Instituto Tecnológico de Costa Rica

Escuela de Ingeniería en Electrónica

Cisco Systems Inc.

"Análisis para el desarrollo y uso de plataforma de supervisión y administración de redes LAN y WAN"

Informe Final del Proyecto de Graduación para optar por el Grado de Bachiller en Ingeniería Electrónica.

José Heriberto Peña Hernández

Cartago, Junio 2001

DEDICATORIA

A la presencia todopoderosa que llamamos Dios...
Y por supuesto a mi querida madre...

AGRADECIMIENTO

Deseo agradecer a mi familia y amigos por el soporte que me han dado para terminar mi carrera.

De igual manera, al profesor Eduardo Interiano, por toda su ayuda y guía.

Al Ing. Paulo González por haberme brindado ésta gran oportunidad y por haberme brindado su confianza para realizar este proyecto. También deseo agradecer a Tonny, Franz, Adrian, Orlando, Marco, Luis Diego, Jorge Z., Jorge B., Harry, Virgilio, Federico, Hugo, Javier, don Róger y don Mauricio por todo la colaboración que me brindaron para que éste proyecto llegara a su término.

Además, quiero agradecer de manera muy especial a Roxana, Alicia, Susan, Angie y doña Paz por su amabilidad y ayuda.

Por último, pero no menos importante, quiero agradecer al “comité”; Mario y Felipe su colaboración y compañerismo.

En fin, agradecer a todo el equipo de Cisco Systems Centroamérica por que me han hecho sentir parte del mismo.

RESUMEN

A medida que las redes de una empresa crecen en tamaño, alcance e importancia estratégica, los administradores de redes deben enfrentarse a numerosos retos de mantenimiento, rendimiento y disponibilidad de su redes. Además, a medida que los clientes implementan aplicaciones y servicios de red nuevos, como voz a través de IP (VoIP) y vídeo en tiempo real, las medidas de rendimiento de la red deben reconocer distintos niveles de servicio basados en múltiples tipos de tráfico de red.

Para mantener el rendimiento de la red, los administradores suelen emplear demasiado tiempo intentando identificar las fuentes de los problemas de rendimiento y demasiado poco en resolverlos. Este método reactivo en la administración del rendimiento de la red es cada vez más difícil de llevar a cabo.

El administrador de redes necesita herramientas de resolución de problemas que puedan identificar los problemas potenciales de rendimiento antes de que afecten seriamente a los usuarios (*mantenimiento proactivo*), o encontrar rápidamente los dispositivos de red que ocasionan los problemas de rendimiento cuando éstos hayan ocurrido. La capacidad para medir los tiempos de respuesta de la red, determinar la disponibilidad de los dispositivos, analizar los patrones del tiempo de respuesta y generar informes de rendimiento (tanto en tiempo real como históricos) es un requisito esencial en las redes empresariales actuales.

El presente documento pretende ser una guía para la consecución de todas las metas administrativas que llevan los encargados de redes que utilizan productos Cisco; y de igual manera una muestra acerca de la estrategia que la empresa Cisco Systems ha desarrollado para dar soporte y mantenimiento de manera proactiva a sus equipos.

Palabras clave: *SwitchProbe, WANProbe*, NAM, Administración, Modelo ISO de administración de redes, RMON, SNMP, CMIP, CiscoWorks2000.

Abstract

As enterprise networks continue to grow in size, scope, and strategic importance, network managers face numerous challenges in maintaining the performance and availability of their network. Furthermore, as customers deploy new network applications and services, such as Voice over IP (VoIP) and streaming video, measurements of network performance must recognize different levels of service based on different types of network traffic.

To maintain network performance, network managers often spend too much time trying to identify the source of performance problems, and too little time solving them. This reactive approach to network performance management has become increasingly unwieldy.

The network manager needs performance troubleshooting tools that can either identify potential performance problems before they seriously impact users, or quickly identify the network devices that caused the performance problems once they have occurred. The ability to measure network response time, determine device availability, analyze response time patterns, and provide performance reports—both real-time and historical—are high priority requirements in today's enterprise networks.

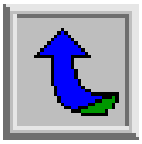
This document pretends to be a guide for the achievement of all administrative goals for network administrators in a Cisco products environment; besides, a example of Cisco's strategy for the support and proactive maintenance for all of their devices

keywords: SwitchProbe, WANProbe, NAM, Network Managment, ISO Network Management Model, RMON, SNMP, CMIP, CiscoWorks2000

INDICE GENERAL

INDICE DE FIGURAS

INDICE DE TABLAS



CAPITULO 1.
INTRODUCCIÓN.

1.1 Descripción de la empresa.

Cisco Systems S. A. Forma parte de la gigantesca red de oficinas de soporte y ventas de Cisco Systems, Inc. Ubicada en el parque empresarial FORUM en Santa Ana, se constituye en una subsidiaria directa, que como parte de la corporación, recibe soporte técnico, administrativo y económico.

La finalidad de la oficina de Cisco Systems en Costa Rica es cumplir con un propósito técnico y social en toda Centroamérica: dar el mejor respaldo posible al creciente mercado tecnológico, brindando apoyo a todos sus canales de distribución en todos los países del Istmo y Panamá. Los profesionales se ubican básicamente en tres grupos: ventas, mercadeo y soporte técnico (formado por cinco Ingenieros en Electrónica, dos Ingenieros Eléctricos y un Ingeniero en Sistemas).

Cisco Systems S.A. cuenta con todos los recursos necesarios para llevar a cabo su propósito y que provienen de su estrecha relación con Cisco Systems Inc. El personal cuenta con amplias oficinas totalmente acondicionadas para el desarrollo de ventas y asesorías, un sofisticado equipo de cómputo, un laboratorio para realizar pruebas y montajes, salas de conferencias, toda la instrumentación y los componentes requeridos para dar soporte a los clientes.

El proyecto de graduación se realiza en el departamento de Ingeniería, específicamente en el centro de soluciones tecnológicas. El departamento de Ingeniería de la empresa Cisco Systems S.A. consta de aproximadamente 8 ingenieros especializados en el área de la Electrónica y un especialista en Computación; éste departamento se encuentra a cargo del señor Paulo González Monge, Gerente de Ingeniería. El departamento de Ingeniería cuenta con cubículos para sus ingenieros y cada uno de ellos un computador personal.

El centro de soluciones tecnológicas de Cisco Systems S.A. es el área encargada de brindar soporte a los clientes, socios comerciales y revendedores de productos Cisco, para el tratamiento de consultas solución de problemas referentes a los productos Cisco.

Para este propósito, el centro de soluciones tecnológicas y todos los ingenieros de la empresa, disponen del Laboratorio Regional de Costa Rica; donde se cuenta con el equipo necesario para realizar pruebas, demostraciones, y entrenamiento de los ingenieros en cuanto a las nuevas tecnologías desarrolladas por Cisco

1.2 Definición del problema y su importancia.

Básicamente, el problema que se pretende resolver, consiste en la falta de experiencia práctica para los ingenieros de la empresa Cisco Systems S.A. y el mercado latinoamericano, que incluya estrategias, y recomendaciones acerca del desarrollo de plataformas de supervisión y administración de *redes de área local* (LAN) y de *área ancha* (WAN). Estas plataformas de administración hacen uso del protocolo de Administración de Redes SNMP y del estándar RMON, para el tratamiento de la información y su adecuada utilización para la supervisión de las redes; ya sea en los mismos dispositivos de *internetworking* o bien en productos especializados para éstas tareas.

Desde la explosión de las telecomunicaciones y la Internet en los últimos 15 años, ha sido evidente la necesidad de un planeamiento en cuanto a la manera en que se debe administrar las operaciones de una red y su crecimiento vertiginoso. Precisamente, éste crecimiento de las redes a nivel privado y público; las nuevas tecnologías y la falta de expertos dedicados al manejo y administración de las mismas, fueron los factores que permitieron el advenimiento de los protocolos de manejo y administración de redes; para realizar éstas tareas de manera sencilla y centralizada

.

Es por esto, que el área corporativa de Cisco Systems S.A. respondiendo a la necesidad en el mercado de soluciones que contemplen la administración y manejo de redes, ha planteado al área de ingeniería la inclusión de éstos conceptos en las soluciones que se comercializan por parte de la empresa; ya que ésta es un área de muy alta rentabilidad; y permitiría a la empresa mantener su liderazgo en latinoamérica por la calidad de los servicios que brinda.

1.3 Objetivos.

1.3.1 Objetivo General.

Elaborar una manual práctico acerca de estrategias y recomendaciones para el desarrollo y uso de plataformas de supervisión y administración basadas en el protocolo de administración de redes SNMP y los estándares RMON, tanto en Redes de Área Local (LAN), como de Redes de Área Ancha (WAN).

1.3.2 Objetivos Específicos.

1- Describir los diferentes modelos y arquitecturas de administración de redes existentes.
2- Establecer las características más importantes que presentan el protocolo de administración de redes SNMP y los estándares RMON.
3- Determinar las características funcionales de los dispositivos de supervisión externo por hardware.
4- Determinar las principales características del software de administración de redes *CiscoWorks 2000*.
5- Plantear las pruebas necesarias para los equipos; con sus respectivos diagramas de conexiones a utilizar.
6- Configuración de software y programación de los dispositivos de red que se utilizarán para realizar las pruebas.
7- Montar y configurar la consola de administración

CAPITULO 2
ANTECEDENTES.

2.1 Estudio del problema a resolver.

El protocolo más utilizado e implementado comúnmente en los productos de Cisco Systems es el Protocolo Simple de Administración de Redes (SNMP *Simple Network Management Protocol*) y el estándar de Monitoreo Remoto (RMON *Remote Monitoring*). Ambos, cuentan con características que los hacen una gran herramienta para mantener una red en óptimas condiciones de funcionamiento. Desde que éstos aparecieron y fueron estandarizados, muchas mejoras y nuevas operaciones han aparecido; de ésta manera, el protocolo SNMP va por su tercera versión y el estándar RMON por su segunda.

El Protocolo SNMP es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red; lo cual permite a los administradores de red, supervisar el desempeño de la red, encontrar y resolver problemas en la misma y planear su crecimiento.

Mientras que, el estándar RMON es una especificación concerniente a las tablas MIB que utiliza el protocolo SNMP para la supervisión estandarizada; lo cual permite, el intercambio de datos entre varios sistemas de supervisión externos; y de manera adicional, provee a los administradores de red con más libertad para la escogencia de analizadores y consolas con características que satisfagan las necesidades de la red.

Este estándar es de especial importancia; pues como se mencionó anteriormente las especificaciones RMON definen un conjunto de estadísticas y funciones que pueden ser intercambiadas entre consolas y analizadores externos, proveyendo a los administradores de red con información acerca del diagnóstico de fallas, planeamiento y mejoramiento del desempeño de la red; sin tener que pagar por esto un aumento en el tráfico de red, pues el uso de éstos dispositivos de administración externo, libera del procesamiento de los datos de administración a los dispositivos de trabajo en red y disminuye el tráfico en la misma.

Los productos de Cisco Systems son totalmente compatibles con las especificaciones antes mencionadas; y aunque éstos ya tienen tiempo de haber aparecido; en el área de Latinoamérica es hasta éste momento en que se le ésta dando más importancia a los conceptos de la administración de redes.

Técnicamente, el problema radica en que pese a la existencia de dispositivos especializados para la recolección, manejo y procesamiento de datos referentes al desempeño de una red de computadoras, éstos no son ampliamente utilizados. En algunos casos, se utilizan las características de administración disponibles dentro de los dispositivos de *internetworking* que conforman la red; pero en una gran parte de las redes, ni siquiera éstas son aprovechadas.

Ésta situación repercute en un pobre desempeño de las redes (colisiones, tráfico de red desmedido, bajo aprovechamiento del ancho de banda disponible, etc.); lo cual representa un inconveniente para su uso, limita el crecimiento de la misma, y en casos extremos, implicaría una gran inversión en la red, cuando lo que se necesita es una mejora en la organización, planeamiento y uso de los recursos disponibles.

Además, los productos Cisco para la administración de redes no se limitan a hardware de supervisión; sino que también incluye soluciones de software para ambientes de redes LAN y WAN. Este software es una herramienta adicional que se complementa con los dispositivos *internetworking* de Cisco y sus productos especializados para la supervisión.

2.2 Requerimientos de la empresa.

Los requerimientos planteados por la empresa se remiten a la necesidad de información práctica acerca de la forma en que se deben desarrollar los dispositivos especializados para la administración de redes. De acuerdo a ésta necesidad; se hizo latente la necesidad de un manual; donde se encontrara ésta información e incluso teoría de administración, características de los dispositivos, características del software y recomendaciones sobre la correcta manera de implementarlos para administrar una red.

2.3 Solución propuesta.

Debido a las múltiples ventajas que presenta la utilización de los conceptos de administración de redes, y a la demanda de soluciones que contemplen los mismos, era imperativo para la empresa contar con un manual práctico, sobre la implementación de plataformas de supervisión y administración de redes; que permita a los ingenieros de una manera rápida adquirir conocimiento extra y explotar las características implementadas en los productos Cisco para este propósito.

El manual consiste de una introducción teórica acerca de las arquitecturas y modelos de administración de redes; del protocolo SNMP y los estándares RMON, sus ventajas y desventajas, diferentes versiones y mejoras. Además, de presentar estrategias para su uso, y recomendaciones que permitan su implementación en *redes de área local* (LAN) *y de área ancha* (WAN). Así mismo, se incluirán recomendaciones para el uso de sistemas externos de supervisión como lo es el *SwitchProbe* de Cisco y el paquete de software de administración *CiscoWorks 2000*.

Ésta solución fue planteada por la empresa; y consistió de una etapa de investigación de protocolos y arquitecturas de administración; otra de planeamiento para la implementación de varios escenarios de administración, incluyendo tanto equipos de comunicaciones como software y hardware de administración. Finalmente, una etapa de pruebas específicamente, seguida de una etapa de análisis de resultados donde se plantearán las recomendaciones y estrategias de administración de red necesarias.

CAPITULO 3.
PROCEDIMIENTO METODOLÓGICO.

3.1 Metodología.

1- Basado en la bibliografía sobre sistemas de redes y documentos en Internet, se recopilará la información referente a los modelos y arquitectura de administración de redes y las características fundamentales del protocolo SNMP y los estándares RMON.

2- Mediante el uso de manuales de usuario, manuales técnicos e Internet se investigará el modo de funcionamiento de los dispositivos de supervisión externo por hardware, y sus características principales

3- De la misma manera, haciendo uso de los manuales de usuario, se investigará las principales características del software de administración de redes *Cisco Works 2000*,

4- De acuerdo a la información recopilada se elaborará un resumen acerca de los principales modelos y arquitecturas de administración de redes, las características que posee el protocolo SNMP y los estándares RMON; principales características de los dispositivos de supervisión externo y el software de administración de redes.

5- Haciendo uso de los conocimientos adquiridos en cuanto a los dispositivos de supervisión externo por hardware, del software de administración de redes, y con la ayuda del ingeniero asesor se planearán los escenarios de administración; para las pruebas a realizar con los dispositivos antes mencionados.

6- Ya planteadas las pruebas a realizar, se procederá a elaborar el reporte de los escenarios que se utilizaran para la etapa de pruebas.
7- Montaje de estación de administración en una máquina Sun Ultra Sparc 10.
8- Disponiendo del planteamiento de las pruebas se iniciará con la etapa de búsqueda de configuración óptima para el software y de la programación necesaria para los dispositivos que se utilizarán en la etapa de pruebas
9- Realización de las pruebas planeadas, en el Laboratorio Regional de Costa Rica, utilizando lo recursos de administración que provee el software *Cisco Works 2000.*
10- Con los resultados obtenidos en la etapa de pruebas se procederá a generar un reporte, para su posterior análisis.
11- De acuerdo a los reportes anteriores y los resultados obtenidos se procederá a realizar el análisis de los mismos; para plantear conclusiones, recomendaciones, estrategias concretas del uso de las herramientas, para la administración de redes y la elaboración de un reporte.

CAPITULO 4
DESCRIPCIÓN DEL HARDWARE UTILIZADO.

4.1 SwitchProbe

4.1.1 Características principales

Este dispositivo provee visibilidad total de las siete capas de red dentro de los paquetes que atraviesan el segmento que es supervisado por el dispositivo. Ésta sonda puede decodificar los encabezados de los paquetes y determinar como son éstos enrutados, dónde fueron originados, hacia a dónde son dirigidos, que protocolos son utilizados y que aplicación originó el paquete.

El SwitchProbe es llamado también "*roving probe"* y puede ser conectado para diagnosticar el puerto SPAN (*Switch Port Analizer*) de un Conmutador para análisis exhaustivos.

Existen 3 maneras de comunicarse con el SwitchProbe, ya sea para configurar o para extraer estadísticas guardadas en el mismo; estas son:

- *In Band Access (acceso en banda):* Ésta ocurre en un ambiente de LAN compartida (*Shared LAN*), las estadísticas son reportadas a través de la misma interfaz que está supervisando el enlace de red. Este método es factible cuando no importa que el tráfico SNMP atraviese el mismo segmento de red que se está supervisando. Sin embargo, cuando el *SwitchProbe* se conecta al puerto SPAN de un conmutador, ésta interfaz no puede transmitir tráfico, por lo que la interfaz de monitoreo no puede utilizarse para administración.
- *Side band Access (acceso de banda lateral):* Este método de acceso se utiliza para FDDI, *FastEthernet*, y *Gigabit Ethernet SwitchProbes*. Este equipo consta de un puerto ethernet adicional el cual es proveído como una interfaz separada, para reportar las estadísticas de vuelta a la plataforma de administración de red.
- *Out of Band Access (acceso fuera de banda):* Una interfaz serial tipo SLIP en el *probe* provee acceso a las estadísticas recolectadas. Este método de acceso permite no incrementar el tráfico de la red, pero está limitado por la velocidad del enlace serie.

Figura 4.1 Bastidor del Switchprobe

Los *SwitchProbes* de Cisco, proveen características para la supervisión de las siete capas de red; además, de una poderosa arquitectura de administración distribuida para el análisis del tráfico de red, *troubleshooting (búsqueda de averías)*, reporte de tendencias, y administración proactiva (*proactive network management*).

Las características de análisis en tiempo real del tráfico de red, y el reporte de tendencias, proveen visibilidad del comportamiento de la red para el planeamiento a largo plazo de la misma. Además, provee información de diagnóstico necesaria para solucionar problemas de las capas de enlace de datos, red y de aplicación, antes de que éstos puedan afectar el desempeño de la red

En resumen; las características mas importante de notar son:

- Soporte para los estándares de IETF (Internet Engineering Task Force) *RMON*, *RMON II* además de estándares emergentes como el *High Capacity RMON, ATM RMON* y *SMON (Switch Monitoring)*.
- Compatibilidad con sistemas de Administración de redes basados en el protocolo SNMP.
- Soporte para configuración remota vía BOOTP y TFTP.
- Captura selectiva de paquetes y funcionalidad de decodificación de protocolo para siete capas con filtros de pre y post. captura.
- Fácilmente actualizable en memoria Flash.

4.1.2 Opciones de software del *SwitchProbe*

Cisco Systems ofrece varias opciones de software, que pueden adquirirse por separado, para la familia independiente de dispositivos *SwitchProbe*.

Cada una de ellas proporciona una funcionalidad añadida al *SwitchProbe* y puede activarse fácilmente a través de unas pocas órdenes principales. Para activar la opción correctamente, debe de tener en el *SwitchProbe*, la versión 4.7 (o superior) del software en el dispositivo.

Tabla 4.1 Opciones de software del *SwitchProbe*

Opciones de software	Disponible en
ART Monitor	Todos los dispositivos SwitchProbe
FEC Monitor-TX	Solamente para los dispositivos SwitchProbe Fast Ethernet TX de cuatro puertos (incluye el kit 1 WS-PB-FEFDTAP-TX)
FEC Monitor-FX	Solamente para los dispositivos SwitchProbe Fast Ethernet FX de cuatro puertos (incluye el kit 1 WS-PB-OPTI-SPLT1)
NetFlow Monitor	Sólo para dispositivos SwitchProbe Ethernet y Fast Ethernet
Resource Monitoring	Todos los dispositivos SwitchProbe, excepto FDDI, HSSI (Interfaz Serie de Alta Velocidad), WAN de un puerto y todos las sondas fraccionales WAN
VLAN Monitor	Sólo para dispositivos SwitchProbe Fast Ethernet y Gigabit Ethernet
Descompresión de WAN	Sólo sondas WAN T1/E1 multipuerto

Los dispositivos *SwitchProbe* son componentes de la completa solución de Cisco para la administración de redes, que también incluye el NAM, los agentes de administración remota mini-RMON incorporados de los dispositivos Cisco (enrutadors y conmutadores), y *TrafficDirector*, la aplicación de supervisión de tráfico de la familia CiscoWorks2000. Estas herramientas ofrecen información de extremo a extremo y de varias capas acerca del tráfico de red y se pueden utilizar para el aislamiento y la solución de problemas, para la planificación de la capacidad de la red y para la administración del rendimiento de las aplicaciones.

4.1.2.1 Opción para supervisión de tiempos de respuesta para aplicaciones (ART Monitor)

El ART MIB (*Application Response Time Management Information Base*) amplía los estándares de RMON2 para medir las demoras entre las secuencias solicitud/respuesta en los flujos de las aplicaciones mas utilizadas en la red, como HTTP y FTP. El ART MIB también puede personalizarse para que admita cualquier aplicación que utilice puertos TCP conocidos. Las aplicaciones de supervisión, como *TrafficDirector*, pueden extraer los datos del ART MIB para la supervisión general, el análisis de tendencias y la generación de informes del tiempo de respuesta global de las aplicaciones. Esto, puede medirse a través de las sondas *SwitchProbe/WanProbe*, tanto desde el servidor de aplicaciones, como del cliente que lo accesa, con la opción de software *ART Monitor*.

