un elemento de CN o NULL

s-siac (b, cn, ia) - establece el límite superior del presente intervalo de acceso

b la UIR a poner - un elemento de B

cn pone el número de la conexión que tiene en la UIR - un elemento de CN

ia el nuevo límite superior del intervalo de acceso - un elemento de IA o NULL

s-iac (b, cn, ia) - establece el límite inferior del presente intervalo de acceso

b la UIR a poner - un elemento de B

cn pone el número de la conexión que tiene en la UIR - un elemento de CN

ia el nuevo límite inferior del intervalo de acceso - un elemento de IA o NULL

El valor NULL indica que la conexión se está terminando

También se crea una función, *actualizar-estado-información()*, como forma apropiada para poner y resetear la información descrita anteriormente. Se define en términos de las cuatro últimas funciones y se ejecuta exclusivamente a petición del MCA

actualizar-estado-información(b1, cn1, b2, cn2, t, ia1, ia2) - será verdadero si y solo si

s-tc(b1, cn, t), s-bc(b1, cn1, b2),

s-ncc(b1, cn1,cn2), s-siac(b1, cn, ia1), y

s-iac(b1,cn,ia2)

y si

t = NULL, b2 = NULL, cn2 = NULL, ia1 = NULL, o

ia2 = NULL entonces t = NULL, b2 = NULL, cn2 = NULL,

ia1 = NULL y ia2 = NULL

La segunda condición existe para que el estado de la información se anule completamente siempre que cualquier parte del estado de la información sea anulada.

El MCA debe llevar la cuenta de todas las conexiones abiertas. Cuando se abre una conexión, el MCA registra el evento introduciendo la correspondiente información en la tabla de conexiones (TC). La TC se define como un subconjunto del Espacio-Conexión que es un producto Cartesiano:

$$Espacio\text{-}Conexión = (B \times CN \times B \times CN \times T \times IA \times AI)$$

El MCA emplea la función *añadir-conexión* para registrar la creación de una conexión en la TC. Esta función introduce dos entradas en la tabla, una por cada UIR implicada. Ambas entradas contienen la misma información. Su definición es:

añadir-conexión(b1, cn1, b2, cn2, t, ia1, ia2) devuelve verdadero si

(b1, cn1, b2, cn2, t, ia1, ia2) y

(b2, cn2,b1, cn1, t, ia2, ia1)

se han añadido a la TC.

El MCA utiliza la función *eliminar-conexión* para borrar las entradas en la TC. A diferencia de *añadir-conexión*, esta función sólo introduce una entrada en la TC. Cuando una UIR notifica al MCA que ya no desea emplear más esa conexión, el MCA invoca

esta función para eliminarla de la entrada del UIR. Esta función se tiene que ejecutar por duplicado para cerrar completamente una conexión.

eliminar-conexión(b1,cn1) devuelve verdadero si *(b1,cn1,b,cn,t,ia1,ia2)* se elimina correctamente de la TC, donde b, cn, t, ia1, ia2, no necesitan ser especificados.

Desde el momento en que el par ordenado (b1, cn1) especifica univocamente una de las conexiones de b1, no es necesario aportar el resto de parámetros.

Ahora ya es posible definir *enviar-paquete()* y *recibir-paquete()*. Cada una de estas funciones devolvera verdadero si se ha completado satisfactoriamente Las dos necesitan cinco argumentos

enviar-paquete(sb, cno, db, cnd, paquete)

recibir-paquete(sb, cno, db, cnd, paquete)

sb la UIR origen - un elemento de B

cno el número de conexión de la UIR origen - un elemento de CN

db la UIR destino - un elemento de B

cnd el número de conexión de la UIR destino - un elemento de CN

paquete el paquete entero que se envia o se recibe - un elemento de P

Está implícito en la definición de ambas funciones que sb, cno, db, y cnd reflejan apropiadamente la dirección de origen y destino del paquete.

Finalmente se incluye, la definición de las funciones *iniciar-conexión y terminar-conexión*. Cada una de ellas devuelve verdadero cuando se inicia o termina una conexión.

El proceso de iniciar una conexión varía dependiendo de qué UIR se trate. Cuando la UIR que pide conexión es la del propio MCA, genera un nuevo número de conexión e informa a la otra UIR de que se ha iniciado una conexión. La otra UIR calcula su propio número de conexión, escribe la información de estado adecuada, y transmite su número de conexión al notificar a la UIR del MCA que está lista. La UIR del MCA ahora tiene la suficiente información para escribir su propia información de estado.

Cuando termina, la UIR del MCA notifica al MCA que la conexión se ha abierto para que el MCA la incluya en la tabla de conexiones. Cualquier UIR que desee abrir una conexión con la UIR del MCA envía una petición de apertura a la UIR del MCA, y ésta entonces procede como si fuera ella la que iniciase el proceso de apertura, siguiendo los pasos descritos anteriormente.

Ninguna UIR puede ir directamente a otra UIR para pedirle abrir una conexión. Para dichas peticiones, el MCA debe ser previamente consultado, a través de su UIR. La UIR que lo solicita (b1) debe abrir una conexión con la UIR de la MCA para preguntar al MCA si le da permiso para abrir una conexión con otra UIR (b2) (para la cual b1 ya ha asignado un número de conexión). Si el MCA no lo permite, entonces la UIR del MCA cierra la conexión. Si el MCA lo aprueba, entonces su UIR abre una conexión diferente con b2, al que se le informa de la petición de b1. Si b2 rechaza la petición, la UIR del MCA lo notifica a b1 y se cierran ambas conexiones. Si la petición se acepta, b2 genera

un número de conexión, establece el estado de la información, y lo reporta a la UIR del MCA. La UIR del MCA envía el número de la conexión de b2 a b1 con instrucciones para establecer el estado de la información y reportarlo de vuelta a la UIR del MCA. Como ahora consideran que la conexión entre ambas está abierta, b1 y b2, ambas, cierran su conexión con la UIR del MCA y el MCA añade la conexión a la TC.

Para terminar una conexión, las acciones a tomar también dependen de qué UIR esté involucrada. Una UIR considera una conexión como terminada cuando su otra mitad está cerrada. La UIR del MCA cierra sus conexiones reseteando sus estados y notificando al MCA que borre la conexión de la TC.

Una UIR que quiera cerrar una conexión con la UIR del MCA debe informarle para que pueda resetearse el estatus de la UIR. Cuando llega la confirmación de que la otra UIR ha sido reseteada, la UIR del MCA resetea el estado de sus información y notifica al MCA para que borre la conexión de la TC. Una UIR que quiera cerrar conexiones en las que no esta implicada la UIR del MCA, debe abrir una conexión con ella para notificar al MCA que la conexión se está cerrando, reseteará su estado de la información cuando se le autorice a hacerlo, y cerrará la conexión con la UIR del MCA. El MCA borra cada extremo de la conexión a medida que se cierra.

La definición de iniciar-conexión es:

iniciar-conexión(b1, cn1, b2, cn2, t, sia, iia)

donde

b1 UIR que solicita el iniciar-conexión - elemento de B

cn1 *parámetro en el que se devuelve el numero de conexión para b1 - elemento de CN.*

b2 *UIR solicitada - elemento de B*

cn2 *parámetro en el que se devuelve el número de conexión para b2 - elemento de CN*

t *tipo de conexión - elemento de T*

sia *limite superior de IA para b1 - elemento de IA*

iia *limite inferior de IA para b1- elemento de IA*

La definición de terminar-conexión es:

terminar-conexión (b1, cn1, b2, cn2)

donde

b1 *UIR que desea cerrar su lado de la conexión*

cn1 *numero de conexión de b1 a cerrar*

b2 *la otra UIR involucrada en la conexión*

cn2 *número de conexión de b2*

Existe otro conjunto, E, que es el conjunto que engloba todos los posibles eventos que ocurren en la red. Algunos elementos de E serán abrir una conexión, enviar un paquete, o añadir un nuevo computador. Otros eventos guardarán relación con la seguridad, como necesidad de ser autorizado. Esto puede ocurrir en la UIR (un paquete con una cabecera inadecuada llega a la UIR) o en el MCA (la petición de una conexión se rechaza).

Hagamos que exista una función, *relevante-seguridad*, donde e es un elemento de E que determina si un evento es relevante en términos de seguridad. También hay otra función,

auditar(e), que provoca que se registre la hora, lugar y las comunidades implicadas en el evento, para que sean auditados en los ficheros de auditoria localizados en el MCA.

Con todo esto, ahora es posible presentar matemáticamente las condiciones que se deben cumplir para respetar las cinco reglas de seguridad establecidas. En el más estricto sentido, la Regla 4 es innecesaria porque se deduce de la Regla 3. Se ha incluido para enfatizar la importancia de que los paquetes lleguen a su destino sin ninguna alteración.

Estas cinco reglas de seguridad quedan formuladas de la siguiente manera:

Regla 1. *Para todo elemento p, de P, existe un elemento l, del Espacio-C, tal que etiquetar(p) l.*

Regla 2: *Para cualquier elemento b, de B; cn, de CN; y p, de P; b puede transmitir p en cn si y solo si enviar-paquete(b, cn, bc(b, cn), nce(b, cn), p) - verdadero.*

Regla 3: *Para cualquier elemento b, de B; cn de CN; y p de P; b puede distribuir un p recibido en cn si y solo si recibir-paquete(bc(b, cn) , nce(b, cn), b, cn, p) - verdadero.*

Regla 4: *Para cualquier elemento b1 y b2, de B; cn1 y cn2 de CN; y p de P; si recibir-paquete(b1, cn1, b2, cn2, p) - verdadero, entonces no-alterar(p) - verdadero.*

Regla 5: *Para todo elemento e, de E, si relevante-seguridad(e) - verdadero, entonces auditar(e) - verdadero.*

4.3. Síntesis de factores claves complementarios con el Modelo de Seguridad Avanzado del NAAP, que condicionan la percepción de un sistema de seguridad, y su estructuración.

Para implementar un sistema de seguridad global, las funcionalidades aportadas por el modelo de seguridad MOSA incorporado en el NAAP se complementa con una serie de actitudes y compromisos de alto nivel recogidos en las siguientes necesidades

a) Conocer los posibles perfiles de atacantes.

Se considera quién podría querer sobrepasar nuestras medidas de seguridad para identificar sus motivaciones, determinando qué busca y qué daño puede causar a nuestra red

Las medidas de seguridad nunca harán imposible al 100% que un usuario pueda llegar a realizar tareas no autorizadas. Solamente podrán hacerlo más difícil

b) Parametrizar el esfuerzo y coste añadido.

Las medidas de seguridad casi siempre provocan inconvenientes extras a los usuarios autorizados La seguridad bien implementada no debe retrasar el trabajo y crear una carga costosa en la gestión y administración del sistema, implicando además el uso excesivo de recursos significativos y hardware dedicado

En el proceso de diseño de las medidas de seguridad se debe estimar su coste frente a los potenciales beneficios, estudiar si se destinan unos recursos desproporcionados a los

daños que se podrían llegar a producir, y lograr un necesario equilibrio.

c) Identificar lo que se da por supuesto.

Todo sistema de seguridad tiene sus propias premisas. Por ejemplo, que ciertos caminos en la red no tienen un trazado alternativo, o que los intrusos saben menos que nosotros o que emplean programas y equipos que no son muy sofisticados, o que una habitación cerrada es un sitio seguro. Las personas responsables de la seguridad no deben trabajar con suposiciones, por poder éstas llegar a ser, posibles agujeros en la seguridad del sistema.

d) Controlar nuestros secretos.

La mayor parte de la seguridad se basa en los secretos Por ejemplo, los "passwords" y las claves encriptadas son secretos, y suele suceder frecuentemente que los secretos no son tales secretos

Los secretos protegen algo y muchas veces la parte más importante de mantener secretos es conocer qué áreas se tienen que proteger. Si éstas son excesivas, más esfuerzo habrá que poner en mantenerlos todos. El sistema de seguridad debe estar diseñado para que solamente se tengan que mantener un número limitado de secretos

e) Recordar los factores humanos.

Muchas medidas de seguridad fallan porque sus diseñadores no han considerado cómo reaccionarán los usuarios ante ellas. Por ejemplo, se pueden encontrar "password" escritos al interpretar que así son más fáciles de manejar, las puertas que dan acceso a

consolas de gestión con perfiles altos están abiertas por conveniencia, módems no autorizados o accesos a PADs suelen estar habilitados sin ninguna protección alegando temporalidad o urgencia en su uso, y después caen en el olvido permanente...

El modelo de seguridad del NAAP no interfiere con el uso esencial del sistema, y por lo tanto no encontrará resistencia pasiva, facilitando así su desarrollo. Para obtener una cierta complicidad se asegura que los usuarios puedan hacer su trabajo, y como todo en la vida, se debe saber vender las medidas de seguridad, a los usuarios, dirección... Cualquier usuario puede comprometer la seguridad del sistema y por ello deben entender y aceptar la necesidad de seguridad.

f) Limitar el ámbito de acceso.

Se crean las apropiadas barreras dentro del sistema para que si los intrusos acceden a una parte del sistema, no tengan acceso automático al resto del sistema. La seguridad del sistema es sólo tan buena como el nivel de seguridad que tenga su elemento más débil

g) Conocer el entorno.

Para implementar estas medidas de seguridad complementarias al modelo de seguridad interno del NAAP, debe realizarse un profundo esfuerzo en entender cómo funciona el sistema, conocer qué se espera de él y qué no, y estar familiarizado con el uso normal de los dispositivos. Esta actitud ayuda a detectar problemas de seguridad

h) Recordar la seguridad física.