4.1.2.2 Opción de Fast EtherChannel

Fast EtherChannel es una tecnología líder de Cisco Systems que combina entre dos y cuatro enlaces Fast Ethernet a *full duplex* en una solo enlace para proporcionar un mayor ancho de banda y un óptimo equilibrio de cargas entre los conmutadores. Ésta conexión entre los conmutadores Catalyst permite llevar grandes volúmenes de tráfico; es por esto, que la supervisión continua de éstos enlaces resulta esencial para maximizar la disponibilidad, el rendimiento de la red y de las aplicaciones. Es posible utilizar un dispositivo *SwitchProbe* Fast Ethernet para sondear un Fast EtherChannel de 400 MB entre dos conmutadores Cisco Catalyst.
Para que una sonda Fast Ethernet de cuatro puertos funcione como si fuese una sonda Fast EtherChannel, el usuario debe adquirir e instalar la opción de software de Fast EtherChannel (FEC-TX o FEC-FX) y configurar la sonda en modo *full duplex* (dos segmentos a *full duplex*). A partir de ese momento, la sonda puede agregar datos de los dos enlaces Fast Ethernet a *full duplex* en una visión consolidada, que abarca todo el tráfico que pasa entre los conmutadores Catalyst.

4.1.2.3 Opción de supervisión para módulos NetFlow (NetFlow Monitor)

Ésta opción proporciona estadísticas detalladas del tráfico en los enrutadores con NetFlow activo y en los conmutadores Catalyst con una tarjeta de función NetFlow (*NFFC NetFlow Feature Card*). Es posible utilizar NetFlow en sus versiones V.1.0, 5.0 y 7.0 .

Las estadísticas recogidas por la tecnología de conmutación NetFlow en los enrutadores o el NFFC en los conmutadores pueden exportarse a través de la función de exportación de datos de NetFlow (*NFDE NetFlow Data Export*) al dispositivo *SwitchProbe*, donde se asignan a los estándares RMON y RMON2 para un análisis del tráfico más a fondo, ofreciendo por tanto funcionalidad RMON y RMON2 en el *backbone* del enrutador.

4.1.2.4 Opción para la supervisión de recursos (Resource Monitor)

Está opción ofrece supervisión remota de los recursos de los sistemas LAN y WAN a través de sondeos distribuidos y supervisión de los límites de las mismas. Además, permite al dispositivo *SwitchProbe* realizar la interrogación proxy SNMP y la comprobación del estado de los dispositivos a través de "pings", ahorrando ancho de banda en los enlaces y permitiendo realizar una administración proactiva.

Inclusive, pueden definirse *traps* para cualquier variable MIB y notificarlas a la consola de administración a través de la interfaz Ethernet o a través del puerto serie usando la comunicación fuera de banda

Los sistemas de administración de redes basados en SNMP tienen la posibilidad de obtener la información acerca del estado y las estadísticas de los dispositivos de la red utilizando la instrucción "*get*" de SNMP para consultar a las variables (objetos) de interés de MIB.

Sin embargo, este proceso debe realizarse utilizando un sondeo continuo. Teniendo en cuenta que una red puede contener un gran número de dispositivos y cada uno de ellos tener, a su vez, muchas variables de MIB, consultar al dispositivo desde la consola de administración resulta muy poco eficaz. Por consiguiente, la administración de SNMP crea problemas a causa de la cantidad de ancho de banda necesario para obtener la información de un sitio remoto. Sin embargo, la reducción al mínimo del sondeo "ping" podría dar como resultado la falta de percepción de condiciones de fallos de la red, lo que podría poner en peligro la salud de la red corporativa.

Para solucionar este problema, la administración de recursos permite supervisar eficientemente los recursos de cualquier dispositivo SNMP. Para ello, la aplicación de administración de tráfico de CiscoWorks2000 descarga las variables MIB seleccionadas de una lista, a la sonda; lo cual crea recursos proxy en la misma. A continuación, en lugar de realizar sondeos de la red de la empresa desde la consola de administración, la sonda examina todos los recursos a intervalos seleccionados y graba el resultado. El administrador de red puede definir alarmas en un valor predeterminado de cualquier variable. En ese momento, la sonda notifica a la consola de administración cuando alguna condición de alarma provoca una interrupción, con lo que se elimina el sondeo y se proporciona gestión por excepción.

Resource Monitor incluye:

- Ping multiprotocolo remoto, lo que proporciona capacidades de ping y "similares a ping" para varios protocolos; los límites de respuestas de los pings pueden basarse en el tiempo de respuesta y en el número y frecuencia de los fallos
- "Get" SNMP remoto, que permite a los usuarios obtener el estado de cualquier variable MIB, incluyendo información acerca de MIB privadas; es posible definir límites para valores predeterminados de la variable MIB supervisada

- La administración "*out of band*" que admiten las sondas puede utilizarse como enlace redundante utilizando un puerto serie para enviar archivos de configuración con acciones correctoras a dispositivos IP designados que se encuentran en el segmento de la LAN remota

4.1.2.5 Opción de supervisión de VLANs (VLAN Monitor)

Está opción admite el creciente estándar SMON (extensiones MIB RMON para redes conmutadas) para poder sondear el tráfico por redes virtuales (VLAN). Las estadísticas de VLAN de las comunicaciones de los tipos *Inter Switch Link* (ISL), Inter *Switch Token Ring Protocol* (ISTP) y 802.1Q (solamente soporte de etiquetas ETPID sin RIF) entre dos conmutadores se recopilan en los dispositivos *SwitchProbe Fast Ethernet y Gigabit Ethernet SwitchProbe*. La opción VLAN Monitor permite al usuario profundizar y obtener información sobre los equipos y las conversaciones por VLAN.

4.2 WanProbe

La red de área amplia (WAN) es un segmento oneroso y vital de la red actual de una empresa, ya que conecta las principales instalaciones empresariales de todo el mundo y proporciona el enlace a Internet. Dado que los costos de la WAN pueden llegar hasta el 95 por ciento del presupuesto de funcionamiento de la misma; para conseguir una administración rentable de la red resulta esencial una total visibilidad de la conexión WAN y del estado del rendimiento.

Al ayudar a los administradores de redes a conocer el uso diario normal de la red, las sondas WAN de Cisco les permiten exigir y verificar que los proveedores de servicios de WAN ofrecen la mayor calidad de servicio posible. Mediante la distribución de las sondas WAN de Cisco por la red, los profesionales de TI pueden constatar que ofrecen a sus usuarios los más altos niveles de servicio y la mejor respuesta posible. La incorporación de sondas a la red reduce considerablemente el tiempo de reparación y mejora las capacidades de predicción y prevención.

El resultado es una red eficaz sobre la que las aplicaciones críticas para las empresas funcionan a la perfección y de forma fiable.

Con las sondas WAN de Cisco, los profesionales de TI pueden realizar eficazmente las siguientes tareas:

- Controlar los flujos de aplicaciones y de rendimiento a través de la WAN
- Determinar una base para el uso actual y la planificación del crecimiento futuro
- Identificar y resolver problemas
- Administrar rentablemente los recursos de la red
- Desarrollar y medir los acuerdos a nivel de servicio internos y de la portadora
- Legislar y validar las normativas de la red

4.2.1 Características del producto Cisco WAN Probe

- Admite una amplia variedad de enlaces WAN: enlaces WAN T1/E1 de un solo puerto, T1/E1 multipuerto, T1/E1 canalizado, T3/E3 High-Speed Serial Interface (HSSI) y DS-3 Frame
- Ofrece control del punto de demarcación con las sondas T1/D, E1/D y DS-3
- Admite multiplexión inversa (IMUX) a través de V.35 o de la interfaz HSSI
- Descubre automáticamente identificadores de conexión de enlaces a datos (DLCI Data Link Connection Identifier) y la tasa de información comprometida (CIR Commited Information Rate) en los enlaces de Frame Relay.
- Mide los datos de uso de la WAN a efectos de planificación de la capacidad, planeamiento de normativas y validación de las mismas.
- Localiza rápidamente problemas de la WAN, lo que ayuda a restaurar los niveles de servicio
- Hace seguimiento de los tiempos de respuesta de las aplicaciones en red a través de la WAN

4.2.1.1 Recolección de datos por DTE y DCE.

Las sondas WAN de Cisco funcionan de forma independiente para el control continuo y en tiempo real de las aplicaciones, tanto del equipo del terminal de datos (DTE) como del equipo de comunicación de datos (DCE) del enlace.

Recopilan los datos vitales: estadísticas, control de eventos y descodificación de protocolos en las capas física, de red y de aplicaciones de la red.

4.2.1.2 Descubrimiento automático del DLCI y de las aplicaciones.

Las sondas WAN de Cisco descubren automáticamente todos los DLCI y sus CIR. También llevan las estadísticas de los DLCI para los enlaces Frame Relay, lo que facilita la identificación de los elementos que degradan el uso del ancho de banda. Además, descubren automáticamente las aplicaciones y los protocolos comerciales y personalizados.

4.2.1.3 Interoperatividad

TrafficDirector es una completa aplicación de control y resolución de problemas del tráfico de red que forma parte de la familia de productos CiscoWorks2000. Proporciona un conjunto de potentes aplicaciones necesarias para configurar, administrar, controlar y resolver los problemas complejos que suelen asociarse con la administración de las redes de área extensa enrutadas.

Tanto el software *TrafficDirector* como un gran número de aplicaciones de otros fabricantes pueden acceder a las sondas WAN de Cisco y actualizar las estadísticas de agregación, análisis y generación de informes. Además, las sondas WAN de Cisco pueden, a través de *TrafficDirector* o de otras plataformas de administración, avisar al personal de administración de redes de la existencia de problemas inminentes, ya que controla los límites de eventos predefinidos. De está manera ambos ofrecen una mayor visibilidad del comportamiento de la red, y ayuda a la identificación inmediata de los cuellos de botella en el rendimiento y las tendencias a largo plazo del rendimiento, y proporcionan una detección inmediata durante la optimización del ancho de banda y su utilización en enlaces caros y críticos de la red.

4.2.1.4 Distribución no intrusiva

La sonda WAN de Cisco es un dispositivo independiente con su propia fuente de alimentación, capacidad de procesamiento e interfaces de red que operan pasivamente y conecta con el enlace WAN a través de terminales externas.

Los administradores de red pueden mover las sondas sin tener que desactivar el enlace, ya que las propias terminales permanecen en su lugar. Además, dado que las sondas de Cisco no son capaces de transmitir a través de enlaces, no tienen ningún efecto sobre la red y no pueden actuar como puntos únicos de fallo.

4.2.1.5 Instalación flexible

Las sondas WAN de Cisco ofrecen una flexibilidad sin paralelo en la conexión al enlace WAN:

La conexión entre la unidad de servicio de canal/unidad de servicio de datos (CSU/DSU) y el punto de demarcación de la portadora proporciona una ventaja importante, ya que una gran cantidad de conmutadores y enrutadores contienen varias DSU/CSU integradas (interfaces WAN T1/D y E1/D RJ-48, G.703, interfaz WAN DS-3 Frame G.703 con BNC de 75 ohmios).

La conexión entre el enrutador y DSU/CSU (interfaces WAN V.35, EI530, X.21, etc.) permite la colocación en los entornos existentes en los que estén presentes DSU/CSU externas**.**

4.2.1.6 Acceso a los datos de la sonda

Las sondas WAN de Cisco pueden configurarse con un puerto de administración de banda lateral *Ethernet o Token Ring* para el acceso por medio de la consola de administración de la red. Este puerto puede conectarse a la red de producción o a una red de administración independiente, lo que permite que los administradores de redes controlen el acceso a los datos de administración de la WAN y limiten el impacto en la red de producción. También incluye un puerto de administración EIA/TIA-232 para el acceso local o para los *modems* sin conexión permanente a la administración de redes. Con el protocolo SLIP, las sondas pueden tener acceso telefónico de forma automática a través del acceso remoto del protocolo punto a punto (PPP) y notificar a la aplicación *TrafficDirector* de las alarmas, las interrupciones y las estadísticas.

4.2.1.7 Compatibilidad de los estándares con las WAN

Las sondas WAN de Cisco son totalmente compatibles con los estándares SNMP (Simple Network Management Protocol) y RMON/RMON2. Además, cumplen con el RFC 1490 y con el método de encapsulación DLSW para *Frame Relay* y el método de encapsulación RFC 1356 para circuitos X.25. Ésta compatibilidad basada en estándares permite a las aplicaciones de administración y a las plataformas de otros fabricantes hacer uso de las estadísticas y de los datos *Frame Relay* que proporcionan las sondas WAN de Cisco.

4.2.2 Modelos de sonda WAN

- *Sondas WAN T1/E1*: control a velocidad completa de enlaces T1 de 1,544 MB o E1 de 2,048 MB de un solo segmento y enlaces *IMUXed* de hasta 3 Mbps
- *Sondas WAN T1/E1 multipuerto*: control de alto rendimiento de entre uno y cuatro T1 o E1 a velocidad completa o de un solo enlace *IMUXed* de hasta 8 Mbps; admite la nueva opción de descompresión WAN de Cisco
- *Sondas WAN T1/D y E1/D multipuerto*: control de T1 o E1 de dos o cuatro puertos, completo o fraccional; diseñada para su colocación en el punto de demarcación de la WAN
- *Sondas WAN T1/E1 multipuerto canalizadas*: control canalizado de T1 o E1 de dos puertos con la posibilidad de profundizaren canales multiplexados individuales. Esta sonda es ideal para distribuciones con enlaces que compartan varias empresas
- *Sondas WAN T3/E3*: control de alta velocidad y alto rendimiento de T3/E3 (HSSI) para un máximo de 45 Mbps con soporte para enlaces IMUXed de hasta 22,5 MB
- *Sonda WAN S-3 Frame*: control de alta velocidad de un enlace basado en DS-3 Frame; diseñada para su colocación en el punto de demarcación de la WAN

4.2.3 Opción de descompresión en enlaces WAN

La más reciente opción de Cisco admite varios esquemas de compresión de WAN en todas las sondas WAN T1/E1 multipuerto. Proporciona al administrador de red una visión mejor del tráfico de las aplicaciones en los enlaces WAN.

Aunque la implementación de la compresión ayuda a controlar los costos de WAN, tiene un precio (la compresión de datos en los enlaces de WAN limita la capacidad del administrador de la red para sondear correctamente éstos enlaces). Con la introducción de la opción de descompresión de WAN, Cisco ofrece a los administradores de redes la necesaria visibilidad de los flujos de aplicaciones de toda la empresa.

La opción de descompresión WAN (que puede administrar una agregación de hasta dos enlaces T1/E1de datos comprimidos completos), admite varios tipos de compresión y permite que las sondas WAN T1/E1 multipuerto de Cisco supervisen todos los enlaces WAN que porten datos comprimidos. Con la opción de descompresión activa, la sonda WAN detecta automáticamente el tipo de compresión y aplica el algoritmo apropiado, para que no sea necesaria ninguna configuración especial. La sonda WAN activará la supervisión de aquellos enlaces que tengan una combinación de datos comprimidos y no comprimidos, y funcionará con total normalidad si el enlace no contiene tráfico comprimido.

La siguiente tabla muestra los tipos de compresión y las encapsulaciones admitidas. Éstos tipos de compresión sólo se admiten en los enrutadores de Cisco, como los enrutadores de las series Cisco 7200 y 7500. La versión inicial de la opción es compatible con los algoritmos de compresión STAC hi/fn y Van Jacobson. Está previsto que en una próxima versión admita al algoritmo de compresión Predictor.

Tabla 4.2 Tipos de compresión y encapsulación admitidas por el *WANProbe*

Tipo de compresión	Admite encapsulación	Admite la versión de Cisco IOS
Van Jacobson Header Compression para TCP/IP (RFC 1144)	HDLC, Frame Relay, PPP, X.25	11.2, 11.3, 12.x
Compresión STAC hi/fn		
Compresión por paquetes	HDLC o Frame Relay	11.2, 11.3, 12.x
Compresión por circuito virtual	Frame Relay	11.2, 11.3, 12.x
Compresión por enlace	Frame Relay o PPP	11.2, 11.3, 12.x

Terminología

- TCP/IP *Van Jacobson Header Compresion*: este algoritmo se basa en RFC 1144. Comprime las cabeceras TCP/IP dentro de un paquete. Este algoritmo es apropiado para el tráfico TCP/IP que conste de pequeños paquetes que tengan pocos bytes de datos (p.ej., telnet).
- Compresión por paquetes: este algoritmo comprime todos los paquetes. Se utiliza principalmente en los enlaces de "escasa integridad". El algoritmo que se suele utilizar es STAC o Predictor.
- Compresión por interfaz/Compresión de enlaces: para gestionar paquetes más grandes, utilizar mayores velocidades de datos y mejorar el rendimiento en varios protocolos en una LAN, la compresión se puede aplicar a todo el flujo de datos que se va a transportar a través de la WAN. Este tipo de compresión, llamada compresión por interfaz, comprime todo el enlace de la WAN como si fuera una aplicación. A diferencia de la compresión de cabeceras, la compresión por interfaz es independiente del protocolo. Utiliza STAC o *Predictor* para comparar el tráfico y, seguidamente, encapsula el tráfico comprimido en otra capa de enlaces, como PPP, para garantizar la corrección de errores y la secuencia de paquetes. Las compresiones STAC y *Predictor* a través de PPP las definen RFC 1974 y RFC 1978, respectivamente.
- Compresión por circuito virtual: este algoritmo está diseñado para redes *Frame Relay* y se basa en el estándar FRF.9. Dicho estándar admite STAC y *Predictor.*

4.3 Módulo de Análisis de Red (Network Analisis Module NAM).

4.3.1 Características

El NAM es una solución para la supervisión del tráfico que provee capacidad RMON, RMONII, NetFlow y VLAN total; además de capacidades de *troubleshooting* relacionados con protocolos y análisis de tendencias. La NAM es una tarjeta que ocupa un *slot* de los Conmutadores Cisco Catalyst 5000 y 6000; y soporta tecnologías Ethernet y Fast Ethernet.

Las funciones del *SwitchProbe* y el NAM son muy similares, pero varían en cuanto a las extensiones opcionales RMON y el tipo la fuente de los datos a analizar.

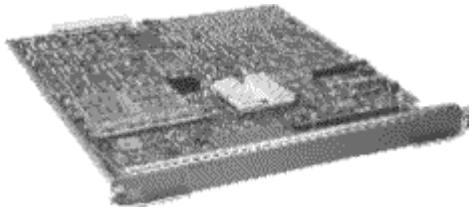


Figura 4.1 Network Analysis Module NAM

El NAM posee los mismos algoritmos que tiene el *SwitchProbe* y opera como una *roving probe* en el Catalyst 5000 y 6000. Sin embargo, la fuente de los datos es muy diferente de la que utiliza el *SwitchProbe*; ya que este toma los datos del tráfico de una conexión con la interfaz física del hub, conmutador o enrutador. Mientras que el NAM obtiene sus datos desde el *Backplane* (conexión física entre la tarjeta, los buses y líneas de poder dentro de un bastidor) del Catalyst usando el mecanismo de SPAN para tomar las estadísticas almacenadas en el MIB RMON por el módulo supervisor.

Una característica clave del NAM es que puede supervisar simultáneamente múltiples puertos de un conmutador o VLANs; y proveer estadísticas RMON/ RMONII para cada uno de éstos; pues mantiene un conjunto dedicado de tablas MIB RMON y RMONII para cada puerto de conmutador o VLAN. Sin embargo, el Módulo de análisis de red admite las siguientes fuentes de datos:

- Uno o varios puertos Ethernet
- Un puerto Fast Ethernet (puede ser un enlace troncal VLAN)
- Una VLAN Cisco ISL o VLAN IEEE 802.1Q

- Exportación de datos *NetFlow* desde un NFFC (*NetFlow Feature Card*) en el mismo bastidor

4.3.1.1 Supervisión de aplicaciones

La supervisión de las aplicaciones de la red en la familia Catalyst 5000 es posible instalando un módulo de análisis de red NAM. La supervisión de aplicaciones se consigue a través de las tablas de distribución de protocolos, *host* y *matrix* de aplicación en el estándar RMON2 que es parte esencial del NAM.

Éstos grupos de MIB ofrecen la información detallada necesaria para determinar las aplicaciones que se están utilizando en la red, los *hosts* a los que están accediendo y las parejas cliente-servidor que están generando más tráfico.

4.3.1.2 Planificación de capacidad y análisis de tendencias

Con la posibilidad que brinda el módulo de análisis de red de hacer seguimiento de tendencias en la red, los administradores pueden preveer el comportamiento de la misma y planificar a largo plazo su crecimiento. Si esto se combina con la aplicación de generación de informes acerca de las aplicaciones que posee *TrafficDirector*, es posible determinar las tendencias de uso del ancho de banda por puerto, enlace troncal, sistema anfitrión, protocolo de red y aplicación. A medida que se introducen usuarios, servidores y aplicaciones en la red, estas herramientas ofrecen datos valiosos para planificar el futuro diseño de la red y la optimización de su topología.

4.3.1.3 Aislamiento de fallos y resolución de problemas

Los grupos *Filter* y *Capture* del estándar RMON del NAM posibilitan la captura remota de paquetes y un análisis detallado de los protocolos que se están utilizando. Los filtros pueden configurarse en el NAM a fin de que capture exclusivamente determinados paquetes del puerto del conmutador o de la VLAN que se supervisarán. Por ejemplo, se puede definir que un filtro capture solamente aquellos paquetes que provengan o vayan a un dispositivo determinado o sólo aquellos paquetes que tengan un protocolo específico, como IPX. Los paquetes que concuerden con el filtro preestablecido se almacenan en *buffers* del módulo de análisis de red. A continuación, estos paquetes capturados se cargan bajo demanda en la aplicación de consola RMON para decodificar el protocolo y realizar un mayor análisis.

4.3.1.4 Análisis del patrón del tráfico

Los grupos *Network Layer Host y Network Layer Matrix* de RMON2 del módulo de análisis de red pueden determinar qué dispositivos están generando más tráfico en un protocolo determinado y ayudar a identificar aquellas conversaciones entre parejas de direcciones del nivel de la red que originan ese gran uso. Esta información es muy útil para ayudar a conocer los patrones de uso actuales de la red y para optimizar los esfuerzos en el diseño de la red y en la evolución de la topología.

4.3.2 Opciones de Software

4.3.2.1 Supervisión de VLANs

El NAM proporciona estadísticas RMON/RMON2 individuales de todos las VLANs de un enlace troncal *Inter-Switch Link* (ISL) o IEEE 802.1Q. Éste, dispone de dos potentes modos de supervisión para analizar el tráfico de VLAN.

El primero, el modo VLAN, ofrece una descripción general del tráfico por medio de VLAN que atraviesa un enlace troncal. Este modo muestra el número de paquetes y bytes que transporta cada VLAN en el enlace troncal.

El segundo modo, llamado VLAN *agents*, puede utilizarse para profundizar aún más permitiendo al usuario instalar cualesquiera grupos RMON/RMON2 para el tráfico de todas las VLAN de interés. Por ejemplo, es posible que las tablas *Network Layer Host y Matrix* supervisen el tráfico de VLAN 2 al mismo tiempo que lo hace con las tablas *Network Layer Host y Application Layer Host* de VLAN 3 a la vez que realiza una captura de paquetes en VLAN 15.

4.3.2.2 Supervisión con módulos NetFlow

Con *NetFlow Data Export* se han ampliado las capacidades para la administración de rendimiento de los conmutadores Catalyst. El mecanismo de *NetFlow Data Export* captura las estadísticas del tráfico de capa 3 a medida que expiran las entradas del caché de NFFC. A continuación, agrupa algunos de éstos registros de estadísticas en un datagrama *User Datagram Protoco*l (UDP) y lo envía a un recolector de datos *NetFlow* como, por ejemplo, un módulo de análisis de red. Con la función opcional de supervisión de *NetFlow* activada, el módulo de análisis de redes actúa como *proxy* o asigna las estadísticas del tráfico del capa 3 de *Netflow* a los grupos MIB RMON2 basados en estándares apropiados para que sean analizados por cualquier aplicación RMON2 que cumpla los estándares.
La siguiente tabla presenta una comparación entre el *SwitchProbe* y el NAM:

Tabla 4.3 Comparación entre *SwitchProbe* y el NAM

Características de Agente	Network Analisis Module	SwitchProbe
RMON	Si	Si
RMON2	Si	Si
FastEtherChannel	Si	Si
VLAN Monitor	Si	Si (opcional)
Netflow Monitor	Si (opcional)	Si (opcional)
Resouce Monitoring	No	Si (opcional)
Application Response Time	No	Si (opcional)
Estadísticas independientes por fuente de datos	Si	No
Características de Aplicación		
Auto-roving (supervisión automatica)	Si	Si
Adminsitracion por inteface gráfica	Si	Si

CAPITULO 5.
DESCRIPCIÓN DEL SOFTWARE UTILIZADO.

Las aplicaciones mas importantes para efectos de supervisión exhaustiva de la red son el **CiscoWorks2000 Routed WAN Management Solution,** y el **CiscoWorks2000 LAN Management Solution.**

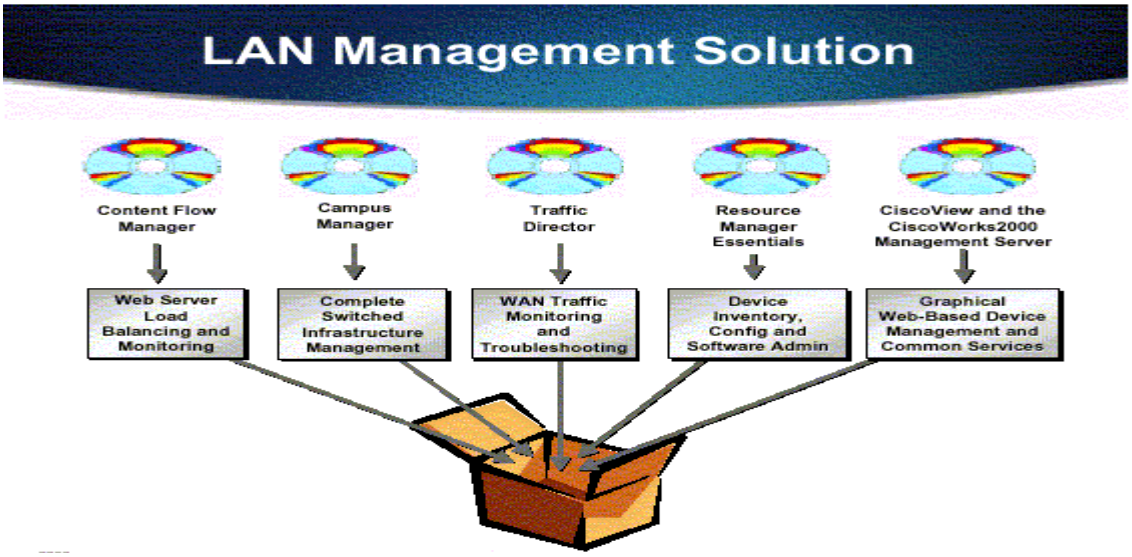


Figura 5.1 Componentes del CiscoWorks2000 LMS

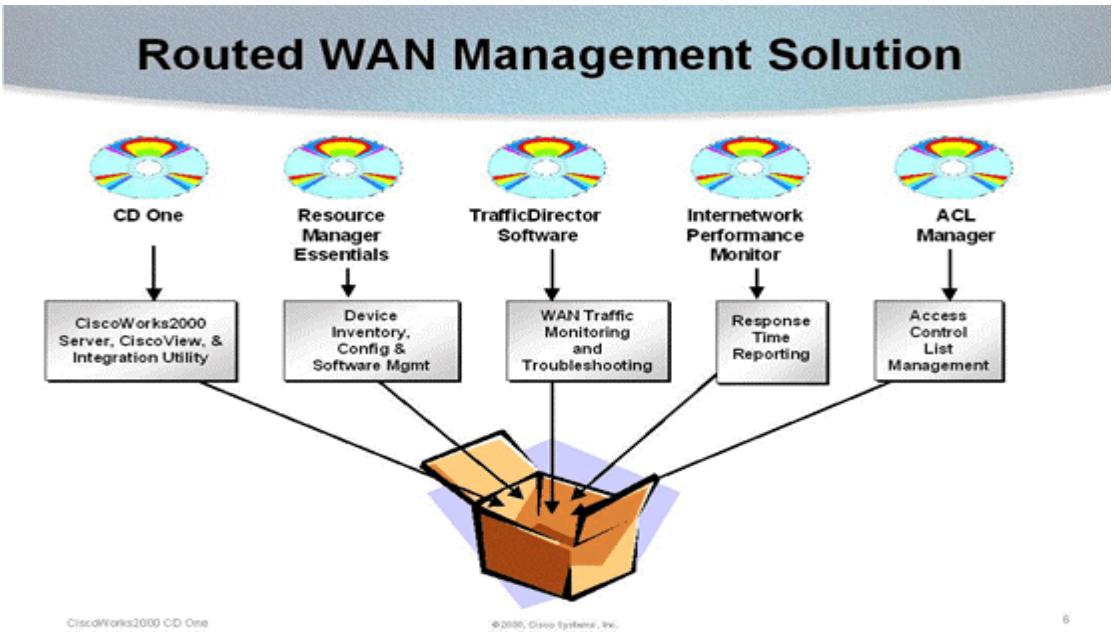


Figura 5.2 Componentes del CiscoWorks2000 Routed WAN

Éstos paquetes de software CiscoWorks, están compuestos por múltiples aplicaciones con funciones especificas; a continuación se presenta una descripción de cada una de ellas:

5.1 CiscoView.

CiscoView, es una aplicación de administración gráfica de dispositivos, la cual provee; información dinámica de estado, sondeo y configuración para el amplio rango de productos Cisco. *CiscoView* despliega una visualización física del bastidor del dispositivo, con codificación de colores de los módulos y puertos para una visualización gráfica de los equipos. Las características de supervisión despliegan estadísticas de desempeño y más; mientras que las características de configuración permiten cambios comprensivos a los dispositivos; siempre que los requisitos de seguridad se lleven a cabo.

El administrador de dispositivos *CiscoView* es la aplicación de software de administración de Cisco de mayor implementación. Al estar basado en Web, *CiscoView* permite al acceso generalizado desde cualquier cliente que disponga de un explorador estándar, acceso a la red y requisitos mínimos de hardware. *CiscoView* admite integración con los productos *CiscoWorks2000* o plataformas asociadas y proporciona administración multiusuario de dispositivos en el contexto más amplio de una solución de intranet de administración de extremo a extremo.

Las características de *CiscoView* ofrecen información dinámica del estado, sobre la configuración y control de los dispositivos de red Cisco.

5.1.1 Características

Sus características incluyen:

- Presentación basada en web de los productos Cisco desde una sola ubicación, ofreciendo a los administradores una representación visual completa de estos productos sin tener que verificar físicamente cada dispositivo.
- Representación física que se actualiza continuamente de los enrutadores, concentradores, conmutadores o servidores de acceso de la red.
- Control y seguimiento en tiempo real de la información esencial y de los datos relativos al rendimiento de los dispositivos, el tráfico y el entorno, con medidas tales como el porcentaje de utilización, las tramas transmitidas y recibidas, los errores y gran variedad de indicadores específicos de dispositivo.
- La capacidad de modificar las configuraciones de dispositivos (enrutador, conmutador o servidores de acceso) a través del web.
- Capacidad de acceder al soporte técnico de los dispositivos Cisco actuales y nuevos a través del *Package Support Updater* (PSU) basado en Web, sin necesidad de adquirir o instalar nuevas versiones de *CiscoView*.
- Acceso multiusuario a un único servidor *CiscoView* a través de un cliente basado en web.

5.2 Resource Manager Essentials (RME)

El RME es un conjunto de aplicaciones basadas en Web que ofrecen soluciones de administración de red para conmutadores, enrutadores y servidores de acceso Cisco. La interfaz *browser* del *Resource Manager Essentials* permite acceso a información critica de la red y simplifica las tareas administrativas que consumen el mayor tiempo.

5.2.1 Características

Las características de RME incluyen:

- La rápida creación de un completo inventario de la red.
- La supervisión y generación de informes sobre el hardware, la configuración y los cambios en el inventario.
- La administración y distribución de cambios en la configuración y en las actualizaciones de las imágenes del software a diferentes dispositivos.
- Simplifica el control y la resolución de problemas en recursos críticos para redes de área local (LAN) y redes de área ancha WAN.
- Una solución para la administración básica de VPN.

RME proporciona un conjunto adecuado de tareas para la administración básica de VPN. Todas las tareas se han creado a partir de un grupo predefinido de dispositivos con capacidad VPN, permitiendo así una rápida determinación de los problemas relacionados con las redes privadas virtuales. Los administradores de redes pueden realizar tareas específicas de VPN relacionadas con:

- Configuración: los usuarios pueden comparar y contrastar con rapidez las configuraciones de dispositivos VPN y hacer búsquedas de configuraciones únicamente en los dispositivos VPN de la red.

- Inventario: es posible interrogar al sistema para identificar a los dispositivos VPN que tienen módulos de cifrado por hardware. Algunos dispositivos Cisco requieren la instalación de la versión correcta de IOS para funcionar como dispositivo VPN. Los usuarios pueden ejecutar la generación de informes para determinar qué dispositivos de la base de datos *Inventory Manager* necesitan actualizarse para funcionar como dispositivo VPN de la red.

El RME está comprendido por seis aplicaciones claves que se complementan; estas son:

- Administrador de inventario *(Inventory Manager)*
- Auditor de cambios *(Change Audit)*
- Administrador de configuración para dispositivos *(Device Configuration Manager)*
- Administrador de imágenes de software *(Software Image Manager)*
- Administrador de disponibilidad *(Availability Manager)*
- Analizador de mensajes Syslog *(Syslog Analyzer)*
- *Cisco Management Connection*

5.2.2 Aplicaciones

5.2.2.1 Inventory Manager: crea y mantiene un inventario actualizado de hardware y software.

Inventory Manager proporciona una base de datos actualizada de los dispositivos Cisco, desde los enrutadores ISDN (RDSI) de la serie Cisco 700 hasta los conmutadores de alto nivel de las series IGX, BPX y MGX. La base de datos del inventario proporciona información detallada sobre los atributos de los dispositivos tales como el tipo de bastidor, las interfaces, la versión del software, la memoria, las características Flash y otros. *Inventory Manager* proporciona una amplia gama de capacidades para la generación de informes, desde informes resumidos de alto nivel hasta informes detallados de cada dispositivo.

Inventory Manager ofrece:

- Un inventario actualizado de todos los dispositivos Cisco de la red, incluyendo compatibilidad con Cisco *CallManager*, el concentrador VPN 3000 (VPN c3000) y tipos de dispositivos IGX, BPX y MGX.
- Información resumida del hardware y software, así como informes detallados por grupos de dispositivos, donde se incluye el nombre del dispositivo, el tipo de bastidor, la memoria, la versión del software, la interfaz, los módulos de apilamiento, y otras características detalladas de software y hardware.
- La importación de dispositivos se puede hacer desde *Cisco WAN Manager*, así como desde *CWSI Campus 2.x, HP OpenView, Tivoli NetView* o desde un archivo sin formato.
- Información para la planificación de la capacidad mediante la identificación del número total de ranuras libres y utilizadas en muchos dispositivos de Cisco.
- Informes de puerto multiservicio sobre el número y lugar de los conmutadores Catalyst que tienen activado el puerto multiservicio.

- Credenciales de los dispositivos (información de contraseñas) que pueden intercambiarse con otras aplicaciones de administración mediante *Extended Markup Language* (XML).
- Capacidad para seleccionar la VPN como un agrupamiento de dispositivos para la generación de informes.

5.2.2.2 Administrador de configuraciones de dispositivos (Device Configuration Manager): mantiene un archivo activo y simplifica la implementación de los cambios en la configuración de varios dispositivos.

Ésta aplicación mantiene un archivo activo y proporciona una forma sencilla de actualizar los cambios en la configuración de varios conmutadores y enrutadores Cisco. Además, controla la red para detectar los cambios de configuración, actualiza el archivo cuando se detecta un cambio y registra la información del cambio en su base de datos. Una potente interfaz de usuario basada en web permite buscar en el archivo los atributos específicos de configuración y comparar el contenido de dos archivos de configuración para identificar fácilmente las diferencias.

RME incluye una aplicación para la edición de configuraciones (*Config Editor*), el cual es un editor basado en web que permite comprobar varios archivos de configuración del archivo de configuraciones, actualizarlos, cambiarlos y posteriormente guardarlos de forma local o descargarlos al dispositivo. El editor proporciona capacidades de edición muy potentes, incluyendo las de buscar, reemplazar, copiar, cortar y pegar, comparar y cambiar información detallada.

Características:

- Mantiene un archivo actualizado identificando y almacenando automáticamente los cambios en los archivos de configuración.
- Proporciona un editor basado en web, para la modificación y descarga de los cambios en la configuración.
- Permite hacer cambios en la configuración de varios conmutadores o enrutadores en la red; los cambios se pueden descargar de forma inmediata o ejecutarse después en una operación programada.

- Proporciona un método basado en asistentes para simplificar y reducir las complejidades y el tiempo asociados con la tarea de implementar cambios globales en toda la red.
- Las plantillas que proporciona Cisco, simplifican el proceso de cambio de configuración para la comunidad SNMP, TACACS (*Terminal Access Controller Access Control System*), los servicios de *syslog*, los destinatarios de *traps* SNMP, *Cisco Discovery Protocol* (CDP), el sistema de nombres de dominio (DNS) y muchos otros.
- Ofrece flexibilidad a la hora de informar de cualquier cambio en la interfaz de línea de ordenes (CLI) a la red a través de plantillas definidas que se publican para un usuario o un grupo de usuarios autorizados para su ejecución.
- Admite la búsqueda en los archivos de configuración para simplificar la localización de determinadas configuraciones de dispositivos y de atributos en las configuraciones.
- Identifica las diferencias entre las configuraciones de inicio y de ejecución.
- Proporciona una interfaz de órdenes simplificada basada en web, que permite mostrar las órdenes que se van a ejecutar contra diferentes conmutadores o enrutadores para mejorar y simplificar la resolución de problemas relacionados con la red.
- Interfaz gráfica para las órdenes de presentación (show), permitiendo así que puedan ejecutarse varias ordenes de presentación contra un grupo de dispositivos como una operación programada.
- Capacidad para aislar y ver los estados de las configuraciones de *firewall* PIX y de dispositivo VPN.

5.2.2.3 Administrador de imágenes de software (Software Image Manager): simplifica y acelera el análisis y la instalación de imágenes de software.

Es un aplicación que simplifica enormemente la administración de las versiones y la instalación rutinaria de actualizaciones de software en enrutadores y conmutadores Cisco. Éstas tareas son realizadas a través de actividades guiadas de planificación, programación, descarga y control de las actualizaciones.

Inclusive, automatiza los laboriosos pasos necesarios para actualizar las imágenes de software, a la vez que reduce las complejidades del proceso de actualización que favorecen la aparición de errores. Los enlaces integrados con CCO relacionan la información en línea de Cisco acerca de los parches de software con el software Cisco IOS y Catalyst instalado en la red, resaltando las notas técnicas relacionadas. Las nuevas herramientas de planificación, también vinculadas con CCO, buscan los requisitos del sistema y envían notificaciones cuando hay que actualizar el hardware (*Boot ROM, Flash RAM*) para admitir las actualizaciones propuestas en las imágenes del software.

Antes de iniciar cualquier actualización, los requisitos previos de las imágenes nuevas se validan frente al conmutador de destino o los datos de inventario del enrutador para asegurar que la actualización se lleve a cabo correctamente. Cuando se actualizan varios dispositivos, este administrador sincroniza las tareas de descarga y permite que el usuario controle su progreso. Las tareas programadas se controlan a través de un proceso de desconexión, que permite a los administradores autorizar las actividades de un técnico antes de iniciar las tareas de actualización. RME 3.3 incluye la capacidad de analizar las actualizaciones de software para las plataformas IGX, BPX y MGX, simplificando y reduciendo notablemente el tiempo necesario para determinar el impacto de una actualización de software.

Características:

- Ofrece informes de los análisis de las actualizaciones del software que muestran los requisitos previos y el impacto de las actualizaciones propuestas.
- Reduce de horas a minutos el plazo medio de la instalación de las imágenes de software en enrutadores o conmutadores.
- Refuerza la autorización de tareas de nivel dos que permite actualizar las tareas que van a aprobarse antes de la ejecución.
- Distribuye una o varias imágenes a los dispositivos en una sola operación de instalación.
- Realiza auditorías de software de las imágenes de la red y una sincronización de la biblioteca del software.

- Utiliza CCO para generar informes sobre los defectos del software y los parches disponibles que afectan a los dispositivos y a las imágenes de la red.
- Ofrece compatibilidad perfeccionada con proxy Web para una mejor conexión con CCO.
- Proporciona un eficaz análisis de actualización de software para las plataformas IGX, BPX y MGX.

5.2.2.4 Auditor de cambios (Change Audit Service): presenta informes completos del hardware, software y los cambios de configuración.

El auditor de cambios, es un punto central en el que los usuarios pueden ver los cambios que se han producido en la red; la información resumida de los cambios se muestra de forma sencilla, ya que muestra que tipos de cambio fueron realizados, así como la persona, el momento en que llevaron a cabo y si se hicieron desde una sesión Telnet o de consola, o desde una aplicación *CiscoWorks2000*. Además, la naturaleza de los cambios se identifica rápidamente a través de informes detallados (tarjetas añadidas o extraídas, cambios en la memoria o en la configuración, etc.). En aquellas organizaciones cuyas políticas definen el momento en el que hay que realizar cambios en la red, *Change Audit* proporciona un resumen de excepciones que resalta los cambios realizados fuera del periodo aprobado.

Características:

- Ofrece una exhaustiva auditoría de los cambios de red mediante informes cronológicos.
- Registra quién ha cambiado qué, cuándo y cómo.
- Ofrece un filtrado de los informes de cambios utilizando criterios de clasificación sencillos o complejos.
- Identifica los cambios que se han realizado en la red en periodos críticos de las operaciones de red.

5.2.2.5 Administrador de Disponibilidad (Availability Manager): resalta los dispositivos críticos y su capacidad de respuesta.

El "tablero dinámico de disponibilidad" del administrador de disponibilidad, determina con rapidez el estado operativo de los enrutadores y conmutadores críticos para la organización. Desde el supervisor de disponibilidad se puede profundizar en un dispositivo en concreto para ver información histórica detallada sobre su tiempo de respuesta, disponibilidad, recargas, protocolos y estado de las interfaces.

Características:

- Proporciona informes que resumen en qué momento los dispositivos más importantes se recargaron o se quedaron fuera de línea.
- Muestra visualizaciones en profundidad sobre el historial de capacidad de acceso y disponibilidad de los dispositivos individuales.
- Ofrece informes gráficos de las tendencias del tiempo de respuesta de los dispositivos.
- Incluye informes de estado accesibles por explorador web para ver la disponibilidad de los conmutadores y enrutadores.
- Proporciona conexión con el *Stack Decoder* de los CCO para simplificar la resolución de problemas en las recargas.
- Muestra resúmenes de los protocolos a los que puede responder un dispositivo (UDP, TCP, HTTP, TFTP, TELNET, SNMP) a través de la herramienta de conexión.

5.2.2.6 Analizador de Mensajes Syslog (Syslog Analyzer): aísla las condiciones de error y sugiere las causas probables.

El analizador de mensajes *syslog* filtra los mensajes que registran los conmutadores, enrutadores, servidores de acceso y *firewalls* Cisco IOS mostrando explicaciones de las causas probables y las acciones recomendadas para solucionar problemas lógicos y de configuración.

Sus informes se basan en filtros definidos por el usuario que destacan los errores específicos o condiciones graves, e identifican cuándo se han producido eventos concretos (como, por ejemplo, la caída de un enlace o el reinicio de un servidor). *Syslog Analyzer* permite enlazar los mensajes syslog con información personalizada, como las medidas administrativas basadas en web o la ejecución de *scripts CGI (Common Gateway Interface*) para realizar acciones correctivas.