El acceso físico a un nodo de comunicaciones puede dar a un persona con los suficientes

conocimientos, un control total sobre el sistema. El acceso físico sobre un enlace de red, permite a una persona modificar ese enlace, meter tráfico en él...No tiene sentido instalar complicadas medidas de seguridad a través del NAAP si el acceso al hardware no está protegido.

i) La seguridad es permeable.

Casi todos los cambios que se realicen en el sistema pueden tener efectos colaterales en la seguridad Esto es especialmente crítico cuando se crean nuevos servicios. Administradores de redes, operadores de gestión, etc., con la implicación del NAAP, se ven ayudados a la hora de considerar las implicaciones en la seguridad que cualquier cambio puede provocar. Comprender dichas implicaciones es algo que requiere práctica.

Finalmente, para completar el plan de seguridad, también se debe contemplar la capacidad de enfrentarse a los problemas una vez que estos aparecen. Los desastres ocurren, y su impacto resulta mucho mayor cuando una vez que se dan, no se responde con medidas concretas, en un plazo de tiempo limitado y adecuado. La magnitud de los problemas ocasionados puede ser variable y por ello hay que se estar preparado pudiendo tener personal disponible y capacitado, teniendo procedimientos de recuperación que tengan en cuenta prioridades en los enlaces y transmisión de datos, planes de intervención en campo avalados con disponibilidad de equipos suficiente y logística apropiada, y procurando que todo este proceso sea lo más trasparente posible al cliente.

4.4. Métrica de ia incidencia del Protocolo de Gestión de Red en la seguridad y robustez de un Sistema de Gestión de Red.

Dentro del esquema general marcado por la relación existente entre las alarmas generadas en la red y los eventos recibidos como consecuencia de ellas, no hay que olvidar que además de los requisitos y limitaciones de tiempo en su gestión, se introduce un nuevo y muy importante factor que es la veracidad y consistencia de la información que se recibe o que la propia red genera.

Se debe tener seguridad de que todos los mensajes se reciben tal y como se enviaron, y para que el supuesto receptor y no otro reciba el mensaje

La integridad se complementa perfectamente con procesos de cifrado, transformando un mensaje legible en otro equivalente que ya no lo es para un receptor no autorizado. En este punto, se tendrán en cuenta factores como el transporte de la clave de cifrado, su seguridad, recursos de computación destinados al proceso, etc

Existe además la posibilidad de que las alarmas normalmente asociadas con un problema se puedan perder en su transmisión por diferentes razones, produciendo que los indicadores directos para un problema no existan. Estas evidencias no siempre son transparentes y el sistema debe ser capaz de inferir la existencia de un problema

Esta situación adquiere una nueva dimensión cuando el causante de la ausencia de

alarmas , de su pérdida, o de la no garantía en su seguridad, no es la propia red en su origen, ni la plataforma y sus aplicaciones con un incorrecto tratamiento en el destino, sino que indirectamente es el propio protocolo de gestión de red.

A simple vista parece razonable nuestra fe ciega en los protocolos de transporte, pudiendo suponer tranquilamente que no tienen ninguna incidencia en la gestión de la red, y en consecuencia ignorarlos, pero en este complicado mundo esta ausencia de dudas puede tener una incidencia negativa. A continuación demostraré que esta situación puede ser realmente un importante agujero del sistema.

4.4.1. Validación de la factibilidad del uso masivo de SNMP v.1. en entornos seguros, razonando con datos incompletos.

A medida que SNMP se ha ido empleando en labores de gestión y no solamente de monitorización, la simplicidad de la que hacía gala y que al principio fue una de sus principales ventajas, se transformó en su punto más débil por su escaso nivel de seguridad

El NAAP también aborda la influencia que SNMP tiene en el razonamiento con datos incompletos

El transmisor y herramienta primitiva con la que se gestionan los dispositivos en la red es el propio protocolo de gestión de red, que en definitiva dictamina la forma en que la

información viaja. Este movimiento de información proveniente de múltiples fuentes puede ser fruto de la adquisición de datos durante un proceso de consulta o decisión, o excepcionalmente, como fruto de una interrupción originada por un dispositivo para informar a su gestor sobre una situación anómala. Siempre se puede dar el caso de que alguna información se pierda y con esta restricción, el proceso de solución del problema debe tener la posibilidad de encontrar una solución empleando los datos disponibles.

Cuando el agente de un elemento de red genera un "trap", SNMP confía ciegamente en que dicha alarma llegue hasta el gestor. Esta fe puede no verse correspondida y la estación gestora no se dará cuenta. Este es un potencial foco de problemas en las Plataformas de Gestión de Red, que si bien son subsanables indirectamente, no deja de contribuir a la necesidad de uso de un NAAP en tiempo real.

Con SNMP no existe ninguna protección ante la pérdida de sus mensajes debido a la encapsulación de mensajes SNMP en datagramas UDP. Sin embargo, intentando solucionar esta deficiencia, la estación gestora afrontará, indirectamente a través del NAAP, la recuperación de los mensajes de tipo "solicitud" y "respuesta", detectando su pérdida por la ausencia de respuesta al expirar el correspondiente "timer". Para mensajes tipo *Get-Requests* y *Get-Next-Requests*, la estación gestora retransmite la petición durante un número finito de veces; si ninguno de los intentos tuviera éxito, asume que o bien el agente se ha caido o que la conectividad con el agente se ha perdido.

La recuperación de una no respuesta a un *Set-Request* también es posible efectuando un *Get-Request* para determinar si tuvo éxito el *Set-Request* anterior.

Sin embargo, los traps no son recuperables. No hay ningún mensaje de respuesta a un trap y no hay forma se saber si llegó a la estación gestora. Esto es un punto importante a la hora de planificar la gestión bajo SNMP. Efectivamente, afirmo que los traps solamente pueden utilizarse como un sistema de aviso temprano: debe existir una forma alternativa para descubrir si se ha producido un evento significativo, como el realizar un sondeo con una cadencia apropiada originado por el NAAP, en la búsqueda de posibles problemas en la red.

Con esta peculiaridad de SNMP, el NAAP es capaz de discernir en los modelos de red con los que trabaja, hasta qué punto puede permitir el concepto de persistencia sin añadir mecanismos directos o capaces de inferir el estado real de los dispositivos. La representación facilita inferencias de la forma "si el hecho P ahora es verdadero, será cierto hasta que se demuestre lo contrario", pero siendo conscientes de la incidencia que puede tener la no verificación por parte del protocolo de la llegada al destino de los traps

4.5. Definición y ajuste de criterios para afrontar el componente "tiempo" del dominio propio de las plataformas.

"Durante la semana pasada se dieron ciertas irregularidades atribuibles en principio a la calidad de línea de un enlace de 2M. (conclusión posterior) entre Bilbao y Barcelona. Esto produjo quejas de varios clientes el Lunes, Martes y Jueves, debido a

interrupciones en la transmisión de datos. Simultáneamente alguno de estos clientes también presentó fallos en sus módems de alta velocidad. Además el nodo que contenía los módems de comunicaciones de los troncales en Barcelona, falló parcialmente en su hardware teniendo efectos colaterales añadidos al final de la semana."

Esta sucesión de hechos, que constituye un auténtico quebradero de cabeza para los operadores de una red de telecomunicaciones y mantenimiento, se desarrolla en un espacio temporal limitado: una semana.

El solapamiento de incidencias en una red activa es constante y es necesario tener recursos para ubicarlos temporalmente de manera que puedan ser tratados automatizadamente. Imaginemos que el periodo de tiempo que transcurre en el ejemplo no es una semana sino unas horas. Esto complica bastante más la situación puesto que el número de alarmas recibidas será enorme

Para poder empezar a procesar toda la información, es necesario en primer lugar, un paradigma de representación y razonamiento apropiado a las características especiales de este dominio en particular. Características especiales que he agrupado y desarrollado de la siguiente forma:

a) Los cambios tecnológicos se suceden a un ritmo abrumador, causando un cuello de botella en la adquisición del conocimiento y en el desarrollo de personal experto. Profesionalmente implica la necesidad de un reciclaje continuo. Las estructuras y esquemas de representación del conocimiento aplicados en otros campos, no tiene por

qué ser siempre apropiados aqui. Los operadores se suelen basar en un conocimiento muy fundamentado en la experiencia más que en heuristicas formalizadas o modelos de dominio estructurados. Su conocimiento está basado en "casos". El conocimiento exclusivo sobre el dominio no es suficiente para alcanzar el rendimiento mostrado por los expertos. Las personas que desarrollan estas tareas adquieren otro tipo de conocimiento, la "experiencia", que les permite concentrarse en las causas más probables del problema y adoptar respuestas especificas a problemas generales.

b) El nivel creciente en la complejidad de un sistema dinámico como éste, causa que la tarea de toma de decisiones sea en ocasiones bastante difícil.

Las aplicaciones software al uso, sólo capturan una foto de este conocimiento cambiante, y se reciclan en la medida que lo hacen las personas responsabilizadas de su mantenimiento. Esto nos lleva, a necesitar y solicitar como claro requisito en sistemas futuros, el auto-aprendizaje del NAAP, incorporando la habilidad real de aprender de sus "experiencias" satisfactorias y de sus fallos.

c) Distribución del control en algunos niveles y descentralización en otros.

El conocimiento y precisión de las aplicaciones se irá mejorando con la incorporación de sistemas que permitan mantener repositorios de conocimiento corporativo para cada área, sin la necesidad de agruparlo todo bajo una visión unificada y permitiendo su gestión distribuida

d) Control en tiempo real de un entorno activo.

La necesidad de respuesta en tiempo real es inherente a muchas operaciones de red, tales

como el control del tráfico. El tiempo de intervención es crucial y sin embargo, muchas veces las reacciones humanas desafortunadamente, excesivamente lentas. Las funciones del humano deberán tender a ser solamente de supervisión, a medida que la cobertura de las aplicaciones se amplie, abarcando otras tareas complementarias a las funciones clásicas de aviso y monitorización, como son las de control.

La representación basada en reglas ha sido la tecnologia básica empleada en un amplio abanico de problemas del mundo real. Ofrece un potencial apropiado aplicado a un propósito ge- al, pero se muestra insuficiente en los requisitos de red

El razonamiento basado en modelos es especialmente apropiado en el diagnóstico y solución de problemas, especialmente cuando falta información, ya que trabaja interactuando con la observación del comportamiento del dispositivo y la predicción basada en el modelo de red. Trabajaria con la premisa de que el modelo es correcto y que todas las discrepancias entre la observación y la predicción surgen de un defecto del dispositivo. Sin embargo, esta clase de razonamiento puede ser empleado cuando el sistema puede ser formalmente modelado y no contiene excesivas interrelaciones, situación que no suele ser lo normal en entornos de red, ya que es dificil modelar una red completa. Se podrian estructurar modelos individuales para ser empleados en un enfoque al dominio completo.

Al razonamiento basado en casos, se le da una descripción de cómo reconocer, tratar y monitorizar el problema. Estas descripciones son los casos, en la forma de experiencias pasadas. El sistema debe encontrar un caso relevante para confrontarlo con el problema.

g) Manejar eficientemente las entradas de estímulos externos, más allá de los humanos.

En una red los datos tienen su origen en sensores y elementos físicos diversos. El software maneja esa información y trata satisfactoriamente estímulos externos, sin conformarse con las solicitadas al operador e introducidas por teclado.

h) Garantizar tiempos de respuesta.

Es necesario asegurar una respuesta en un tiempo finito. Se debe tender a no esperar un tiempo preciso de ejecución de un proceso de cálculo, sino a diseñar el sistema de una manera lo suficientemente flexible como para que sea capaz de responder eficazmente dentro de un abanico de requisitos temporales, independientemente de la configuración del sistema, del estado inicial del que parte, etc. Debe hacer en cada momento el mejor uso del tiempo de computación y de los recursos disponibles.

Por lo general, como pauta de comportamiento genérica el NAAP posibilita respuestas temporalmente correctas, a costa de sacrificar el aspecto funcional, produciendo resultados menos deseables. Es decir, a medida que aumenta el tiempo disponible para el cálculo, la solución dada podría ser más exacta, pero se debe optar por primar el requisito temporal

En general, estas dificultades añadidas explican la dificultad que el tratamiento de la variable "tiempo" produciría en el diseño del presente NAAP aplicado a la Gestión de Red. La mejora de los aspectos informáticos deberán permitir a más largo término introducir progresivamente formalismos generales para expresar conocimiento temporal,

que en las versiones actuales de los lenguajes se encuentran en un estado primitivo. Esta lógica evolución, potenciará el desarrollo de herramientas aplicables a este aún por explotar y atractivo mundo de las Telecomunicaciones: los Sistemas de Gestión de Red.

5. Conclusiones

En este previsible caminar, y como objeto principal de la Tesis, se diseña un nivel lógico avanzado e integrador de los factores seguridad y tiempo real para su aplicación en un Sistema de Gestión de Red Automatizado. Este diseño se logra satisfaciendo dos objetivos claves:

1°) El primer objetivo es estructurar y diseñar las relaciones y funcionalidades criticas para una integración positiva de las aplicaciones de Gestión de Fallos con las Plataformas de Gestión de Red.