Características:

- Acelera la resolución de problemas al mostrar los patrones de error principales a lo largo del tiempo.
- Resume eventos *syslog* basándose en su gravedad o en criterios de usuarios para los conmutadores, enrutadores y *firewalls* PIX y Cisco IOS.
- Admite el filtrado selectivo de recolectores remotos *syslog* y permite que se envíen al servidor RME solamente los mensajes deseados.
- Separa los mensajes no deseados utilizando para ello filtros o *scripts* definidos por el usuario a través del filtrado local y remoto.
- Abre *scripts* o enlaces definidos por el usuario a una página web con información relativa basada en mensajes *syslog* específicos.

5.2.2.7 Cisco Management Connection: crea las conexiones de administración Cisco a sus aplicaciones preferidas de administración

Cisco Management Connection incluye un conjunto de herramientas para integrar aplicaciones utilizando estándares y tecnologías basadas en Internet. Estas herramientas permiten que el usuario pueda vincular aplicaciones de administración basadas en Web a CiscoWorks2000 a través de un mecanismo certificado de registro. Cisco Management Connection es una herramienta utilizada por Cisco y por más de 45 fabricantes de administración de redes (incluyendo Aprisma, Computer Associates, Evidian, Fujitsu, Hewlett-Packard y Tivoli Systems) para crear conexiones de administración Cisco certificadas para sus aplicaciones. Esta rápida adopción ha generado un entorno en el que los usuarios pueden crear fácilmente intranets de administración que interconectan sus aplicaciones de administración preferidas basadas en web.

Características:

- Vincula a *CiscoWorks2000* con sus aplicaciones favoritas a través de conexiones de administración Cisco certificadas.
- Vincula a *CiscoWorks2000* con otras aplicaciones de Cisco basadas en web.
- Mejora la integración con aplicaciones de administración de redes de otros fabricantes.

5.3 TrafficDirector

TrafficDirector, es otro componente de la familia de productos de CiscoWorks2000, es una aplicación de fácil manejo para el control y la resolución de problemas del tráfico de la red, y que proporciona a los administradores WAN y LAN una visibilidad rápida de las cuestiones y problemas de la red antes de que se conviertan en asuntos cruciales. Si se usa en combinación con las sondas WAN de Cisco, los dispositivos LAN *SwitchProbe* y los módulos de análisis de la red (NAM), el software *TrafficDirector* ofrece más de 30 aplicaciones integradas necesarias para controlar el rendimiento y la utilización de los enlaces, resolver y aislar problemas en la red y proporcionar estadísticas, gráficos e informes históricos en tiempo real para llevar a cabo la planificación de la capacidad de la red.

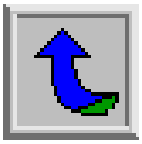
TrafficDirector ayuda a identificar los cuellos de botella en el rendimiento y las tendencias del rendimiento a largo plazo, y proporciona una rápida detección al optimizar el ancho de banda y la utilización en enlaces caros, críticos para los negocios.

TrafficDirector abarca cinco elementos esenciales de la administración de la red: supervisión basada en estándares, sondeo de la red de extremo a extremo, análisis del tráfico de las capas de las aplicaciones, capacidad máxima de ampliación y una perfecta integración con otros dispositivos y herramientas de la red.

5.3.1 Funciones principales y herramientas para la solución de problemas:

5.3.1.1 Aislamiento de errores

- Alarmas incorporadas para adelantarse a la degradación del rendimiento.



- Profundización mediante el uso de *TopNTalkers* para encontrar los orígenes de los errores.
- Decodificación de 11 protocolos a través de las siete capas.
- Interrogaciones para variables MIB SNMP a través del *Resource Monitor* y de las sondas WAN y LAN de Cisco, que correlacionan los datos con las estadísticas de la red.

5.3.1.2 Puesta a punto del rendimiento y planificación de las capacidades

- Cuantificar y poner a punto el rendimiento de los enlaces.
- Optimizar los recursos de las aplicaciones y de la red, los gastos actuales en documentos, así como administrar y justificar los costos del crecimiento.
- Planear las necesidades futuras de conexión mediante un análisis organizado de las líneas básicas y las tendencias.
- Mejorar la calidad de servicio (QoS) en toda la red, optimizando los enlaces.
- Establecer y controlar los acuerdos de servicio con las portadoras.

5.3.1.3 Control de conmutadores y Frame Relay

La aplicación *TrafficDirector* incluye una amplia lista de capacidades y funciones que simplifica las tareas asociadas con el control del tráfico de la red y con la resolución de problemas relativos a la conexión o al ancho de banda.

La siguiente sección da una idea general de las áreas funcionales clave de la aplicación *TrafficDirector*:

- Control del tráfico: visualización gráfica simultánea de las estadísticas actuales de enlaces, tráfico y errores para un máximo de 100 agentes, identificadores de conexiones de datos-enlace (DLCI) o puertos de los conmutadores.
- Control de las aplicaciones: visualización gráfica de las estadísticas actuales para un máximo de 20 aplicaciones y 100 agentes o DLCI a la vez.
- Control de los protocolos: visualización gráfica de las estadísticas actuales para un máximo de 20 protocolos y 100 agentes o DLCI a la vez.

5.3.1.4 Control de los enlaces

La aplicación *TrafficDirector* es especialmente útil y económica en sitios remotos, en los que elimina el tráfico relacionado con la administración de la red causado por la consulta a través de enlaces WAN caros. Además, simplifica los informes para que se puedan mostrar varios segmentos en un solo informe, sin importar la consola *TrafficDirector* a la que estén realmente registrados los datos.

- Ampliación de los segmentos: visualización gráfica de las estadísticas actuales e históricas de los enlaces, el tráfico y los errores.
- Detalles de los segmentos: visualización numérica de las estadísticas actuales e históricas de los enlaces, el tráfico y los errores.
- Historial a corto plazo: visualización gráfica de las estadísticas históricas de los enlaces, el tráfico y los errores de los últimos 25 minutos, con una resolución de 30 segundos.
- Historial a largo plazo: visualización gráfica de las estadísticas históricas de los enlaces, el tráfico y los errores de las últimas 25 horas, con una resolución de 30 minutos.
- Control de los anillos: visualización numérica de las estadísticas de los enlaces FDDI o Token Ring.
- Control de ruta de la fuente: visualización numérica de las estadísticas actuales de enrutamiento de las fuentes Token Ring o FDDI.
- Retraso del viaje de ida y vuelta: se utiliza cuando una sonda LAN envía una instrucción ping a un dispositivo SNMP; visualización numérica del tiempo medio del viaje de ida y vuelta entre una sonda LAN y un dispositivo SNMP.
- Proxy SNMP: se utiliza cuando una sonda está interrogando a un dispositivo SNMP; visualización numérica de los resultados de la interrogación y del valor MIB; puede utilizarse por ejemplo para controlar la utilización de los discos, la CPU o la memoria RAM de los servidores.

5.3.1.5 Supervisión de aplicaciones y protocolos

- Descubrimiento de dominios: visualización numérica de las estadísticas totales de las aplicaciones y los protocolos para todo el tráfico reconocido de la red.
- Historial de las aplicaciones: visualización gráfica de las estadísticas históricas del tráfico de las aplicaciones.
- Historial de los protocolos: visualización gráfica de las estadísticas históricas del tráfico de los protocolos.
- Aumento de los protocolos: visualización gráfica de las estadísticas del tráfico actual para cada uno de los protocolos del sistema apilado del conjunto del protocolo.

5.3.1.6 Supervisión de los *hosts* y de las conversaciones

- Personas con mayor utilización: visualización gráfica de las estadísticas actuales de tráfico y de errores para las fuentes con mayor tráfico por enlace, protocolo o aplicación; todo ello clasificado por mayor tiempo de utilización, emisor o fuente del error.
- Todos los conversadores: visualización numérica de las estadísticas del tráfico y de los errores de todas las fuentes de tráfico por enlace, protocolo o aplicación.
- Historial del *host*: visualización gráfica de las estadísticas históricas de tráfico y errores de un *host* en particular.
- Todas las conversaciones: visualización numérica de las estadísticas actuales de tráfico y errores de las fuentes y destino de tráfico principales (conversaciones) por enlace, protocolo o aplicación.
- Historial de las conversaciones: visualización gráfica de las estadísticas históricas de tráfico y errores entre dos estaciones.

5.3.1.7 Resolución de problemas

- Control de alertas: presenta la información relativa a las alarmas y a la resolución de problemas recibidas desde las sondas y los dispositivos NAM.
- Captura de datos: configura las sondas y los servicios de NAM con el fin de capturar paquetes para su análisis detallado; tamaño de los filtros, del buffer y de las partes del paquete definidos por el usuario.
- Decodificación de los protocolos: muestra los paquetes capturados en decodificación de protocolos, por códigos de color y siete capas en formato resumen, detallado o hexadecimal.

5.3.1.8 Administración del software.

- Administrador de configuración: define los conmutadores, sondas NAM, LAN, WAN y *Frame Relay* y agentes que van a controlarse; crea grupos de agentes para el control de los grupos y de la configuración por lotes.
- Editor de propiedades: establece normativas de control, incluyendo qué protocolos controlar y cuáles registrar para los informes y en qué límites establecer las alarmas; las normativas se aplican a las sondas y a los grupos de agentes.
- Configurar servidor : define los servidores remotos y las aplicaciones *TrafficDirector* para los informes agregados en cualquier sonda; define los límites de las alarmas en cualquier sonda, sea cual sea el servidor o la aplicación *TrafficDirector* en la que realmente se registran los datos.

- Configurar resumen: establece los límites de tiempo y de tráfico para administrar el tamaño de las bases de datos *Structured Query Language* (SQL).
- Editor de filtros: define qué filtros de tráfico utilizar para la captura de datos.
- Editor de dominios: define qué aplicaciones, protocolos o dispositivos personalizados controlar.
- *Conexión remota*: configura los dispositivos de las sondas remotas.

5.3.1.9 Confección de informes

El Informador de tendencias (Trend Reporter): genera informes exhaustivos utilizando datos LAN, WAN, *Frame Relay*, conmutador, LAN virtual (VLAN) y *NetFlow* para la aplicación de normativas de resolución de problemas y planificación de la capacidad.

Informes de aplicaciones y protocolos

- Utilización de protocolos: informe gráfico del tráfico histórico de las aplicaciones y los protocolos.
- Distribución de los protocolos: informe numérico del tráfico total de las aplicaciones y los protocolos para todos los protocolos de un sistema apilado específico.

Informes de *hosts*, conversaciones y departamentos

- Resumen de las conversaciones: informe gráfico de las estadísticas totales entre las fuentes de tráfico (conversaciones).
- Resumen de los *hosts*: informe gráfico de las estadísticas del tráfico total de las fuentes o los departamentos con mayor tráfico.
- Historial de los *hosts*: informe gráfico de las estadísticas históricas del tráfico de las fuentes o departamentos con mayor tráfico.
- Salida de los *hosts*: informe numérico de las estadísticas totales de tráfico, enlaces y errores por fuentes o departamentos de tráfico.
- *Host verbose*: informe numérico de las estadísticas totales de tráfico, enlaces y errores por fuentes de tráfico o departamentos.

Otros informes

- Tiempo de respuesta de la red: informe gráfico de las estadísticas del tiempo de respuesta histórico entre los dispositivos de las sondas y los dispositivos interrogados.
- Utilización de la *backbone* de los enrutadores: informe gráfico de las estadísticas totales de tráfico, enlaces y errores para cada una de las interfaces de un enrutador con *NetFlow*.
- Facturación: informe numérico de la salida total de bytes y de la cantidad a facturar por fuente de tráfico o departamento.

5.4 Campus Manager

Los entornos campus actuales son el corazón de las empresas y de los sistemas de tareas críticas. *Campus Manager* se diseñó para satisfacer las demandas de estas necesidades operativas. La necesidad de entender, controlar y reaccionar a condiciones cambiantes de la red hace imprescindible el uso de herramientas de administración sofisticadas, aunque no por eso difíciles de utilizar. *Campus Manager* forma parte de *LAN Management Solution* y *Campus Bundle* para HP-UX/AIX, una de las muchas soluciones orientadas a productos de la familia CiscoWorks2000, dirigidas al entorno de red de campus.

5.4.1 Características

Las características de *Campus Manager* incluyen:

- Descubrimiento y presentación inteligente de grandes redes de Capa 2 en mapas topológicos accesibles a través de navegador.
- Configuración de LAN virtual (VLAN), emulación LAN (LANE) y servicios de modo de transferencia asíncrona (ATM) y asignación de los puertos del conmutador a éstos servicios.
- Pantallas de enlace y estado del dispositivo basadas en consultas SNMP.
- Identificación de discrepancias de configuración de Capa 2.
- Herramientas de diagnóstico para problemas relacionados con la conexión entre estaciones terminales y dispositivos de Capa 2 y 3.

- Localización automática y correlación de la información de los usuarios por control de acceso a medios (MAC), dirección IP, NT o acceso *NetWare Directory Services* (NDS) o nombre del servidor UNIX, con sus conexiones físicas a la red conmutada.
- Visibilidad y punto de inicio de Cisco *CallManager* desde los servicios topológicos, así como seguimiento del auricular telefónico a IP, dirección Mac y puerto del conmutador.
- Traza de las rutas de Capa 2 y Capa 3 entre los auriculares de origen y de destino.
- Exportación de los mapas topológicos a Visio.
- Complementos Java para mejorar el rendimiento de la interfaz gráfica de usuario (GUI).

Campus Manager permite a los administradores cambiar, administrar y controlar relaciones de red más fácilmente, mejorando su eficacia a la hora de proporcionar servicios avanzados de red y otros servicios críticos en la empresa a los usuarios y clientes.

5.4.2 Aplicaciones

Campus Manager es un conjunto de aplicaciones ejecutado desde el "escritorio de administración" común, usado por todas la aplicaciones basadas en web de CiscoWorks2000. *Campus Manager* contiene tres aplicaciones que pueden ejecutarse desde el navegador del cliente:

5.4.2.1 Servicios de topología: es la interfaz principal de una variedad de mapas de topología de gran escala, resúmenes tabulados, informes y configuración de servicios en la capa 2 de la red. Una interfaz de tipo árbol de directorios crea un listado de la capa 2 física y lógica, *Virtual Trunking Protocol (VTP)* y vistas de dominios ATM con tablas resumen de los dispositivos e interfaces asociados con esas vistas.

Ésta estructura en árbol actúa como el punto de inicio para los mapas topológicos, las funciones de informes de discrepancia y los servicios de configuración. En los menúes del servicio de topología se pueden encontrar capacidades de configuración de VLAN y LANE, software ATM de herramientas de diagnóstico y configuración para circuitos virtuales permanentes (PVC), además de informes de comprobación de discrepancias físicas y lógicas en la configuración y herramientas de resaltado. También admite el descubrimiento y la presentación de las aplicaciones de respuesta a los clientes de Cisco e informes sobre los servicios de éstos dispositivos.

5.4.2.2 ***User Tracking***: diseñada para ayudar a localizar conexiones de estaciones finales basándose en el conmutador de acceso, ésta aplicación es una herramienta útil en el análisis de conectividad y resolución de problemas. A través de adquisición automática, se genera una tabla con la información de las estaciones de usuarios finales y las conexiones de Capa 2. Ésta tabla se puede ordenar y consultar y, por tanto, los administradores pueden encontrar a los usuarios con facilidad. Los usuarios pueden identificarse por nombre, auricular IP, dirección MAC e IP, así como por el puerto del conmutador y el conmutador al que están conectados, junto con la asignación VLAN y VTP del puerto. Informes predefinidos, como duplicados MAC por puerto de conmutador o direcciones IP duplicadas, permiten a los administradores localizar usuarios móviles o infracciones en las normativas de puerto.

5.4.2.3 ***Path Analysis***: es una aplicación para administración de redes conmutadas, una herramienta extremadamente eficaz en la resolución de problemas de conexión. *Path Analysis* utiliza *User Tracking*, servicios topológicos y el árbol de conmutación en tiempo real para determinar la conexión de Capa 2 y Capa 3 entre dos extremos de la red o auriculares IP. La traza resultante se presenta en vista gráficas de topología que muestran los dispositivos de Capa 2 y Capa 3, las direcciones de rutas y los tipos de enlaces. También pueden presentarse en formato de tabla, ofreciendo información sobre interfaces específicas, direcciones IP, VLAN y tipos de enlace

5.4.2.4 Configuración y asignación de puerto VLAN/LANE

Campus Manager proporciona medios sencillos y gráficos para crear, modificar o eliminar VLAN, elementos LANE o asignar puertos de conmutador a VLAN. Cuando las VLAN se crean o modifican, los cambios de puertos o usuarios se actualizan instantáneamente y se transmiten a los conmutadores, lo que elimina la necesidad de actualizar y configurar individualmente a todos los conmutadores implicados. Cuando se seleccionan VLAN, la vista de tabla muestra los puertos participantes, el estado de los puertos y la información del, y el mapa de topología puede ejecutarse para resaltar de forma gráfica los dispositivos participantes y los enlaces de las conexiones VLAN. Herramientas adicionales de asignación permite a los administradores mostrar el estado de los árboles de conmutación, los enlaces troncales VTP, enlaces de los puertos del conmutador y los elementos de servicio LANE existentes.

5.5 Content Flow Monitor

Content Flow Monitor es una aplicación basada en web para el control del rendimiento y el equilibrado de carga en tiempo real de servidores y ha sido diseñada para satisfacer las necesidades actuales de hospedaje web empresarial. El control y la administración de los dispositivos servidores de contenido como, por ejemplo, *Cisco LocalDirector* o Catalyst 4840G, pues ambos son esenciales en la distribución de aplicaciones y servicios críticos. *Content Flow Monitor* ofrece a los administradores de redes una visualización inmediata del rendimiento de los elementos de equilibrado de carga de los servidores de Cisco. Esto proporciona estadísticas en tiempo real del equilibrado de cargas, de forma que las decisiones que afectan a la configuración del equilibrado de cargas de los servidores puedan tomarse más rápidamente y con mayor precisión para satisfacer los cambiantes modelos de utilización y flujo. *Content Flow Monitor* forma parte del *suite LAN Management Solution* de la familia de productos de administración de redes CiscoWorks2000.

5.5.1 Características de *Content Flow Monitor*

Content Flow Monitor utiliza la arquitectura Cisco *ContentFlow* para controlar de forma dinámica la red de entrega de contenidos. Éste administrador, presenta el estado de salud actualizado de los dispositivos *content*, así como la disponibilidad de servicios, la configuración y estadísticas detalladas de los mismos en tiempo real. *Content Flow Monitor* se ejecuta desde un navegador y es accesible desde cualquier lugar de la red, de forma que la información crítica está siempre disponible.

A medida que crece la necesidad de información de Internet y de las intranets, también se incrementa el número de dispositivos de red desplegados para satisfacer las necesidades de una infraestructura de distribución de contenidos de gran tamaño y en expansión. *Content Flow Monitor* reduce notablemente la complejidad de la administración del equilibrado de carga, ya que ofrece una plataforma unificada para el control de todos los dispositivos Cisco para el equilibrado de carga de servidor en la red. *Content Flow Monitor* es una herramienta esencial de visualización para comprender, navegar y resolver problemas en el flujo de contenidos.

Content Flow Monitor es una auténtica aplicación cliente/servidor basada en web, se ha creado sobre los protocolos abiertos estándar de la industria y se integra plenamente con el servidor de administración CiscoWorks2000. *Content Flow Monitor* tiene dos componentes integrales:

- Servidor *Content Flow Monitor*.
- Cliente *Content Flow Monitor*.

El servidor *Content Flow Monitor*, instalado en un servidor CiscoWorks2000, utiliza el protocolo SNMP para descubrir de forma inteligente los componentes de la arquitectura *ContentFlow* y sus relaciones, como son los FMA (*Flux Manager Administrator*), los FDA (*Flux Distribution Agent*), los servidores reales y los virtuales. Recoge las características de la configuración de los dispositivos de distribución de contenidos y las estadísticas en tiempo real, como el número total de entradas de flujo y caché por agente de envío por FDA, el número total de conexiones y paquetes por servidor virtual, y el tipo y estado de la unidad de recuperación de fallos por *LocalDirector*.

El servidor *Content Flow Monitor* ofrece una interfaz gráfica de usuario (GUI) de administración basada en web a la que se accede a través del escritorio común de CiscoWorks2000 y que proporciona interfaces de configuración para:

- Añadir/borrar/modificar dispositivos base FDA y FMA para el descubrimiento de elementos *ContentFlow*.
- Especificar intervalos de consultas para los dispositivos FDA y FMA.

El cliente *Content Flow Monitor* es un applet Java accesible desde la consola común CiscoWorks2000 a través de una interfaz de navegador. Proporciona al usuario la información y las estadísticas esenciales de los elementos *ContentFlow* como:

- Mostrar con gráficos las estadísticas en tiempo real como, por ejemplo, el número de conexiones, recuentos de paquetes por servidor virtual o servidor real.
- Control de la distribución del tráfico en tiempo real entre servidores reales para cualquier servidor virtual dado.
- Estado y disponibilidad de servicio de los dispositivos en toda la red de distribución de contenidos.
- Una intuitiva capacidad de profundización que permite la visualización de los dispositivos de distribución de contenidos.
- Características de configuración detallada de los dispositivos de distribución de contenidos y estadísticas de rendimiento.
- Actualización bajo demanda de las características de configuración y estadísticas para los dispositivos de distribución de contenidos.

Content Flow Monitor admite todas las arquitecturas y diseños de redes de distribución de contenidos de Cisco, como la implementación del equilibrado de carga de servidores (ISLB) Cisco IOS, equilibrado acelerado de carga de servidores, LocalDirector independiente y equilibrado de carga multinodo (MNLB).

El servidor *Content Flow Monitor* se instala sobre el servidor de administración CiscoWorks2000 junto con otros productos de la familia CiscoWorks2000.