En este sentido, y como paso previo, se estructura el marco en que los Sistemas de Gestión de Red se mueven y en el que se encuadran todas las acciones, funciones e información que se emplea para planificar, organizar, ejecutar y controlar con efectividad una red de comunicaciones. Para ello se define y diseña la arquitectura **ASSEF** (Arquitectura de Soporte al Software de Gestión de Fallos) para la Gestión de Comunicaciones en un entorno WAN generalizado. En el desarrollo de la arquitectura ASSEF se llevan a cabo los siguientes pasos:

a) Desarrollo funcional.

b) Síntesis del componente estructural, que da también lugar a una estructuración jerárquica de la red y a la elaboración de una métrica para determinar el grado de gestión descentralizada adecuado.

c) Diseño del componente interface. En este apartado también se realiza una

aproximación concreta a los procesos de red, dejando abiertas futuras vías de investigación que sirvan para sintetizar procesos y que aporten modelos de relación basados en dicha arquitectura ASSEF.

Una vez diseñado el ámbito en que toda Gestión de Fallos se desarrolla, y aún constituyendo un muy adecuado cimiento sobre el que construir toda una gestión integrada, el conjunto formado por una Plataforma de Gestión junto con sus aplicaciones adolece actualmente de herramientas y principios de actuación elaborados que tengan en cuenta elementos y situaciones especificas propias de un entorno caracterizado principalmente por desarrollarse en tiempo real y con imperativos muy elevados de seguridad, rigor y exactitud en las actuaciones que en él se desencadenan

Es por ello que se sintetiza un nivel de soporte a decisiones especificas de cierta complejidad a tomar por las aplicaciones que funcionan sobre las Plataformas: **NAAP** (Nivel Avanzado de Apoyo a Plataformas de Gestión), adaptando por tanto, su funcionalidad a la gestión de red en tiempo real.

También se aportan claves para su representación e implementación algoritmica con un modelo concreto para la detección de problemas y su diagnóstico. Para realizar un acercamiento a la representación exacta del conocimiento propio del entorno, este modelo empleará el conocimiento estructural o topologia de red, las deducciones o tipos de datos creados y manipulados durante el razonamiento, y el conocimiento sobre la detección de problemas, o lo que es lo mismo, cómo interpretar los eventos de la red, cómo reconocer los problemas y cómo enfrentarse a ellos.

Finalmente, para completar el valor añadido del NAAP y su contribución a las aplicaciones de gestión de red actuales, se diseña el método **CNOD** (Cuantificación de la Necesidad y su repercusión en los Objetivos basado en Lógica Difusa), que mejora el comportamiento humano a la hora de reaccionar ante los eventos de la red, pudiéndose implementar e integrar como un módulo software dentro del NAAP. Este método se elabora para ayudar por un lado al gestor de la red y por otro, para poder incorporar dentro de las Plataformas de Gestión la posibilidad de trabajar con objetivos dando respuesta a una situación cambiante en la búsqueda de metas, a través de una cuantificación de la necesidad y permitiendo así establecer una relación directa entre los recursos de la red, las prioridades de empresa y la probabilidad en los diagnósticos realizados por el NAAP.

El método CNOD automatizando la mecánica de operación, es capaz de simular expresiones imprecisas del lenguaje humano, puede enfrentarse a situaciones compuestas por múltiples estímulos concurrentes y destaca por la facilidad que proporciona para influir dinámicamente, tanto sobre la importancia que se le quiere dar a las probabilidades que el NAAP asigna a sus diagnósticos, como sobre las prioridades que en cada momento el Centro de Operaciones de Red pueda establecer internamente.

2°) Las características de seguridad en los entornos de red y su tratamiento concreto, conforman otro de los objetivos de la presente Tesis. Teniendo como finalidad que la seguridad de red, en su más amplio concepto, debe incorporarse como elemento imprescindible de los Sistemas de Gestión de Red, y no como valor añadido a implementar de una forma complementaria y sin ninguna integración con las Plataformas

o con las aplicaciones que sobre ellas funcionan, se establece la necesidad de un discriminador de amenazas basado en un estudio empírico en un entorno real, con varios casos de accesos múltiples a través de PAD/FRAD/IFRAD.

En este área se diseña, especifica y concreta el **MOSA** (Modelo de Seguridad Avanzado), formulándolo matemáticamente. De este modo se especifican un conjunto de reglas para mejorar la calidad del proceso de seguridad de una red, integrando el MOSA en el NAAP.

Igualmente se realiza una síntesis e integración de factores claves complementarios con el MOSA, que condicionan la percepción de un sistema de seguridad y su estructuración, y se modelizan, esquematizan y acotan las vulnerabilidades de una arquitectura actual para la Gestión de Comunicaciones WAN.

Dentro del esquema general marcado por la relación existente entre las alarmas generadas en la red y los eventos recibidos como consecuencia de ellas, no hay que olvidar que además de los requisitos y limitaciones de tiempo en su gestión, se debe introducir un nuevo y muy importante factor que es la veracidad y consistencia de la información que se recibe o que la propia red genera. Se debe tener seguridad de que todos los mensajes se reciben tal y como se enviaron, para que el supuesto receptor y no otro reciba el mensaje.

Esta situación adquiere una nueva dimensión cuando el causante de la ausencia de alarmas , de su pérdida, o de la no garantía en su seguridad, no es la propia red en su

origen, ni la plataforma y sus aplicaciones con un incorrecto tratamiento en el destino, sino que indirectamente es el propio Protocolo de Gestión de Red. Este apartado aborda también la influencia que SNMP tiene en el razonamiento con datos incompletos y la correlación en el tiempo.

Finalmente, completo este segundo objetivo con un diseño adaptativo de criterios para afrontar el componente tiempo del dominio propio de las plataformas, y sintetizando las facilidades y requerimientos relativos a dicho factor, que el NAAP orientado a la Gestión de Red puede llegar a aportar en un entorno integrado con las Plataformas de Gestión de Red. Es dentro de este campo, y concretamente en la necesidad de garantizar tiempos de respuesta finitos, independientemente del estado y carga de trabajo del NAAP, donde se abren nuevas posibilidades de investigaciones posteriores.

Bibliografía

[ABRA87] Abrams, Marshall D., Podell, Harold J., "Tutorial Computer and Network Security". IEEE Computer Society Press, (1987)

[AFEK96] Afek, Y., Awerbuch, B., Plotkin, S.A., Sanks, M.,"Local Management of a Global Resorce in a Communication Network", pág. 1-19, Journal of the ACM, Vol. 43, N° 1, (Enero 1996).

[AMOR94] Amoroso, E., "Fundamentals of Computer Security Technology". Prentice-Hall, Englewood Clifs, New Jersey, (1994).

[AMSE88] Amsel, E. "Network Security and Access Controls". Computers and Security, vol. 7, n° 1, pp 53-57, (1988).

[AREI96a] Areitio, J., Garay, L.M. "Gestión de Red: Consideraciones en torno a la seguridad". Mundo Electrónico, n° 263. (Enero 1996).

[AREI96b] Areitio, J., Garay, L.M. "Plataformas de gestión de red: Análisis del comportamiento en tiempo real". Automática e Instrumentación n° 263 (Abril 1996).

[ASHA88] Ashany, R., Ferrari, D., Pasquale, J., "Application of IA Techniques to Adaptive Routing in Wide-Area Networks". Proc. of the Seventh Annual International Phoenix Conference on Computers and Communications, AZ, pp 157-160, (1988).

[BALL92] Ball, L., "Network Management Standards". McGraw-Hill, New York, (1992).

[BARB88] Barber, K., Nelson L. D., "Security Standards - Goverment and Commercial". AT&T Technical Journal, (Mayo - Junio 1988).

[BAY95] Bay, P., Bilardy, G.,"Deterministic On-Line Routing on Area-Universal Networks", pág. 614-640, Journal of the ACM, Vol. 42, N° 3, (Mayo 1995).

[BAYL88] Bayle, A.J., "Security in an Open System Network: A Tutorial Survey". Information Age, Vol. 10, N° 3, (Julio 1988).

[BEAM93] Beam, A., Wood, D., Fairclough, W., "Specifying Goal-Oriented Network Management Systems", pág. 30-36, IEEE Communications Magazine, (Mayo 1993).

[BLAC88] Black, U., "Physical Level Interfaces and Protocols". IEEE Computer Society Press, New York, (1988).

[BLAC90] Black, U., "Computer Networks Protocols, Standards and Interfaces". Prentice-Hall, Inc., (1990).

[BLAC92] Black, U., "TCP/IP and Related Protocols". Prentice-Hall, Inc., (1992).

[BOUL94] Bouloutas, A. T., Calo, S., Finkel, A., "Alarm Correlation and Fault Identification in Communication Networks", pág. 523-533, IEEE Transactions on Communications, Vol. 42, N° 2/3/4, (Feb./Marzo/Abril 1994).

[BRAN82] Branstad, K., Smid, M. E., "Integrity and Security Standards Based on Cryptography". Computers and Security, (1982).

[BRIE83] BrieCAy, B. B., "Introduction to Telephone Switching". Addison-Wesley, Reading, MA, (1983).

[CARN85] Carne, E. B., "Modern Telecommunications". Plenum Publishing, New York (1985).

[CAVA92] Cavanagh, J. P., "AppCAying the Frame Relay Interface to Private Networks", pág. 48-64, IEEE Communications Magazine, (Marzo 1992).

[CHAN91] Chandrasekaran, B., Bhatnagar, R., Sharman, D. D., "Real-Time Disturbance Control", pág. 33-47, Communications of the ACM, Vol. 34, N° 8, (Agosto 1991).

[CHES94] Cheswick, W. R., Bellovin, S. M., "Firewalls and Internet Security". Addison-Wesley, (1994).

[CLAR87] Clark, D., Wilson, D. R., "A comparison of commercial and military computer security policies". Proc. 1987 IEEE Symp. on Security and Privacy, (1987).

[CLAR92] Clark, D., Shewker, S., Zhang, L.,"Supporting real-time applications in an integrated services packet network: Architecture and mechanism", pág. 14-26, Proc. ACM SIGCOMM'92, (Agosto 1992).

[CMU94] Waldbusser, Steve. "lancaster.andrew.cmu.edu - pub/cmu-snmp1.0.tar". Carnegie-Mellon University.

[COLB87] Colbourn, C. J., "The combinatorics of network reliability". Oxford University Press, New York, (1987).

[COLL96] Collins, O., "Crytographic Redundancy and Mixing Functions", pág. 423-426, IEEE Transactions on Communications, Vol. 44, N° 4, (Abril 1996).

[COME91] Comer, D., "Internetworking with TCP/IP". Volume I, 2nd Edition, Prentice-Hall, New Jersey, (1991).

[CRAW88] Crawford, J.L., "Network management using object-oriented graphics". Proceedings of the IEEE Workshop on the Application of Energy Technologies in Network Operations and Management, (1988).

[CRON89] Cronk R. N., Callahan P. H., Bernstein L. "Rule-Based Expert Systems for Network Management and Operations: An Introduction". Expert Systems Applications in Integrated Network Management, Artech House, (1989).

[COWO94] Comunicaciones World. "Gestión de redes". pp 35-45, (Dic. 1994).

[COWO95] Comunicaciones World. "Gestión y administración de red bajo el imperio de SNMP". (Feb. 1995)

[DAIG90] Daigle, A , "Queuing theory for Telecommunications". Addison-Wesley, Reading, Mass. (1990).

[DAWE95] Dawes, N., Altoft, J., Pagurek, B., "Network Diagnosis by Reasoning in Uncertain Nested Evidence Spaces", pág. 466-476, IEEE Transactions on Communications, Vol. 43, N° 2/3/4, (Feb./Marzo/Abril 1995).

[DEER90] Deering, S.E.,"Multicast routing in internetworks and extended LANs", pág 85-110, ACM Trans. Information Systems, 8, (2), (1990)

[DENN89] Denning, D.E., "Cryptography and Data Security". Addison-Wesley, Reading, Mass. (1989).

[DENN90] Denning, P., "Computers Under Attack: Intruders, Worms and Viruses". ACM Press, Addison-Wesley Publishing Company, Reading, Mass (1990)

[DEWA93] Dewan, P., Chouldhary, R., "A High-level and flexible framework for implementing multiuser interfaces", pág. 345-380, ACM Trans Information Systems, 10, (4), (1993).

[DIFF88] Diffre, W., "The First Ten Years of Public-Key Cryptography". Proceedings of the IEEE, Vol. 76, N° 5, (Mayo 1988).

[DUPU90] Dupuy, A., Schwartz, J., Yemini, Y., Bacon, D., "NEST: A network simulation and prototyping tested", pág. 63-74, Communications of the ACM, Vol. 33, N° 10, (Octubre 1990).

[EGAN91] Egan, B. L., "Information Superhighways, the Economics of Advanced Public Communication Networks". Artech House, NorWood, MA, (1991).

[FERR87] Ferris, M., Cerulli, A., "Certification: A Risky Business". Proceedings of the 10th National Computer Security Conference, (1987).

[FILI91] Filipiak, J., "AnaCAysis of Automatic Network Management Controls", pág. 1777-1786, IEEE Transactions on Communications, Vol. 39, N° 12, (Dic. 1991).

[FRAN81] Franklin, F. Kuo, "Protocols & Techniques for Data Communication Networks". Prentice-Hall, Inc., New Jersey, (1981).

[FREE89] Freeman, R.L., "Telecommunications System Engineering". Second Edition, John Wiley and Sons. Chichester (1989).

[GARA96] Garay, L.M., Areitio, J., "Sistemas de Gestión de Red: Una necesidad urgente". Base Informática, n° 28. (Mayo 1996).

[GOUD95] Gouda, M. G , Netravali, A. N., Sabnani, K., "A Periodic State Exchange Protocol and Its Verification", pág. 2475-2483, IEEE Transactions on Communications, Vol 43, N° 9, (Sept. 1995).