Como parte de *LAN Management Solution* saca partido de la familia de productos CiscoWorks2000, ofreciendo una solución de administración integrada que simplifica el flujo de trabajo en una red de gran tamaño para la distribución de contenidos. Las interfaces basadas en web y los servicios compartidos hacen más sencilla la tarea del operador para dar respuesta a los problemas de equilibrado de carga, dirigir el análisis de la ruta de Capa 2 para resolver la conexión o evaluar rápidamente las condiciones del conmutador y cambiar las propiedades del enlace. *Content Flow Monitor* es una extensión natural de la amplia gama de herramientas que forman parte de *CiscoWorks2000 LAN Management Solution*.

5.6 *El Internetwork Performance Monitor* IPM

5.6.1 Características

Internetwork Performance Monitor (IPM) es una aplicación para la resolución de problemas de disponibilidad y de tiempo de respuesta en redes de área ancha enrutadas. Ésta herramienta permite a los ingenieros resolver de forma dinámica los problemas de rendimiento de la red utilizando informes en tiempo real e históricos..

IPM satisface éstos requisitos realizando mediciones dinámicas de la disponibilidad y los tiempos de respuesta de la red, incluyendo análisis históricos y en tiempo real.

Con IPM, los administradores de red disponen de la herramienta que necesitan para identificar problemas de rendimiento, cuellos de botella, diagnosticar latencia, fluctuaciones e identificar tendencias de rendimiento en la red WAN para la que sirven. IPM permite al administrador realizar análisis de rendimiento de rutas y saltos, simplificando así la identificación de los dispositivos de red que contribuyen a generar problemas de rendimiento. IPM puede determinar las rutas posibles de red utilizadas entre dos dispositivos de red y mostrar el tiempo de respuesta de cada uno de los saltos del enrutador en cada ruta.

Además, IPM es una herramienta esencial para facilitar la implementación de los futuros servicios de red. IPM proporciona mediciones del rendimiento de la red para una amplia gama de protocolos de red, incluyendo las que utilizan VoIP y calidad de servicio (QoS) basadas en la precedencia IP.

5.6.2 Uso de la tecnología Cisco IOS para medir el rendimiento de la red

IPM mide el rendimiento de la red basándose en la tecnología de "generación de tráfico sintético" del software Cisco IOS, conocida como el *agente Service Assurance* (agente SA). El uso del tráfico sintético por IPM ofrece al administrador de la red un alto grado de flexibilidad en la selección de los puntos de terminación en una red entre los que se va a medir el rendimiento de la misma. Ésta flexibilidad hace de IPM una herramienta muy eficaz para la resolución de problemas de rendimiento.

Además, el uso de la tecnología del agente SA en los enrutadores de Cisco permite utilizarlos como plataforma para la medición del rendimiento de la red, además de su función tradicional de enrutamiento de tráfico. Como resultado, los usuarios pueden sacar partido a la inversión financiera que hayan hecho en sus enrutadores de Cisco.

IPM hace un óptimo uso de la tecnología del agente SA de Cisco IOS mediante la configuración de los agentes de rendimiento de red en el enrutador, denominados recolectores. Éstos recolectores, como parte de su configuración, incluyen un enrutador fuente, un dispositivo destino y un tipo de operación.

La definición de una operación IPM incluye el tipo de protocolo, el intervalo de medición, el tamaño de paquete y el valor de precedencia IP. IPM 2.2 puede medir el rendimiento basándose en una variedad de protocolos de red, incluyendo:

- Eco ICMP (Internet Control Message Protocol).
- Eco de ruta IP.
- Ping 3270.
- Systems Network Architecture (SNA).
- Eco UDP (User Datagram Protocol).
- Fluctuación UDP.

- Conexión TCP (Transmission Control Protocol).
- Sistema de nombres de dominio (DNS).
- Dynamic Host Configuration Protocol (DHCP).
- HTTP (para direcciones URL estáticas).
- DLSw.

Además, para las redes que hayan sido implementadas con calidad de servicio basada en valores de precedencia IP, IPM puede medir el rendimiento de cualquiera de éstos protocolos a través de cualquiera de los seis valores de precedencia IP. Como resultado, IPM ofrece una representación precisa del rendimiento de la red, mediante mediciones del rendimiento del tráfico sintético que es notablemente similar al del tráfico en tiempo real. Asimismo, IPM permite la medición del rendimiento de servicios diferenciados (por ejemplo, voz, vídeo y datos) en una red empresarial.

Una vez que el recolector IPM se ha configurado e instalado en el enrutador fuente, IPM recolectará de forma constante información sobre el rendimiento, basándose en los parámetros del recolector que hayan sido definidos para las siguientes medidas:

- Latencia.
- Fluctuación (sólo para tipos de operación de fluctuación UDP).
- Disponibilidad.
- Errores.
- Pérdida de paquetes.

5.6.3 Funciones principales:

5.6.3.1. Resolver problemas de disponibilidad y de tiempo de respuesta de la red

IPM permite administrar de forma dinámica los problemas de tiempo de respuesta de la red. IPM facilita la notificación al administrador en caso de cualquier degradación en los tiempos de respuesta o cuando no se encuentre disponible un enlace controlado. Inclusive, contribuye a localizar el dispositivo o el enlace que ocasiona del problema.

IPM permite que las medidas de rendimiento se tomen automáticamente para una ruta entera o para cada uno de los saltos (esto es, un enlace o un dispositivo) dentro de una ruta. Los administradores de la red pueden reducir fácil y rápidamente la fuente del problema de rendimiento a un único salto. Como resultado, las capacidades de diagnóstico rápido de problemas consiguen una mayor disponibilidad permitiendo a los administradores encontrar rápidamente los cuellos de botella en el rendimiento.

IPM ofrece las siguientes funciones para la resolución de problemas:

- Identificación y análisis del rendimiento de todas las rutas entre dos dispositivos de una red.
- Análisis del rendimiento de cada salto en la ruta entre dos dispositivos conectados.
- Informes gráficos históricos y en tiempo real de los tiempos de respuesta entre dos dispositivos conectados.
- Notificación dinámica con interrupciones SNMP cuando el tiempo de respuesta excede los límites predefinidos.
- Notificación dinámica con una interrupción SNMP cuando algún enlace no se encuentre disponible.

5.6.3.2 Solucionar violaciones del límite de tiempo de respuesta de la red

IPM permite el control continuo del tiempo de respuesta entre parejas de dispositivos de red utilizando la tecnología del agente SA de Cisco IOS; para esto, se debe configurar el agente SA en el enrutador para que envíe una notificación usando un *trap* SNMP, siempre que se excedan los límites de tiempo de respuesta o se haya perdido la disponibilidad de la red entre el enrutador y cualquier otro dispositivo de red. Los límites que configura IPM en el enrutador pueden ajustarse al nivel adecuado de sensibilidad basándose en los siguientes parámetros de configuración:

- Límites en aumento: se produce la notificación cuando el valor en el tiempo de respuesta sobrepasa un nivel específico.
- Límites en descenso: se produce la notificación cuando el valor en el tiempo de respuesta desciende por debajo de un nivel específico.

- Límites inmediatos: se produce la notificación cuando un ejemplo viola el límite.
- Límites intermitentes: se produce la notificación basándose en la satisfacción del límite en un porcentaje específico de tiempo.
- Límite medio: se produce la notificación si se excede el límite de una media. En este caso, las notificaciones no se tramitan hasta que no se haya tomado un número determinado de muestras.
- Límite consecutivo: la notificación se basa en la violación de los límites de los tiempos de respuesta de las muestras en un número consecutivo de veces.

5.6.3.3 Resolución de problemas de rendimiento de red para VoIP

Cuando se ha implementado VoIP en la red corporativa, IPM puede usarse para resolver problemas de rendimiento y para permitir una identificación y aislamiento rápidos de los problemas de rendimiento y, por tanto, garantizar un servicio de voz continuo en la red. IPM puede identificar y aislar rutas de red específicas donde las medidas de fluctuación y latencia de la red hayan superado los niveles de rendimiento necesarios para admitir servicios de telefonía de alta calidad.

IPM es capaz de proporcionar un análisis detallados de la fluctuación entre los dispositivos fuente y destino en una recolector IPM. Este análisis incluye tanto la fluctuación negativa como positiva, así como la fluctuación de envío e inversa entre la fuente y el destino.

5.6.3.4 Rendimiento de red SNA/IP

IPM también proporciona una solución para el control del rendimiento de las redes interconectadas SNA e IP; en concreto, para aquellas en las que el tráfico SNA es transportado a través de IP por medio de una red de enrutadores hasta un procesador frontal, hasta un procesador de interfaz de canal de Cisco o un adaptador de puerto de canal en un enrutador. En éstos entornos, IPM puede medir el tiempo de respuesta IP desde una estación de trabajo origen a través de la red de enrutadores sobre la que se está encaminando el SNA.

Además, IPM puede medir la ruta del tráfico SNA nativo, bien desde el último enrutador de la red directamente hasta la computadora, o bien desde el último enrutador de la red a través del FEP hasta la computadora. Utilizando todas estas funciones combinadas, los operadores de redes pueden obtener una administración del rendimiento de la ruta completa.

IPM ofrece las siguientes funciones SNA:

- Mide los tiempos de respuesta para los enlaces de red entre enrutadores de Cisco y la computadora.
- Admite múltiples tipos de sesiones.
    - Punto de control de servicios de sistema (SSCP).
    - Unidad lógica (LU) 0.
    - LU 2.
- Informa a los administradores de la red de cualquier violación del límite a través de alertas NMVT.

5.7 Cisco Access Control List (ACL)

5.7.1 Características

El Administrador de listas de control de acceso (ACL) de Cisco es una importante incorporación a la familia de productos CiscoWorks2000. Este administrador ofrece una interfaz tipo web con un conjunto de aplicaciones que gestionan las ACL de los dispositivos de Cisco en los entornos de redes empresariales. El administrador de ACL cuenta con herramientas para configurar y administrar filtros IP e IPX, para controlar el acceso a los dispositivos. Entre estas herramientas se incluyen editores de listas, administradores de plantillas de normativas, administradores de clases de redes y servicios para ampliabilidad, herramientas para el desplazamiento por las listas de acceso para resolver problemas y la distribución automatizada de las actualizaciones en las listas de acceso.

El administrador de ACL reduce drásticamente el tiempo necesario para desarrollar filtros nuevos y mantener los filtros del tráfico existente en instalaciones a gran escala de dispositivos de Cisco.

Este administrador ayuda a mejorar la fiabilidad de la red, ya que garantiza una instalación precisa y consistente de los filtros ACL en la red. Su interfaz de explorador y el uso de plantillas ofrece una importante alternativa al esfuerzo redundante propicio para cometer errores necesario para editar las listas de acceso individualmente desde una interfaz de la línea de ordenes (CLI). En redes más grandes, su característica de administrador de plantillas y de instalación automatizada permite gestionar centralmente la instalación de configuraciones de listas de acceso para grupos de usuarios, dispositivos, servidores de acceso, enrutadores de redes virtuales privadas (VPN), servidores web y servidores de correo electrónico. Además, el administrador de ACL facilita la optimización de los contenidos de las listas de accesos, incluyendo la eliminación de las entradas redundantes, la fusión y consolidación correcta de las entradas de las listas de acceso para garantizar que se reducen los ciclos de búsqueda de dispositivos del procesador y aumenta la velocidad de envío de paquetes.

El administrador de ACL ayuda a asegurar la tarea de administración de listas de acceso enlazándose con el nuevo sistema de administración de seguridad multinivel en servidores *CiscoWorks2000*. A través de este sistema, el administrador del sistema controla el acceso de los usuarios a las herramientas del administrador de ACL y a muchas de las otras que se incluyen en la solución enrutada de administración de WAN.

El administrador de ACL hace uso de las posibilidades de administración de seguridad de acceso a las aplicaciones del servidor CiscoWorks2000 y la información del inventario y la configuración de *Resource Manager Essentials*.

CAPITULO 6.
ANÁLISIS Y RESULTADOS.

6.1 Explicación del diseño.

Los profesionales en redes de hoy en día conocen de la necesidad de supervisar la red, pero no entienden completamente las capacidades de los dispositivos de recolección de datos. En muchos casos, el usuario puede entender mal las características disponibles en éstos, y como resultado no utilizarlas. Y lo peor que puede suceder es que el usuario puede desarrollar de manera incorrecta estos dispositivos y recibir poco o ningún beneficio.

La idea principal de este proyecto de graduación consiste en demostrar la necesidad de conocer las formas, en que se puede mantener una red de computadoras en perfectas condiciones; y la importancia de su mantenimiento en entornos de red donde una falla puede significar la pérdida de mucho dinero. Aquí se presentan varios escenarios para el desarrollo de dispositivos de administración de redes; los cuales pretenden ser una guía para demostrar la manera en que éstos dispositivos pueden ser utilizados y sacar provecho de las características que los hacen tan especiales.

Inicialmente, se describirán los pasos necesarios para la configuración básica de los dispositivos y el software que se utilizará en los escenarios de desarrollo. Luego, se hará un enfoque aplicado a la administración del desempeño de la red aplicado a la utilización de los dispositivos de sondeo dedicado para redes LAN y WAN; configuración y pasos para obtener los resultados a los que se llegó; e implementar de manera óptima la plataforma de supervisión con los dispositivos.

Finalmente, se ampliará el enfoque a las demás áreas definidas por el modelo ISO de administración de redes (inventario, cambios, configuración, seguridad y faltas.); que también forman parte fundamental de la administración; y son manejadas por los restantes módulos del software *CiscoWoks2000*.

6.1.1 Configuración de equipos.

Antes de iniciar con la explicación de los escenarios y las herramientas para administración de la red; es necesario cumplir con algunos requerimientos de configuración para que los equipos trabajen correctamente.

Para los conmutadores Catalyst:

- Asignar la dirección IP para la administración.

  "set interface sc0 900 172.20.18.180 255.255.255.240"
  (en la VLAN apropiada)
- Habilitar CDP/ILMI (ATM) **habilitado por defecto.**
- Configurar el dominio VTP.

  "set vtp domain [Building-1] mode [server|client|transparent]"
- Habilitar SNMP.

  "set snmp community read-only public" (habilitado por defecto)
  "set snmp community read-write private" (habilitado por defecto)
  NOTA: Cambie su read-write string!
- Habilite el Logging (para mensajes Syslog)

  "set logging server enable"
  "set logging server 172.20.18.5" (Servidor CiscoWorks 2000)
  "set logging level informational"
  (limita mensages syslog para niveles 0–5)

Para dispositivos IOS:

- Asignar la dirección IP para la administración.

  Enrutadores: asignar dirección IP a la interfaz Loopback0
  "interface Loopback0"
  "ip address 172.20.18.154 255.255.255.255"

  ATM Switches: Asignar dirección IP a un puerto interno o interfaz ethernet
  "interface ATM2/0/0" (ejemplo de configuration de LEC interno)
  "ip address 172.20.28.162 255.255.255.248"
  "lane client ethernet core-mgt"
- Habilitar CDP (Cisco Discovery Protocol) o bien ILMI en ATM(*Interim Local Management Interface*)

"atm pvc 2 0 16 ilmi"

- Habilitar SNMP

"snmp-server community public RO"
"snmp-server community private RW"
"snmp-server host 172.20.18.5 public"
"snmp-server enable traps"

- Habilitar Logging (Mensajes Syslog) **"logging on"**
"logging 172.20.18.5" (dirección del servidor CiscoWorks 2000)
"logging trap informational" (limita los mensaje a los niveles 0–5)

- Habilitar los agentes SAA
"rtr responder"

Por supuesto; además de esto, se deberá configurar también el acceso Telnet de sus equipos; y configurar apropiadamente los dispositivos de supervisión; ya sean éstos *SwitchProbe*, *WanProbe* o bien un NAM en los conmutadores Catalyst 5000 o 6000.

6.1.2 Configuración Básica *SwitchProbe/WanProbe*

La configuración de éstos dispositivos es muy sencilla; pues la interfaz para el usuario es presentada en manera de menús. En las siguientes páginas encontrará texto capturado sobre la configuración de éstos dispositivos; y en la sección de anexos; podrá encontrar la configuración completa de éstos dispositivos para su uso en los escenarios de desarrollo.

Los parámetros mas importantes que tiene que configurar son:

- Dirección IP de la sonda.
- Máscara de red
- Dirección IP del servidor de administración (NMS)
- Dirección IP del *gateway*.
- *Community Strings (read-only y read-write)*

```
***** Cisco SwitchProbe  V4.7.0 (Build 125) *****

Interface number : 1

[1]  Change IP Address                  10.1.200.200
[2]  Change Net Mask                    255.255.255.0
```

```
[3]  Change Default Gateway Address     10.1.200.1
[4]  Change Read Community              public
[5]  Change Write Community             private
[8]  Select Interface                   ETHERNET
[9]  Change Server Address              10.1.200.203
[10] Upgrade Software
[11] Enter Command-line mode
[12] Reset Agent

[31] Go to Next Page

          Enter your response or Enter "exit" to logout
```

- Modo de las interfaces (*Manage o Monitor*). El modo *manage* se utiliza para especificar que la interfaz es específicamente para tráfico administrativo; mientras que el modo *monitor* es el que especifica que la interfaz será utilizada para la supervisión.

  Por defecto, la interfaz ethernet que acompaña a las sondas debe estar en *modo manage-monitor*. Y las otras interfaces en modo *monitor*. Sin embargo, si necesita liberar la interfaz ethernet del modo *manage*; puede configurar y utilizar la interfaz serie para la administración. (Selección 8 del menú principal)

```
Selection#: 8

Select Interface :

[1]ETHERNET MODE = MANAGE + MONITOR
[2]SERIAL MODE = MANAGE
[3]GIGABIT-ETHERNETMODE = MONITOR
[4]GIGABIT-ETHERNETMODE = MONITOR

New Interface [1] :<cr>
```

- Cuando haya seleccionado la interfaz que desea utilizar; es necesario configurar las opciones de agente y de interfaz; al escoger una interfaz en el menú anterior, se le direcciona al siguiente menú; donde puede realizar las modificaciones que sean pertinentes.

```
***** Cisco SwitchProbe  V4.7.0 (Build 125) *****

Interface number : 3
```

```
[13] Configure Agent Options
[14] Configure Interface Options
[15] Change RMON parameters
[16] Change RMON2 parameters
[18] Software Options
[19] Security Options
[20] Console Logout
[21] Change ARTMIB parameters
[23] Change Probe Mode

[32] Go to Previous Page

          Enter your response or Enter "exit" to logout

Selection#: 13

           ***** Cisco SwitchProbe  V4.7.0 (Build 125) *****
Agent Options Menu:

[1]   Toggle router_discovery     on
[2]   Toggle router_enable        on
[3]   Toggle modem_log            on
[4]   Toggle slip_ip              off
[12]  Toggle ncp_request          on

[13] Go Back to Main Menu

***** Cisco SwitchProbe  V4.7.0 (Build 125) *****
Interface number : 3

[13] Configure Agent Options
[14] Configure Interface Options
[15] Change RMON parameters
[16] Change RMON2 parameters
[18] Software Options
[19] Security Options
[20] Console Logout
[21] Change ARTMIB parameters
[23] Change Probe Mode

[32] Go to Previous Page

          Enter your response or Enter "exit" to logout

Selection#: 14


          ***** Cisco SwitchProbe  V4.7.0 (Build 125) *****
Interface Options Menu:

Interface number : 3

[2]   Toggle vlan_mode            on
```

```
[8]   Toggle rawhdr_capture       on
[17]  Toggle Manage mode          off
[18]  Toggle Monitor mode         on

[19] Go Back to Main Menu
```

- Si adquirió alguna de las opciones de software; debe habilitarlas para poder utilizarlas. (seleccione la opción 18) y escoja la opción que desea habilitar.

```
***** Cisco SwitchProbe  V4.7.0 (Build 125) *****
Interface number : 3

[13] Configure Agent Options
[14] Configure Interface Options
[15] Change RMON parameters
[16] Change RMON2 parameters
[18] Software Options
[19] Security Options
[20] Console Logout
[21] Change ARTMIB parameters
[23] Change Probe Mode

[32] Go to Previous Page

          Enter your response or Enter "exit" to logout

Selection#: 18

           ***** Cisco SwitchProbe  V4.7.0 (Build 125) *****

Software Options Menu:

Interface number : 3

[1] Resource Monitor      on
[2] Netflow Monitor       off
[3] VLAN Monitor          on
[4] ART MIB Support       on

[32] return to previous menu
```

Para el caso de una sonda *WANProbe*; el proceso de configuración es el mismo; sin embargo, como es de suponer, las interfaces no son las mismas; por lo tanto, hay que configurarles el tipo de encapsulación, la velocidad de los enlaces, etc. Refiérase a la sección de anexos; para un ejemplo de la manera en que se deben configurar éstos parámetros en las interfaces de que se van a sondear.

NOTA: Recuerde deshabilitar la negociación de velocidades en el puerto del conmutador donde conecte el *SwitchProbe*; si no hace esto, podría tener algunos inconvenientes con el conmutador; el *SwitchProbe* es un elemento de supervisión; por lo tanto no envía información por ninguna interfaz que no sea la de administración(manage mode).

6.1.3 Configuración del módulo NAM.

Las tarjetas NAM son configuradas desde la interfaz gráfica del *TrafficDirector* de *CiscoWorks*. Sin embargo, antes de hacerlo, deben realizarse algunos pasos desde el CLI (*Command Line Interface*) del conmutador donde se encuentre.

1. Utilice el comando **show snmp**; este comando desplegará cuales características SNMP están habilitadas. La figura siguiente muestra la salida en pantalla en respuesta a la orden.