[HENS93] Henshall, J , Shaw, A., "OSI Explained. End to End Computer Communication Standards ". Second Ed. Ellis Horwood. England. (1993).

[HELD92] Held, G , "Network Management: Techniques, Tools, and Systems". Wiley, New York, (1992)

[HOFF77] Hoffman, L. J , "Modern Methods for Computer Security and Privacy", Prentice-Hall, Englewood Cliffs, New Jersey, (1977)

[JENN93] Jennings, Fred, "Practical Data Communications: Modems, Networks and Protocols" Blackwell Scientific Publications, (1993).

[KARE90] Karen, A F., "The european community and information technology", pág. 405-410, Communications of the ACM, Vol. 33, N° 4, (Abril 1990).

[KEIT88] Keith G. K., Terry, L. J , "Standards for Open Systems Interconnection". MacGraw-Hill, (1988)

[KENT86] Kent, S. "Encrytion-based Protection Protocols for Interactive User-Computer Communication". S.M. thesis, MIT Department of Electrical Engineering and Computer Science, (Mayo 1986)

[KERS90] Kershenbaum, A., Malek, M., Wall, M., "Network Management and Control" Plenum Press, New York, (1990).

[KIM90] Kim, B.G., "Current Advances in LANs, MANs and IDSN". Artech House, Norwood, MA. (1990).

[KLIR94] Klir, G J., Folger, T. A., "Fuzzy Sets, Uncertainty and Information". Prentice Hall, Englewood Cliffs, New Jersey (1994).

[KUBA92] Kubat, P., Lam, C. Y. T., "Optimal Monitoring Strategies for SlowCAy Deteriorating Repairable Systems", IEEE Transactions on Communications, Vol. 40, N° 4, (Abril 1992).

[LAZA91] Lazar, A., Pacifici, C., "Control of resources in broadband networks with quality of service guarantees", pág. 66-73, IEEE Communications Magazine, (Oct. 1991).

[LEIN93] Leinwand, Allan, Fang, Karen. "Network Management: A Practical Perspective". Addison-Wesley (1993).

[LAFF89] Laffey T. J., Cox P A., Schmidt J. L., Kao S. M., Read J. Y., "Real-Time Knowledge-Based Systems". Expert Systems Applications in Integrated Network Management, Artech House , pp 133-150 (1989).

[LEBL89] LeBlanc, R., Robbins, A., "Event-driven monitoring of distributed programas in Tutorial: Distributed Software Engineering". IEEE Computer Society Press, (1989).

[LEIN93] Leinwand, A., Fang K., "Network Management: A Practical Perspective" Addison-Wesley, Reading, Mass., (1993).

[LOBE91] Lobel, J., "Foiling the System Breakers". McGraw-Hill, (1991).

[MADR91] Madron, T., "Enterprise-Wide Computing". John Wiley and Sons, Inc. New York (1991).

[MADS90] Madsen, J., "A lower cost on High Performance". Satellite Communicactions, (February 1990).

[MAST88] Mastascusa, E. J., "Computer-Assisted Network and System AnaCAysis", John Wiley & Sons, Inc., (1988).

[MCCA86] McCalmont, Arnold M , "End-to-End Encryption in X.25 Packet Switched Networks". Proceedings of the 1986 Phoenix Conference on Computers and Communications, pp 53-56 (1986).

[MACP90] Macpherson, A.C., "International Telecommunications, Organizations and Standards". Artech House, Norwood, MA, (1990).

[MEUN88] Meunier, J.M , "An Interactive Display System for Network Management". Proceedings of IEEE Network Operations & Management Symposium (1988).

[MCQU92] McQuillan, J. M., "Broadband Networks- The End of Distance". Data Communications, (Junio 1992).

[MELL83] Mellichamp, D., "Real-Time Computing". Van Nostrand Reinhold, New York, (1983).

[MIBP96] MIBs propietarias. "Zippy.Telcom.Arizona.EDU - /pub/mibs".

[MICH85] Michelson, A. M., Levesque, A. H., "Error-Control Techniques for Digital Communication". John Wiñey & Sons, New York (1985).

[MILL90] Miller, Marck A., "LAN Protocol Handbook". M&T Booksl, (1990).

[MILL91] Miller, Marck A., "Troubleshooting InterNetworks". M&T Books, (1991).

[MINO91] Minoli, D., "The New Wide Area Networking Technologies: Frame Relay Network Computing". Network Computing (Mayo 1991).

[MINO93a] Minoli, D., "AnaCAytical Design Techiniques for Broadband Networks". Artech House, Norwood, MA, (1993).

[MINO93b] Minoli, D., "Enterprise Networking: Fractional T1 to SONET, Frame Relay to BISDN". Artech House, Inc., (1993).

[MOAY94] Moayeri, N., "On the Memory Sharing Problem", pág. 1490-1495, IEEE Transactions on Communications, Vol 42, N° 2/3/4, (Feb./Marzo/Abril 1994)

[MURA95] Murata, H., "Handbook of Optical Fibers and Cables". Third De. Marcel Dekker, Inc., New York, (1995).

[NANC94] Nance, Barry, "Introduction to Networking", 3rd Edition, Que Corporation, (1994).

[NANY90] Nanying, Y., San-Qi, L., Stern, T. E., "Congestion Control for Packet Voice by Selective Packet Discarding", pág 674-683, IEEE Transactions on Communications, Vol 38, N° 5, (Mayo 1990)

[NASS94] Nassar, D J., "Network Optimization and Troubleshooting". New Readers Publishing, (1994).

[NAUG94] Naugle, M., "Network Protocol Handbook". McGraw-Hill, Inc., (1994).

[PAUL91] Paul, C. J., Acharya, A., Black, B., Strosnider, J. K., "Reducing Problem-Solving Variance to improve predictability", pág. 80-93, Communications of the ACM, Vol. 34, N° 8, (Agosto 91).

[PIAT95] Piattini, Mario, "Métodos y herramientas CASE orientadas a objetos - Aplicaciones reales: Lecciones aprendidas". WorkShop sobre Tecnologías Orientadas a Objetos -Unidad de Estrategia Tecnológica - SPRI, S.A (1995).

[RABI88a] Rabie, S., Rau-Chaplin, A., Shibaharay, T. "DAD: A Real-Time System for Monitoring of Data Packet Networks". IEEE Network, (Sept. 1988).

[RABI88b] Rabie, S., "Introduction of Advanced Software Technologies into Network Operations". Proceeding of IEEE Globecom Workshop on the Applications of Emerging Technologies in Network Operations and Management, (Dic. 1988).

[RIND76] Rinde, J., "TYMNET: An Anternative to Packet Technology" Proceedings of the 3rd International Conference on Computer Communications, Toront, (Agosto 1976).

[ROSE90] M.T.Rose, McCloghrie, K., "Structure and Identification of Management Information for TCP/IP-based Internets". RFC 1155, (1990).