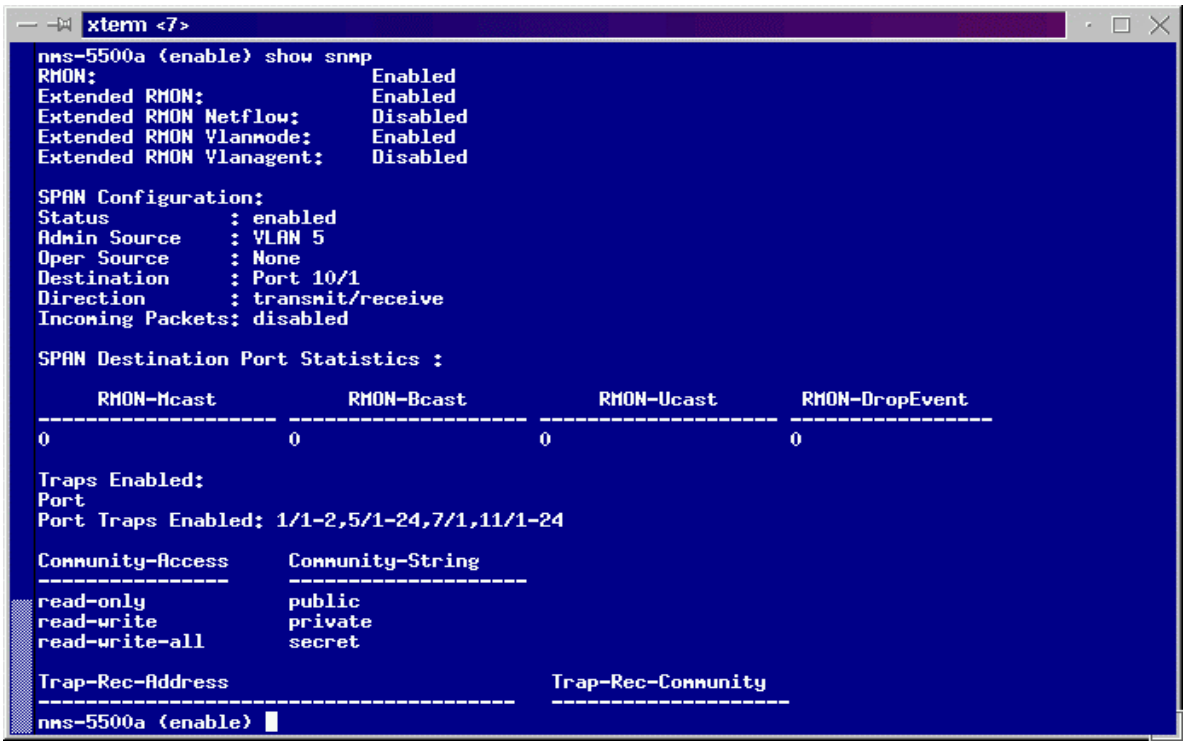


Figura 6.4 Respuesta en pantalla de la orden show snmp

2. Para que su NAM funcione correctamente debe tener las opciones de RMON y extended RMON habilitadas en el conmutador. Si en la información que obtuvo aparece que ninguna de las dos están habilitadas; utilice las ordenes:

switch-prompt: **set snmp rmon enable**
switch-prompt: **set snmp extendedrmon enable**

La figura siguiente muestra la respuesta en pantalla que obtendrá.

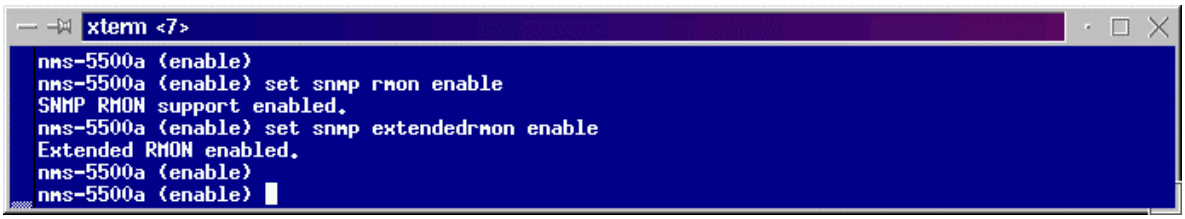


Figura 6.5 Respuesta en pantalla a las ordenes de habilitación RMON

3. Si además de eso, en su planes se encuentra el de sondear VLANs; debe utilizar las ordenes:

   switch-prompt: **set snmp extendedrmon vlanmode enable**
   switch-prompt: **set snmp extendedrmon vlanagent enable**

La primera orden le permitirá ver estadísticas por VLAN en vez de por dirección MAC (si el puerto SPAN está definido como el reflejo de un *Trunk*). Mientras que la segunda le permitirá ver estadísticas por VLAN además de estadísticas por puerto.

NOTA: La opción de VLANagent aumenta la carga en el NAM y quizá no sea recomendable para conmutadores con mucha carga

Éstos pasos son suficientes para que poder comunicarse con el NAM desde el NMS con la aplicación *TrafficDirector*. Asegúrese que la versión del *firmware* del la NAM sea compatible con la versión de *TrafficDirector* que posea.

6.1.4 Configuración del puerto SPAN (Switch Port Analyzer) en los conmutadores.

La utilización de SPAN es requerida para el funcionamiento correcto de los *SwitchProbes* y módulos NAM; ésta característica de los conmutadores permite el análisis de tráfico en puertos específicos o VLANs.

Para configurar esto, utilice las siguientes ordenes en modo privilegiado:

```
set span {src_mod/src_ports | src_vlan | sc0} dest_mod/dest_port [rx | tx | both] [inpkts{enable | disable}][multicast {enable | disable}] [create]
ej:
Console> (enable) set span 1/1 2/1
Enabled monitoring of Port 1/1 transmit/receive traffic by Port 2/1
```

```
Console> (enable) show span
Destination : Port 2/1
Admin Source: Port 1/1
Oper Source : Port 1/1
Direction : transmit/receive
Incoming Packets: disabled
```

Los siguientes ejemplos le permitirán comprender como configurar un puerto SPAN; ya sea con puertos como fuentes o bien VLANs.

Para hacer la VLAN 522 como la fuente SPAN y el puerto 2/1 como el destino:

```
Console> (enable) set span 522 2/1
Enabled monitoring of VLAN 522 transmit/receive traffic by Port 2/1

Console> (enable) show span
Destination : Port 2/1
Admin Source: VLAN 522
Oper Source : Port 3/1-2
Direction : transmit/receive
Incoming Packets: disabled

Console> (enable)
```

Ahora bien; si se requiere dedicar un puerto para el sondeo puede utilizar la siguiente orden:

```
crlab-5500a> (enable) set span 1 7/1 create
Created Port 7/1 to monitor transmit/receive traffic of VLAN 1
Incoming Packets disabled. Multicast enabled.

crlab-5500a> (enable) sh span
Destination : Port 7/1
Admin Source: VLAN 1
Oper Source : Port 5/2,5/9-24,6/1-5,6/7-9,9/1-2
Direction : transmit/receive
Incoming Packets: disabled
Multicast : enabled
```

Especifique los puertos fuente y destino, la dirección del tráfico a través del puerto fuente que desea sondear al puerto destino; y si el puerto destino, puede o no recibir paquetes. Para una descripción más detallada del uso del puerto SPAN consulte la dirección electrónica del caso, estipulada en la sección de bibliografía

NOTA: Si el puerto SPAN de destino está conectado a otro dispositivo y la recepción de paquetes está habilitada (usando la orden **inpkts enable**) el puerto destino SPAN recibe tráfico de cualquiera VLAN a la que este puerto pertenezca. Sin embargo, el puerto destino no participa en el *spanning tree* para esa VLAN.

Por lo tanto, tenga cuidado para evitar la creación de lazos cerrados de red con el puerto SPAN destino. Para lograr evitar los "*spanning tree loops"* , asigne el puerto destino SPAN a una VLAN que no esté siendo utilizada.

6.1.5 Configuración de TrafficDirector (TD)

Antes de iniciar la configuración de ésta aplicación; y para entender el concepto de cómo se logra el sondeo de la red utilizando la combinación de *SwitchProbes/WANProbes/NAM* y *TrafficDirector*, es importante tener en cuenta las siguientes definiciones:

Roving: el termino "*roving*" se refiere a cómo la aplicación *TrafficDirector* puede realizar un análisis completo RMON I y II a cualquier puerto de un conmutador que sea seleccionado. Esto implica realizar una conexión SPAN con un SwitchProbe/NAM donde se "refleje" de la información desde el puerto que se pretende sondear a un puerto destino; donde estará conectadá físicamente la sonda y que así se logre examinar el tráfico directamente. De aquí es donde viene el termino *"roving agent"* para referirse a cada una de las interfaces que la sonda posee; ya que éstas son definidas en el *TrafficDirector* como "agentes".

Archivo de Propiedades(Property Files): Este es un archivo que contiene las definiciones de varios tipos de protocolos o tráfico de capa 3 o superior, para ser sondeado. A éstos protocolos definidos en el archivo de propiedades, se les llama "dominios".

Para decirle al *"roving agent*" que datos recolectar y cuando, el proceso de configuración requiere que se utilice un archivo de propiedades para definir los parámetros necesarios.

Dominios (Domains): Como se dijo anteriormente, éstos son los protocolos que se definen en los archivos de propiedades. Existen 3 opciones para utilizar los dominios:

- Utilizar los dominios por defecto que vienen incluidos en el software *TrafficDirector* para utilizar con *SwitchProbes* y NAM (fw45prop y NAMprop respectivamente)

- Usar el *Domain Editor* para definir un nuevo dominio, o bien, seleccionar otros de los muchos que se encuentran definidos y utilizarlo como una plantilla.
- Crear un dominio personalizado

Existen 2 categorías de dominios soportados:

- Dominios de protocolo *(Protocol Domains)*: Requieren que se de un seguimiento de estadísticas RMONII en el *SwitchProbe* o NAM; éstos se utilizan cuando se quiere obtener datos de protocolos de capas 3 y 4.
- Dominios Genéricos *(Generic Domains)*: Requieren que se de un seguimiento de estadísticas RMON y se utilizan cuando se quiere obtener datos acerca del tráfico de capas 1 y 2

6.1.5.1 Configuración.

Los siguientes tres procesos de configuración están relacionados en la definición de un *SwitchProbe*, un conmutador o la combinación conmutador y NAM como agentes.

1. Agregar (Adding) la definición del Agente.
   - En la ventana principal del *TrafficDirector*, seleccione el botón circular de configuración; y seleccione el botón del *Config Manager*. La figura 6.6 muestra la ventana de configuración que se le desplegará.

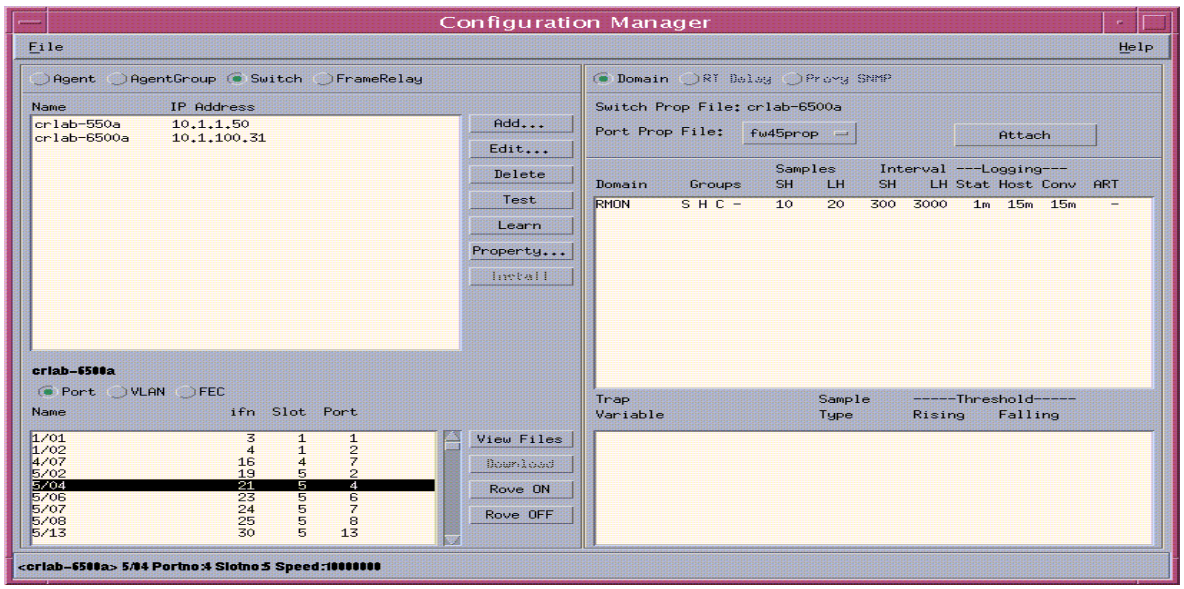


Figura 6.6 Ventana del *configuration manager*

- Seleccione el botón circular (*agent, switch o frame relay*) para identificar el agente de sondeo que va a definir, y presione el botón de agregar (*add*) La figura 6.7 muestra la ventana que se le presentará.

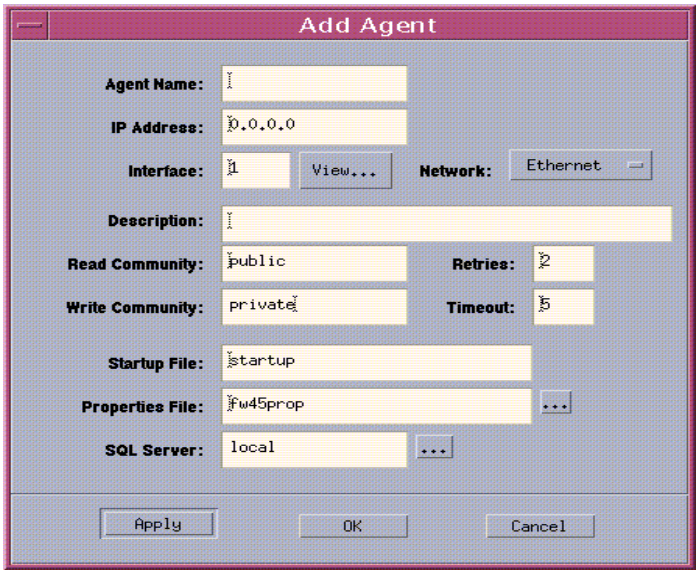


Figura 6.7 Ventana para la definición de agentes

- Asigne al agente un nombre y especifique la información pertinente para localizarlo en la red.

  Agent Name: Especifique el nombre que le dará a su agente.

  IP address: Dirección IP del Agente.

  Interface: Coloque aquí el número de la interfaz del SwitchProbe que está conectada físicamente al segmento que quiere sondear. (Asegúrese que esa interfaz esté en modo monitor) El botón *view* le permite ver y escoger las interfaces que desea agregar como agente.

  Read/Write community: Rellene con las palabras de seguridad que haya especificado para el dispositivo. Note que éstas son sensibles a las mayúsculas; y que si no son correctos, al *TrafficDirector* se le negará el acceso de los datos MIB.

En el caso de que quiera agregar un conmutador como agente la ventana de definición necesita los siguientes datos:

SwitchType: Seleccione el tipo de dispositivo a agregar.

Roving: seleccione aquí el agente *roving agent* (SwitchProbe/NAM) que tiene conectado al conmutador.

Analizer Port: identifique aquí el nombre del puerto donde se encuentre el agente físicamente conectado. (Si se tiene una NAM, ésta información es generada automáticamente; si se trata de un SwitchProbe debe especificar el #módulo/0#puerto; ej: 5/02 para el puerto 2 en el módulo 5)

La siguiente figura presenta la ventana de definición para un agente, en un conmutador.

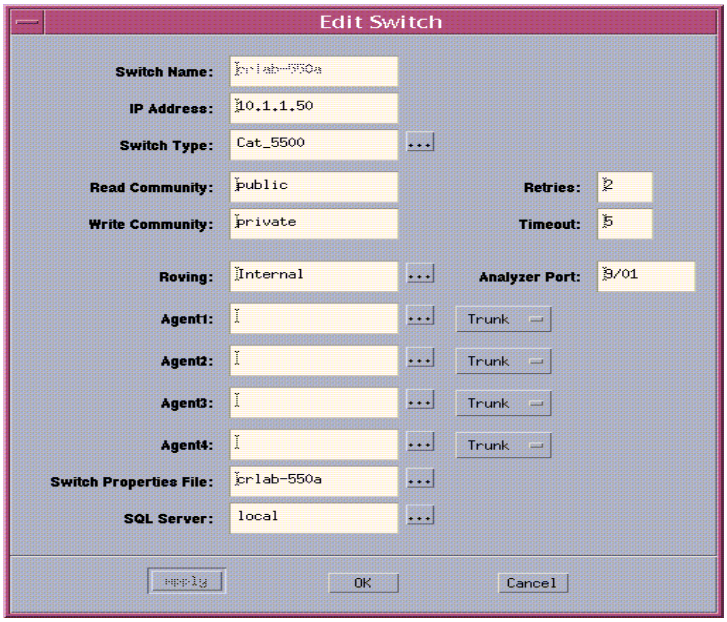


Figura 6.8 Ventana para la definición de un conmutador como agente

2. Prueba del dispositivo (*testing agent*). Después de que se ha definido el dispositivo como un agente en el *Configuration Manager*, es necesario verificar que la consola *TrafficDirector* puede comunicarse con el agente, éste proceso envuelve los siguientes pasos:
   - En la ventana del *Configuration Manager* seleccionar el nombre del agente y hacer click en el botón *Test.*
   - Si la prueba es satisfactoria se presenta una ventana con el resultado de las pruebas que la estación hizo al dispositivo (ver figura 6.9). Si la prueba no es satisfactoria, aparecerá una ventana que se lo informará.

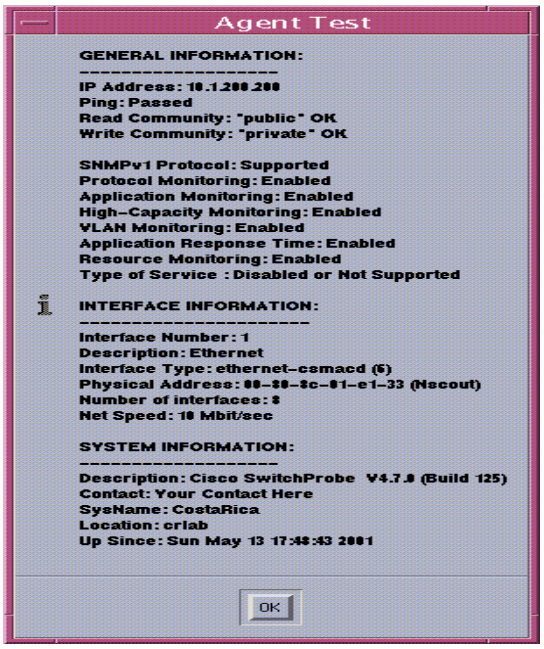


Figura 6.9 Ventana de información de la prueba del agente

3. Instalar las propiedades por defecto.

   Un archivo de propiedades es instalado después de definir las sondas como agentes. Los archivos de propiedades en un dispositivo con múltiples interfaces aplican para todas las interfaces que éste tenga.

   Éste proceso envuelve la selección del nombre del agente en la ventana del *Configuration Manager* y dar click en *Install*. La figura 6. muestra las opciones que tiene para instalar las propiedades; es recomendable utilizar la segunda opción; ya que se aplican los cambios y los contadores del agente se mantienen. Si después se desea realizar algún cambio en éste archivo, debe realizar el proceso descrito anteriormente e instalar esos cambios en el agente.

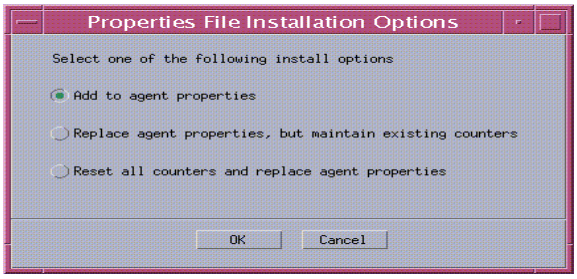


Figura 6.10 Opciones de instalación del archivo de propiedades

6.1.6 Configuración básica del servidor CW2000.

Antes de comenzar a utilizar las aplicaciones web de las que consta el CW2000; se necesita ingresar al servidor web; y configurar diversos parámetros para el correcto funcionamiento de las aplicaciones que corren sobre este servidor. Para correr estas aplicaciones y configurar el servidor, se debe tener acceso a la consola central de administración, por medio de un navegador. La dirección que permite accesar éste servidor es*:* http://servername:1741

La siguiente figura muestra la pagina web que se despliega al entrar al servidor web del CW2000.

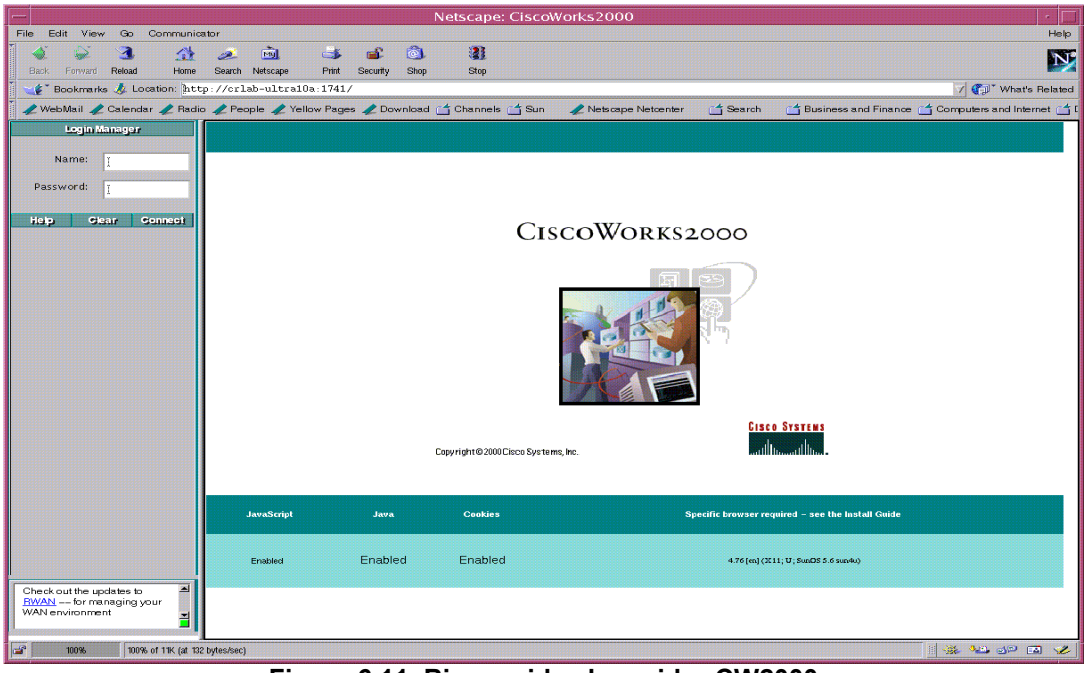


Figura 6.11 Bienvenida al servidor CW2000

Ya ingresado en éste, (utilice el ingreso por defecto (*login: admin, password:admin*); al lado izquierdo, aparecerán las etiquetas de los módulos instalados que corren sobre el servidor CW2000. Para configurar el servidor debe de escoger la etiqueta de ***Server Config*** → **Setup →ANI Server Admin** como se muestra en la siguiente figura.

Figura 6.12 Opciones de configuración para el servidor CW2000

A partir de aquí, debe de configurar las siguientes opciones:

- ***Discovery Settings*:**

  La figura 6.13 muestra los campos necesarios a rellenar para configurar la manera en que el servidor CW2000 utilizando un proceso con el servidor ANI (*Asynchronous Network Interface*); descubrirá todas las características de los equipos Cisco que posea en su red. Ésta configuración es quizá una de las más importantes; pues las aplicaciones CM y RME utilizan estos datos para realizar su trabajo en la red.

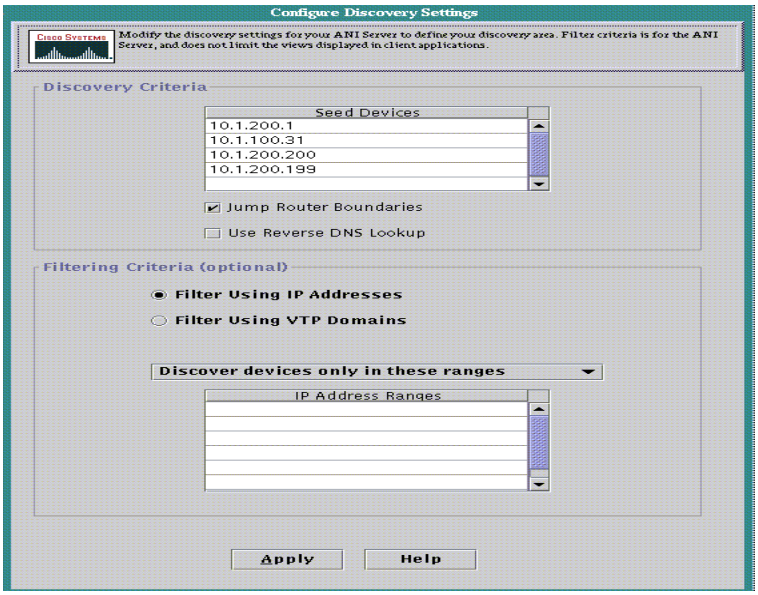


Figura 6.13 Configuración de los procesos de descubrimiento de dispositivos

Debe rellenar los campos de *Seed Devices*, con la direcciones IP de los conmutadores principales que se encuentren en la red.

- ***Discovery Schedule***

  En esta ventana; debe de escoger un horario adecuado para que el descubrimiento de los dispositivos de la red sea realizado. Consiste un definir una programación de los descubrimientos periódicos que el servidor puede realizar.

- ***SNMP settings***

  Coloque aquí, los *community strings* que haya asignado a los dispositivos; siga el formato indicado. Si solamente tiene un juego de palabras para toda su red, solo debe de rellenar una línea; si de lo contrario, tiene juegos de palabras diferentes, entonces deberá hacer una lista.

- ***Device Sync***

  La sincronización de dispositivos es una de las funciones importantes que debe de configurar. Si la consola de administración no tiene una plataforma NMS como *HP open view* , se pueden utilizar las funciones del *Campus Manager* en conjunto con el ANI server, para exportar los dispositivos descubiertos en su red, hacia la base de datos del módulo RME. Este proceso le ahorrara mucho tiempo; porque de lo contrario, debería definir todos los dispositivos manualmente o exportarlos desde otra plataforma NMS. También es posible realizar el proceso de manera inversa; para que el CM se encargue de descubrirlos y mostrarlos en su pantalla y el RME los encueste para obtener sus características.

- ***Client manager admin***

  El CAM es una administrador que mejora el desempeño del servidor, al bajar e instalar archivos del servidor a la máquina del cliente local; esto permite mejorar la respuesta inicial del cliente y las operaciones con *cache* de varias aplicaciones del CW2000. Para el correcto funcionamiento, debe instalar el CAM; y registrar todas las aplicaciones (*tasks*) en éste administrador (se realiza automáticamente cuando instala el CAM).

En la etiqueta de ***Setup*** el único proceso configurable, es la habilitación del uso del *Plug-In* de JAVA. Esto es de suma importancia, ya que la mayoría de las aplicaciones corren utilizando este lenguaje.

Finalmente, para comprobar el correcto funcionamiento de los procesos en el servidor, seleccione ***Server Config → Administration →Process Management →Process Status***; para asegurarse que éstos procesos corran normalmente; es normal que alguno procesos estén desactivados, pues se activan al correr una de las aplicaciones de los módulos que conforman el CW2000.

6.1.7 Escenarios de administración en redes LAN

Los siguientes escenarios de desarrollo de dispositivos para administración de redes pretenden ser una guía para demostrar la manera en que éstos dispositivos pueden ser utilizados y sacar provecho de las características que los hacen tan especiales.

La siguiente figura muestra un ejemplo de una red *enterprise* común que servirá como la base para los escenarios.

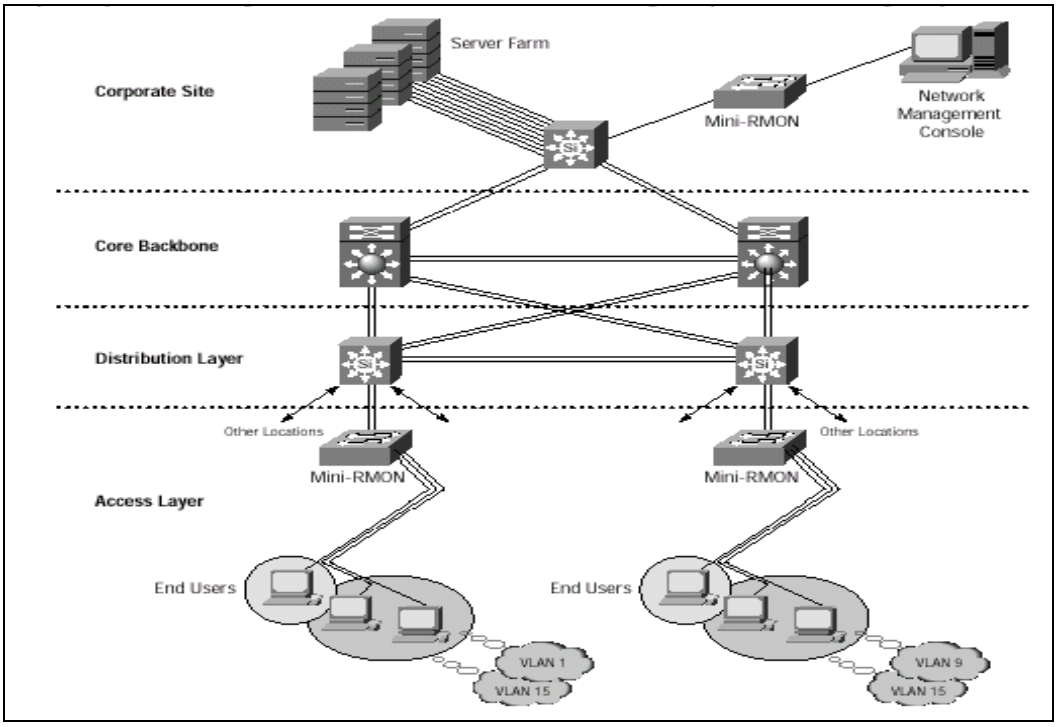


Figura 6.14 Diagrama de una red *enterprise* común

6.1.7.1 Escenario #1 *Troubleshooting* en ambientes LAN conmutados.

Introducción:

Para la administración de ambientes conmutados para la búsqueda de averías, es necesario contar con una sonda RMON en cada puerto del conmutador; pero esto no es efectivo. Cada puerto de los conmutadores Catalyst implementa un subconjunto de los MIB RMON conocido como mini-RMON; cada uno de éstos subconjuntos recoge información de estadísticas básicas de capa 2 en el tiempo (*packets in/out*, errores). Y también provee la habilidad de poner umbrales entre todas las estadísticas colectadas, con el envío de un mensaje *trap* cada vez que se alcance el límite umbral.

El *SwitchProbe* provee visibilidad total de las siete capas del modelo OSI de los paquetes que atraviesan el segmento supervisado y puede ser conectado al puerto analizador SPAN de un conmutador para análisis extensivos. El puerto SPAN de los Catalyst 5000/6000 puede ser configurado para ser un reflejo de los datos de cualquier puerto, grupo de puertos o una VLAN.

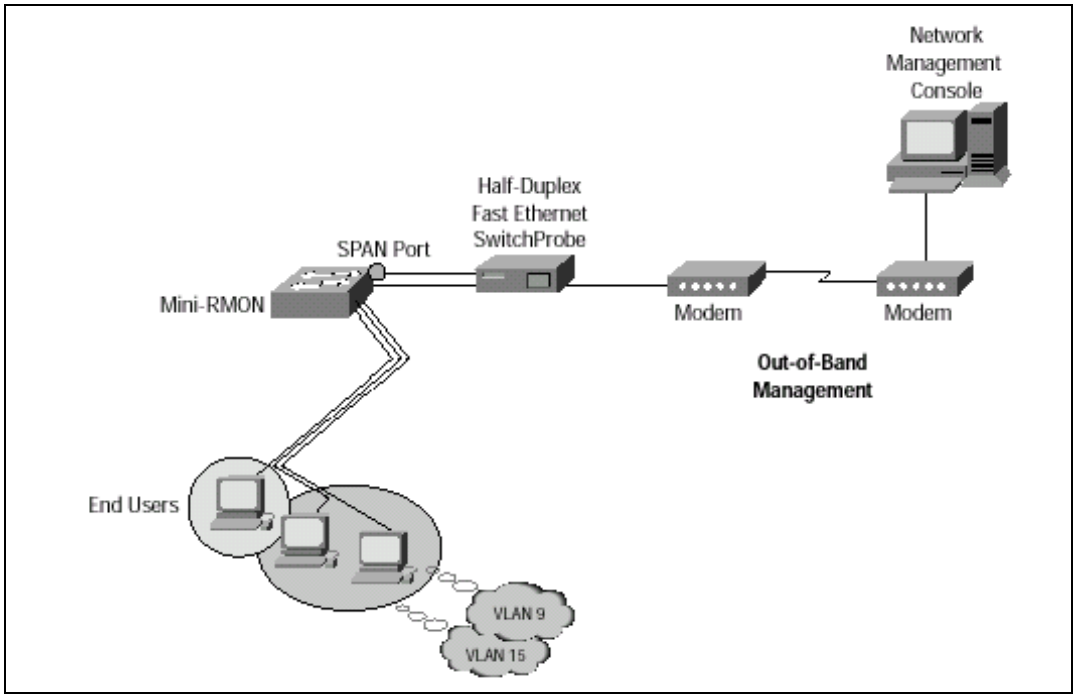


Figura 6.15 Escenario para la búsqueda de averías en ambientes LAN conmutado

Objetivos:

El objetivo primordial para la implementación de este escenario es que al conectar el *SwitchProbe* como se ilustra anteriormente, y lograr que la visibilidad dentro de la red sea extendida. Los agentes mini-RMON localizados en el conmutador proveen estadísticas básicas del enlace; y si además, se hace que el conmutador copie la información del tráfico de las VLANs al puerto SPAN el *SwitchProbe* podrá decodificar los paquetes que atraviesen ese segmento supervisado y determinar como éstos son enrutados, dónde fueron originados, a dónde van dirigidos, qué protocolos están siendo utilizados, y cuál aplicación generó el paquete.

Hay que tener en cuenta que el puerto SPAN en un conmutador no puede transmitir tráfico (simplemente es la imagen del puerto configurado); solo puede recibirlo. De ésta manera, una interfaz adicional es necesaria en el *SwitchProbe* para reportar los datos de vuelta a alguna aplicación de administración como el *TrafficDirector*.

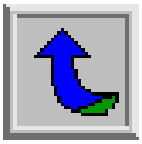
Como segundo objetivo, se demostrara la utilidad de los módulos NAM disponibles en los conmutadores de la familia Catalyst 5000, para realizar el sondeo de las 7 capas de manera integrada; utilizando el puerto SPAN del conmutador.

Dispositivos Necesarios:

- Conmutador de la familia Catalyst 5000 ó 6000(Con módulo NAM).
- SwitchProbe GE.
- Consola Central de Administración
- Demás recursos del laboratorio conectados al conmutador para la simulación de la carga.

Configuración Previa.

Para la ejecución de éste escenario, es necesaria la configuración previa del conmutador Catalyst 5500, de manera que se haga SPAN del puerto o VLAN que se desea sondear, al módulo NAM colocado en algún *slot* de expansión en el conmutador; de la manera que se explicó en la sección de configuraciones.



De igual manera se debe conectar el *SwitchProbe* a un puerto cualquiera del conmutador 6500 y hacer SPAN al mismo, para que así el tráfico pueda ser analizado por el agente.

En este caso, el *SwitchProbe GigabitEthernet (GE)* se conectó al puerto 1/1(puerto ethernet del *Supervisor Engine*) del conmutador Catalyst 6500 disponible en el laboratorio y se realizó el SPAN de las VLANs 1 y 100. Mientras que para el caso del módulo NAM, el SPAN se hizo al puerto 9/1 pues éste es el *slot* que el NAM ocupa en el Catalyst 5500.

Se procedió a configurar los agentes en *TrafficDirector* de la manera especificada en la sección de configuración.

Resultados.

Como era de esperar y se planteaba en los objetivos, con ambos agentes se logró visibilidad completa de las 7 capas de red.

La figura 6.16 muestra el gráficos acerca del tipo de tráfico que se observaba utilizando la opción *Segment Zoom (*Ventana de análisis de Tráfico); mientras que la figura 6.17 muestra el resultado de utilizar la opción *Protocol Zoom*(Ventana de análisis de protocolo) la cual muestra que el protocolo de capa 4 que estaba siendo utilizado en mayor porcentaje fue IP, especialmente UDP.

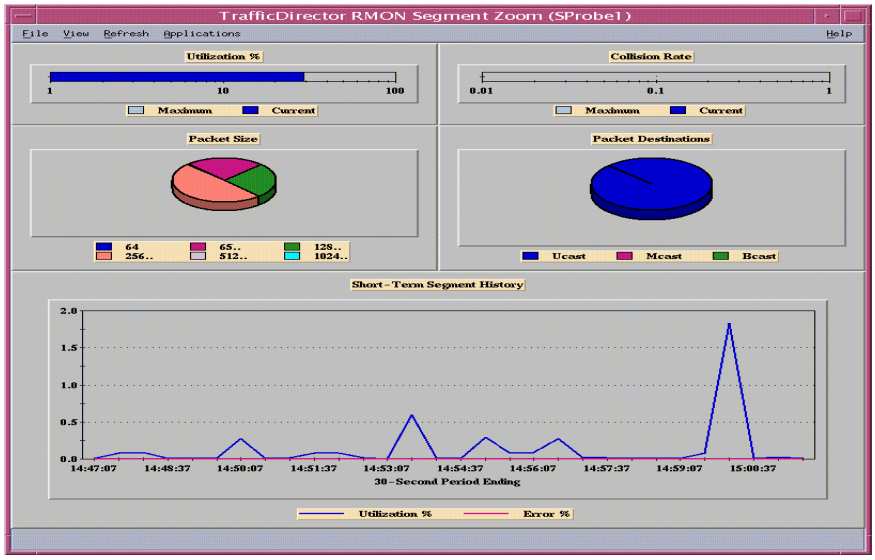


Figura 6.16 Estadísticas de tráfico "*segment zoom*"

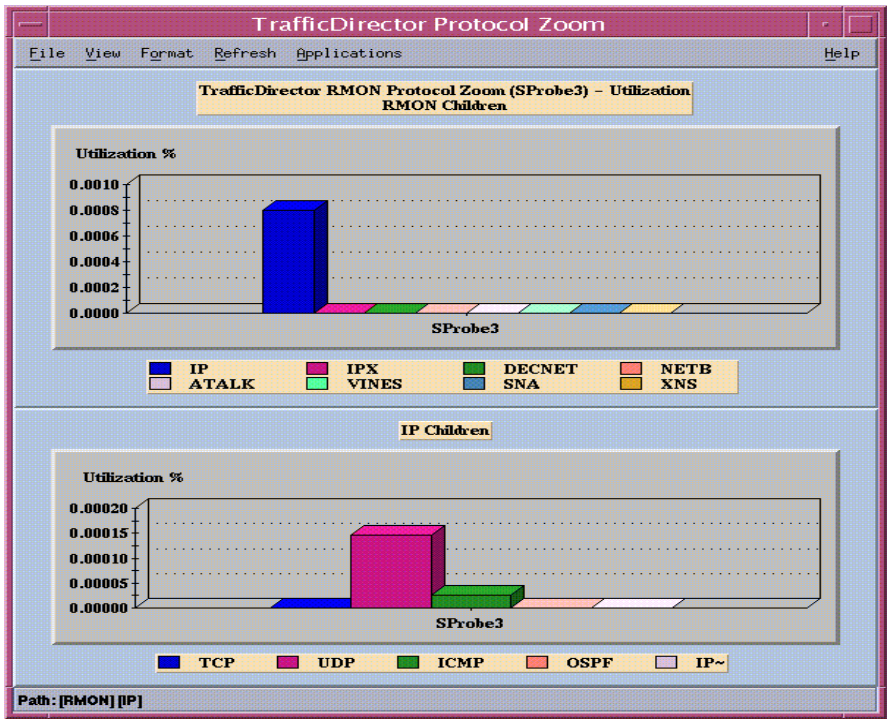
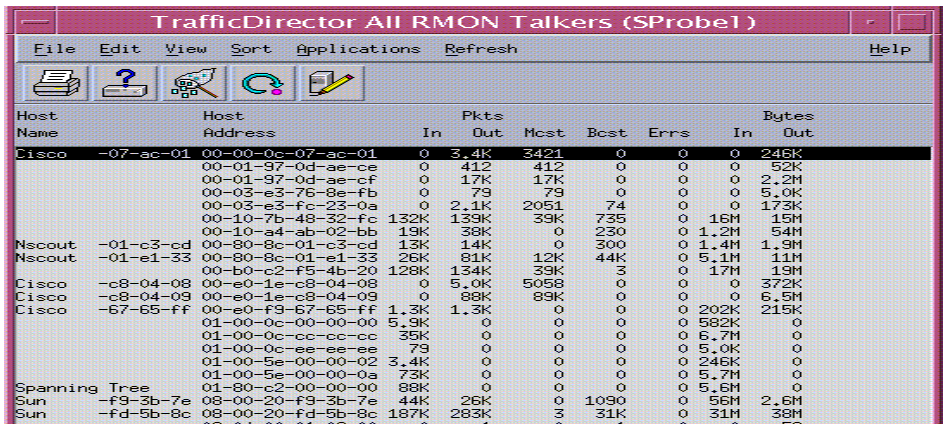


Figura 6.17 Estadísticas de utilización por protocolo

Ahora bien; además de esto, fue posible visualizar los conversadores "*Talkers*" que estaban generando éste tipo de tráfico (opción *allTalkers* en ventana de análisis de tráfico) y las conversaciones que utilizaban el protocolo ip; específicamente UDP (opción *all conversations* en la ventana de análisis de protocolos); estos resultados se muestran como figuras 6.18 y 6.19 respectivamente.