[RABI88] Rabie, S., Rau-Chaplin, A., Shibaharay, T., "DAD: A Real-Time System for Monitoring of Data Packet Networks". IEEE Network, (Sept. 1988).

[SARI88] Sarikaya, B , "Protocol test generation. trece anaCAysis and verification techniques". Proceedings of the Second Workshop on Software Verification and AnaCAysis, IEEE Computer Society Press, (Julio 1988).

[SARC87] Sarch, R., "Integrating Voice and Data" McGraw-Hill Data Communications, (1987)

[SCHW87] Schwartz, M , "Telecommunications Networks: Protocols, Modeling and AnaCAysis". Addison-Wesley. Reading Mass, (1987)

[SHIR82] Shirey, "Security in Local Area Networks". Proceeding of the Computer Security and Integrity Symposium, (December 1982)

[SOWA89] Sowa, J.F., "Conceptual Structures: Information Preocessing in Mind and Machine". Third Ed. Addison-Wesley, Reading, (1989)

[STAL88] Stallings W., "Data and Computer Communications". Second Edition Macmillan Publishing Company, New York, (1988).

[STAL92] Stallings W., "ISDN: An Introduction". Second Ed. Macmillan Publishing Company, New York, (1992).

[STAL94] Stallings W., "The OSI Reference Model; The OSI Infrastructure: Layers 2 through 5; OSI Network Management". Networking Standards A Guide to OSI, ISDN, LAN and MAN Standards, pp 17-98;437-498, (1994)

[STAL95] Stallings W., "SNMP, SNMPv2, and CMIP: The Practical Guide to Network-Management Standards". Addison Wesley, Reading, (1995)

[STAN93] Stankovic, J.A., Ramamritham, K., "Advances in Real-Time Systems". IEEE Press. New York. (1993).

[TANE89] Tanenbaum, A., "Computer Networks". 3rd Edition, Prentice-Hall, New Jersey, (1996).

[TATS89] Tatsuya Suda, Tracy T. Bradley, "Packetized Voice/Data Integrated Transmission on a Token Passing Ring Local Area Network", pág. 238-244, IEEE Transactions on Communications, Vol. 37, N° 3, (Marzo 1989).

[TOW88] Tow, D. M., "Network management - Recent advances and future trends", pág. 732-741, IEEE Transactions on Communications, Vol. 6, (Mayo 1988).

[TRUL91] Trulove, J.E., "A guide to Fractional T1". Artech House, Norwood, Ma, (1991).

[TYME71] Tymes, L., "Tymnet - A Terminal Oriented Communications Network". Proceeding of the AFIPS Spring Joint Computer Conference, 38, (1971).

[VORU94] Voruganti, R. R., "A Global Network Management Framework for the 90's", pág. 74-83, IEEE Communications Magazine, (Agosto 1994).

[WALL90] Wallenstein, G. W., "Setting Global Telecommunications Standards: The Stakers, The Players, and The Process". Artech House, Norwood, MA, (1990).

[WENP89] Wen-Pai, Lu., Malur K. Sundaresman, "Secure Communication in Internet Environments: A Hierarchical Key Management Scheme for End-To-End Encryption", IEEE Transactions on Communications, Vol. 37, N° 10, (Octubre 1989).

[WIGG88] Wiggert, D., "Codes for Error Control and Synchronization". Artech House, MA., (1988).

[WOO77] Wood, P. H., "The Use of Passwords for Controlled Access to Computer Resources". NBS Special Publication, n° 500, (Mayo 1977).

[WOOD85] Wood, P. H., Kochan, S. G., "UNIX System Security". Hayden Books, (1985).

[YOUN91] Young, W.D., Boebert, W.E., Kain, R.Y., "Proving a computer System Secure". Scientific Honeyweller, pp 18-27, (1991).

Apéndices

Datos relativos al tráfico VOZ + DATOS de una Organización, tomados en diferentes franjas horarias.

Horario Recogida	9:00	10:00	12:00	13:00	17:00
Port 1 Station 1 BYPASS					
Characters IN	17270543	17757210	17977077	18472438	18660465
Characters OUT	5996866	6192872	6294490	6493756	6576944
Frames IN	110568	114320	116265	120012	121506
Frame OUT	114608	118444	120416	124253	125802
Port 1 Station 2 VOICE RELAY					
Characters IN	526426	526426	592149	749619	749619
Characters OUT	538141	538141	696403	839027	839027
Packets IN	25375	25375	28564	36184	36184
Packets OUT	26114	26114	33689	40631	40631
Port 1 station 4 X.25					
Frame SUMMARY					
Info IN	1095	2843	3063	3372	3748
Info OUT	1114	2881	3104	3418	3814
RNR IN	0	0	0	0	0
RNR OUT	0	0	0	0	0
SABM IN	6	6	6	6	6
SABM OUT	136	136	136	136	136
DM IN	0	0	0	0	0
DM OUT	0	0	0	0	0
RR IN	285814	287756	288526	289835	292961
RR OUT	286102	288291	289094	290448	293619
UA IN	3	3	3	3	3
UA OUT	6	6	6	6	6
Pack SUMMARY					
Data IN	244	556	590	642	706
Data OUT	854	2303	2490	2750	3081
RNR IN	0	0	0	0	0
RNR OUT	0	0	0	0	0
Call Request IN	4	7	8	9	10
Call Request OUT	0	0	0	0	0

Clear Request IN	3	6	7	8	9
Clear Request OUT	0	0	0	0	0
Restart Request IN	9	9	9	9	9
Retart Request OUT	9	9	9	9	9
RR IN	835	2265	2449	2704	3014
RR OUT	244	556	590	642	705
Call Accept IN	0	0	0	0	0
Call Accept OUT	4	4	8	9	10
Clear Confirmation IN	0	0	0	0	0
Clear Confirmation OUT	3	3	7	8	9

SNMP Agent					
snmpInPkts	261	261	261	261	267
snmpOUTPkts	261	261	261	261	267
snmpInGetRequests	29	29	29	29	29
snmpInGetNexts	232	232	232	232	238
snmpInTraps	0	0	0	0	0
snmpOutGetResponses	261	261	261	261	267
snmpOutTraps	27	27	27	27	27

Detailed Port					
PORT 1					
Characters IN	22743274	23302825	23627956	24334497	24582274
Characters OUT	11012080	11424433	.11791912	12200159	12379108
Frames IN	832761	843095	851740	866696	876369
Frames OUT	837914	848619	861764	876175	885992
PORT 2					
Characters IN	6956046	7164380	7275798	7473700	7567484
Characters OUT	18736799	19254206	19494655	19991830	20196671
Frames IN	194923	199403	201804	205915	208347
Frames OUT	190885	195279	197653	201674	204048
PORT 13					
TxPackets	23772	23772	26961	26961	26961
RxPackets	23542	23542	31118	31118	31118
PORT 14					
TxPackets	1603	1603	1603	9223	9223
RxPackets	2572	2572	2572	9515	9515