Host Name	Host Address	Pkts In	Pkts Out	Pkts Mcst	Pkts Bcst	Pkts Errs	Bytes In	Bytes Out
Cisco -07-ac-01	00-00-0c-07-ac-01	0	3.4K	3421	0	0	0	248K
	00-01-97-0d-ae-ce	0	412	412	0	0	0	52K
	00-01-97-0d-ae-cf	0	17K	17K	0	0	0	2.2M
	00-03-e3-76-8e-fb	0	79	79	0	0	0	5.0K
	00-03-e3-fc-23-0a	0	2.1K	2051	74	0	0	173K
	00-10-7b-48-32-fc	132K	139K	39K	735	0	16M	15M
	00-10-a4-ab-02-bb	19K	38K	0	230	0	1.2M	54M
Nscout -01-c3-cd	00-80-8c-01-c3-cd	13K	14K	0	300	0	1.4M	1.9M
Nscout -01-e1-33	00-80-8c-01-e1-33	26K	81K	12K	44K	0	5.1M	11M
	00-b0-c2-f5-4b-20	128K	134K	39K	3	0	17M	19M
Cisco -c8-04-08	00-e0-1e-c8-04-08	0	5.0K	5058	0	0	0	372K
Cisco -c8-04-09	00-e0-1e-c8-04-09	0	88K	89K	0	0	0	6.5M
Cisco -67-65-ff	00-e0-f9-67-65-ff	1.3K	1.3K	0	0	0	202K	215K
	01-00-0c-00-00-00	5.9K	0	0	0	0	582K	0
	01-00-0c-cc-cc-cc	35K	0	0	0	0	6.7M	0
	01-00-0c-ee-ee-ee	79	0	0	0	0	5.0K	0
	01-00-5e-00-00-02	3.4K	0	0	0	0	246K	0
	01-00-5e-00-00-0a	73K	0	0	0	0	5.7M	0
Spanning Tree	01-80-c2-00-00-00	88K	0	0	0	0	5.6M	0
Sun -f9-3b-7e	08-00-20-f9-3b-7e	44K	26K	0	1090	0	56M	2.6M
Sun -fd-5b-8c	08-00-20-fd-5b-8c	187K	283K	3	31K	0	31M	38M

Figura 6.18 Lista de todos los dispositivos activos el segmento "All Talkers"

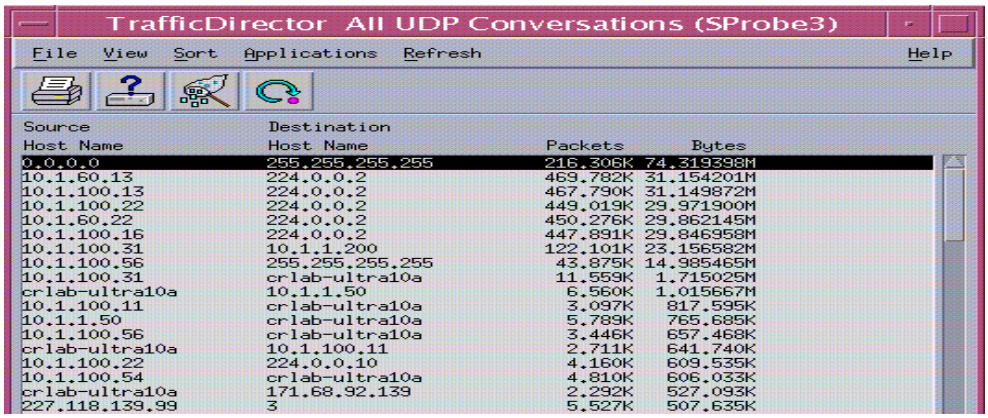


Figura 6.19 Lista de todas las conversaciones que utilizan el protocolo UDP

Ya hasta este punto, se ha demostrado la visibilidad de las capas 2, 3 y 4 que provee la sonda; pero hace falta demostrar visibilidad en la capa de aplicaciones. Para este caso, se realizó una trasferencia FTP entre las estaciones SUN que se tienen en el laboratorio. La interfaz ethernet del *SwitchProbe* se colocó de manera que se pudiera analizar el tráfico entre éstas estaciones. La figura 6.20 muestra como se registra el aumento de la utilización de la aplicación FTP en el segmento analizado (seleccionar TCP_APPS en la ventana de análisis de aplicaciones y luego seleccione el botón de *Aplication Monitor*); mientras que la figura 6.21 muestra los *Talkers* que producen ese aumento (seleccione una aplicación (FTP_CTRL) de la caja de dominios y luego la opción *all Talkers*)

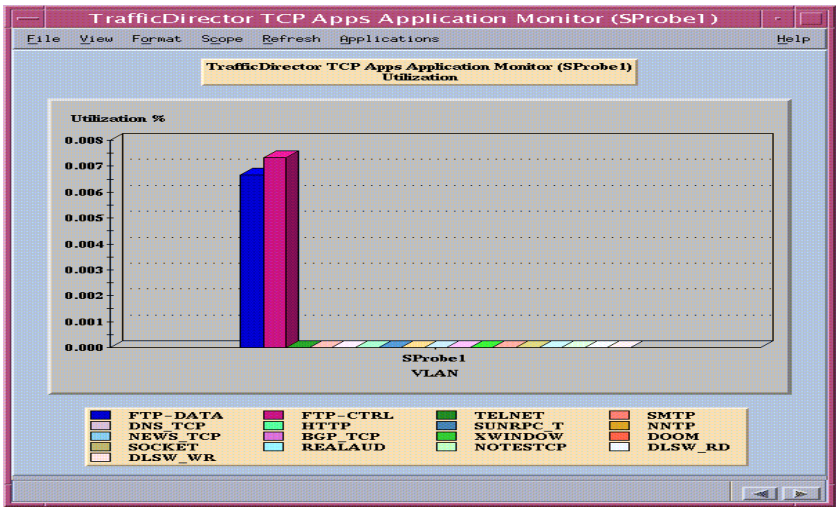


Figura 6.20 Análisis de tráfico por protocolos

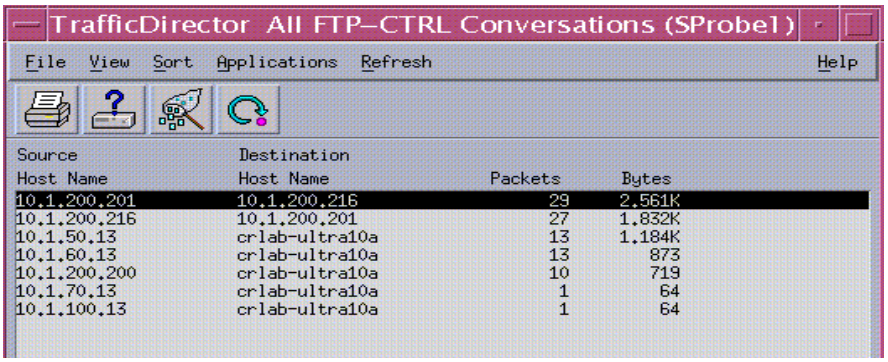


Figura 6.21 Análisis de las conversaciones por protocolo FTP

De esta manera, se logra demostrar que los dispositivos de sondeo dedicados, permiten visibilidad completa de las siete capas de red en el segmento que se desea administrar. Así; los agentes mini-RMON localizados en cada conmutador proveen las estadísticas básicas del estado del equipo; mientras que los equipos dedicados como el *SwitchProbe/NAM* complementan estas características y permiten visibilidad e información acerca del desempeño de los componentes del segmento; la cual refleja el estado de "salud" del mismo. Es importante destacar que los resultados obtenidos fueron los mismos para ambos equipos de sondeo lo cual resalta la importancia de la estandarización de RMON/RMON2 para el área de la administración de desempeño.

6.1.7.2 Escenario #2: Administración de Backbones y VLANs

Introducción:

Los *backbones* LAN comprendidos por los *conmutadores* y los enlaces troncales entre éstos requieren de supervisión estricta. La correcta y eficiente operación de los troncales es crítica para aplicaciones orientadas a negocios. La arquitectura VLAN permite a los administradores de red a construir LANs sin importar la localización de cada usuario. Las VLAN segmentan la LAN en grupos lógicos definidos, proveyendo ventajas en administración, seguridad y administración de tráfico. Sin embargo, esto introduce más retos para los esfuerzos en supervisar la red.

Un enlace troncal puede entenderse como múltiples segmentos que van a través del mismo cable. Así, para proveer información útil acerca del ambiente VLAN, deben ser recolectadas y reportadas estadísticas que reflejen la configuración actual de la VLAN.

Objetivo:

El objetivo de la implementación de éste escenario es el de demostrar que la capacidad de supervisar VLANs es soportada por el *SwitchProbe Switch Monitoring MIB (SMON MIB)*; la cual permite tratar cada VLAN como una interfaz individual con soporte RMON II total. Así, cuando un *SwitchProbe* es colocado entre dos conmutadores, la sonda decodifica los protocolos ISL o 802.1Q del troncal para obtener la información de la VLAN dentro del encabezado del paquete. Éste paquete puede ser decodificado luego para ser analizado respecto a las conversaciones, *top talkers*, protocolos de capas superiores y aplicaciones por VLAN.

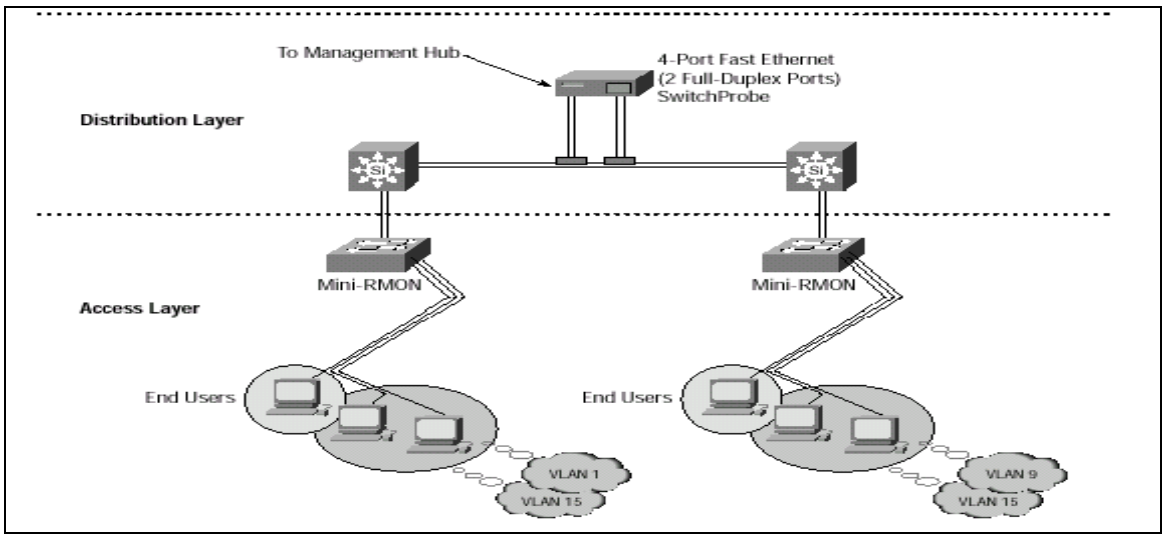


Figura 6.22 Escenario para la administración de Backbones y VLANs

De manera similar a la implementación del primer escenario, el segundo objetivo es demostrar la utilidad del módulo NAM para la administración de VLANs. El módulo NAM provee estadísticas individuales RMON I y II para cada VLAN ISL o IEEE 802.1Q en un enlace troncal.

Dispositivos Necesarios:

- 2 Conmutadores de la familia Catalyst (5000, 5500, 6500)
- SwitchProbe GE.
- Consola Central de Administración
- Demás recursos del laboratorio conectados a los conmutadores para la simulación de la carga.

Configuración Previa.

Para la ejecución de éste escenario fue necesario la utilización de un troncal entre los conmutadores 6500 y 5500 presentes en el laboratorio. Además, de necesaria la utilización de un *TAP kit* (divisor de señal) para fibra óptica para hacer la adquisición de datos que atravesaban el troncal. No se requirió de ninguna configuración especial (a excepción de la definición del *VLAN trunk*); pero si se tuvo que definir un nuevo agente en el *Configuration Manager*; pues se utilizarían ambas interfaces de *SwitchProbe GE* (procedimiento usual ver figura 6.23). Asegúrese de habilitar las opciones *vlanagent* o *vlanmonitor* en el conmutador que posea la NAM; y de habilitar la opción de software v*lan monitor* en el *SwitchProbe*.

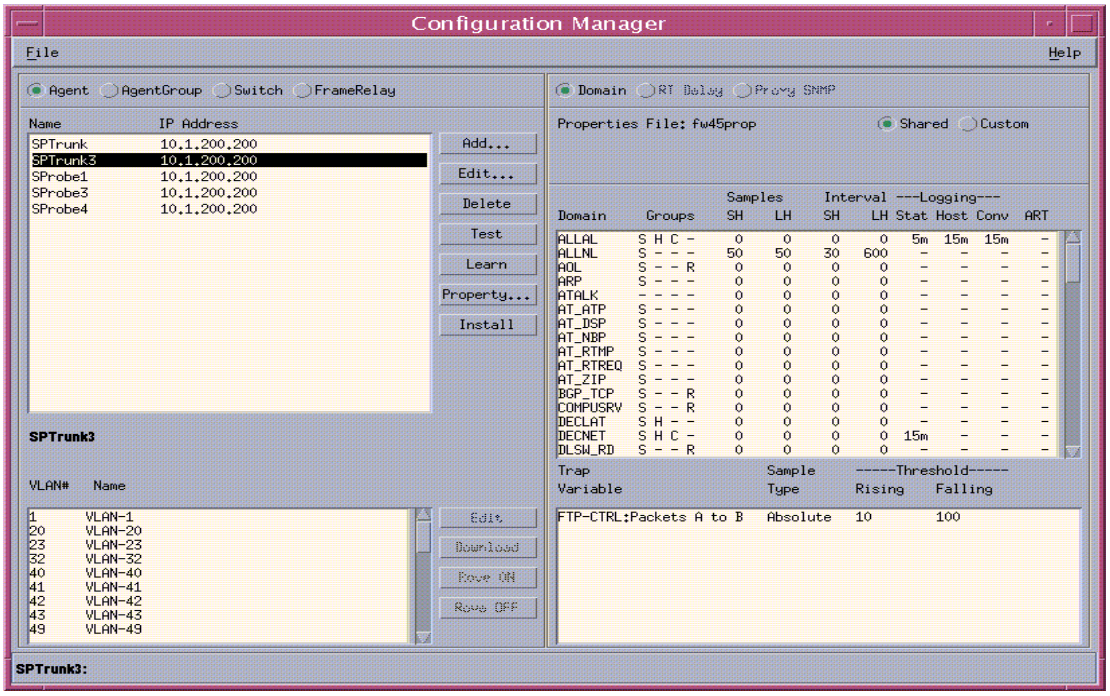


Figura 6.23 Definición del agente troncal en el *configuration manager*.

Resultados.

Inicialmente se procedió a recolectar la información acerca del tráfico que atravesaba el troncal para observar el tráfico por VLAN; ésta información puede ser observada utilizando la opción *VLAN Monitor* en la ventana de análisis de tráfico; seleccionando previamente el agente que tiene la conexión física. La figura 6.24 muestra los resultados obtenidos; en ellos se puede observar que en ese momento las VLANs 100 y 160 eran las que estaban más activas.

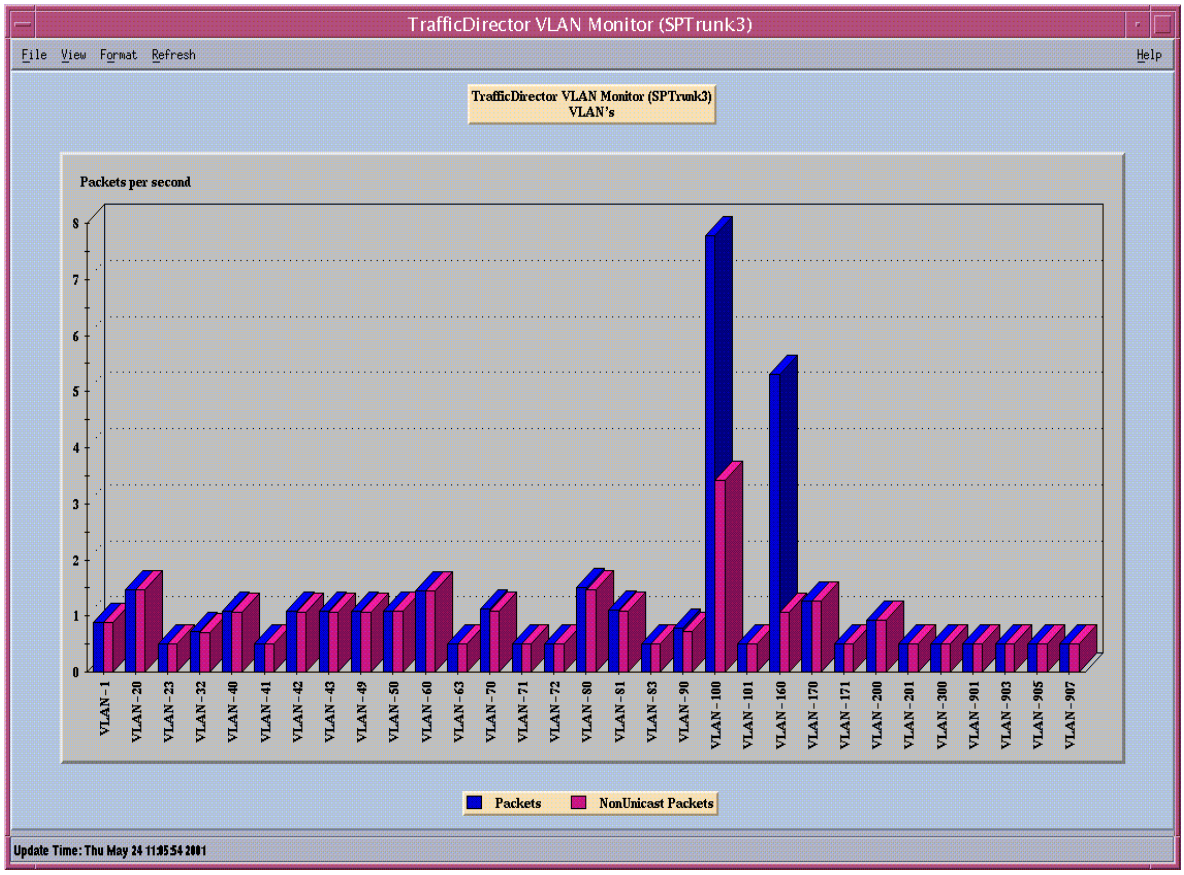


Figura 6.24 Análisis de tráfico en el troncal por VLANs

Ahora bien, si es necesario conocer cuántos bytes por segundo y cuáles son los conversadores "*talkers*" más activos en el troncal, se utiliza la opción *AllTalkers* en la ventana de análisis de tráfico; la siguiente figura presenta la información.

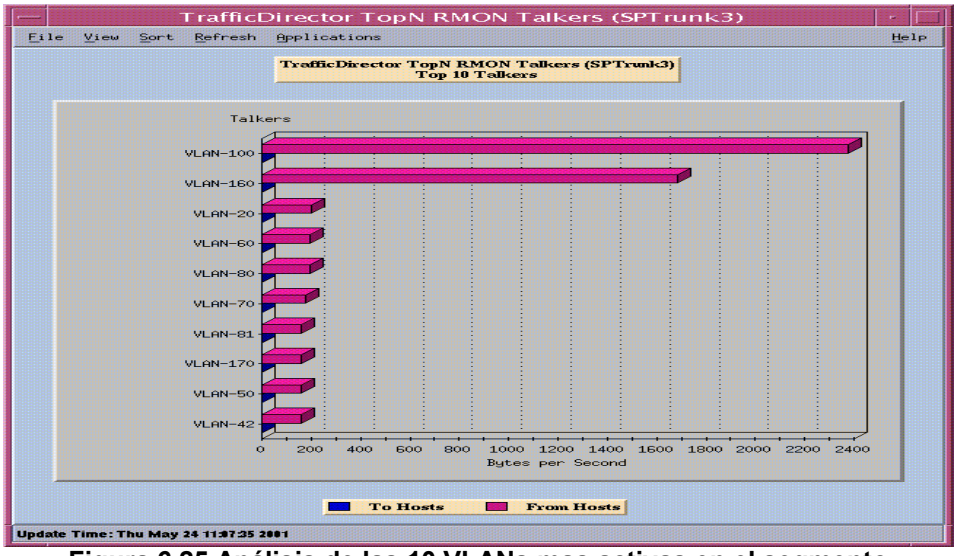


Figura 6.25 Análisis de las 10 VLANs mas activas en el segmento

De igual manera que en el escenario anterior, si es necesario conocer que tipo de protocolos se utilizan de mayor manera en cada VLAN. Para esto se utiliza la opción *Protocol Monitor* en la ventana de análisis de protocolos, previa selección de un dominio de protocolos. El caso que se presenta en la figura 6.24, el dominio que se analizó fue el de protocolos IP, así, se observa que de los protocolos IP, los que se estaban utilizando en mayor medida fueron el UDP e IGMP.

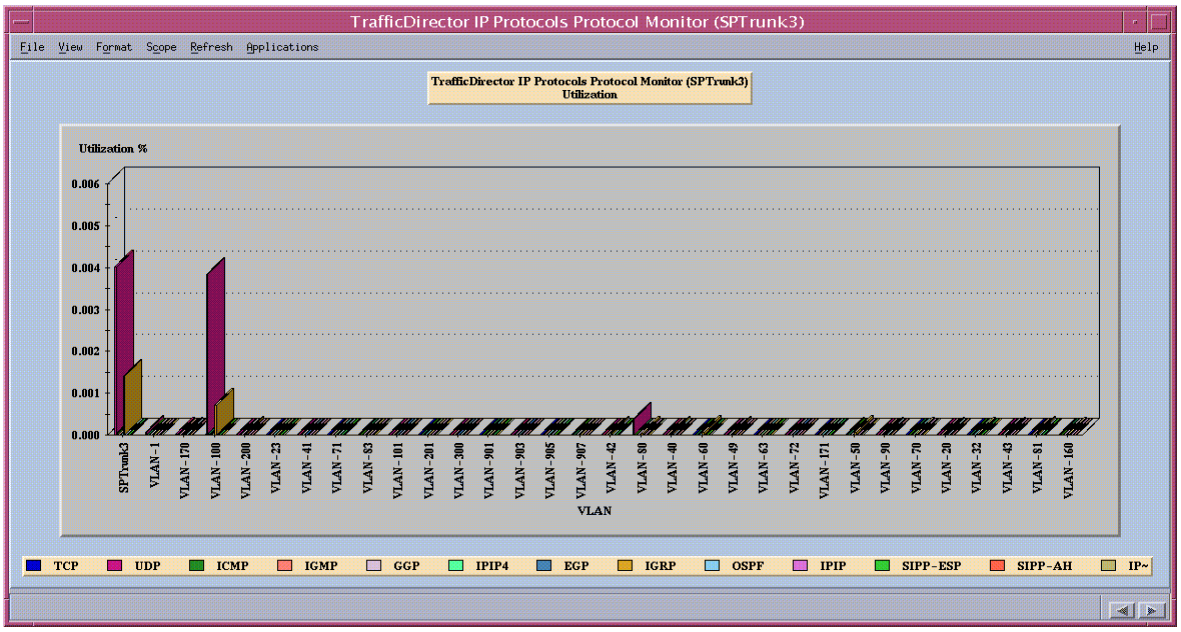


Figura 6.26 Análisis de utilización de protocolos por VLAN

Otra de las herramientas útiles para el análisis de los troncales es la opción de *TopNTalkers* (ventana de análisis de protocolos); ésta nos informa los diez dispositivos que se encuentran más activos en el troncal; y la dirección que esta conversación tiene; hacia el dispositivo o desde el dispositivo. Los resultados de este análisis se observan en la figura 6.27

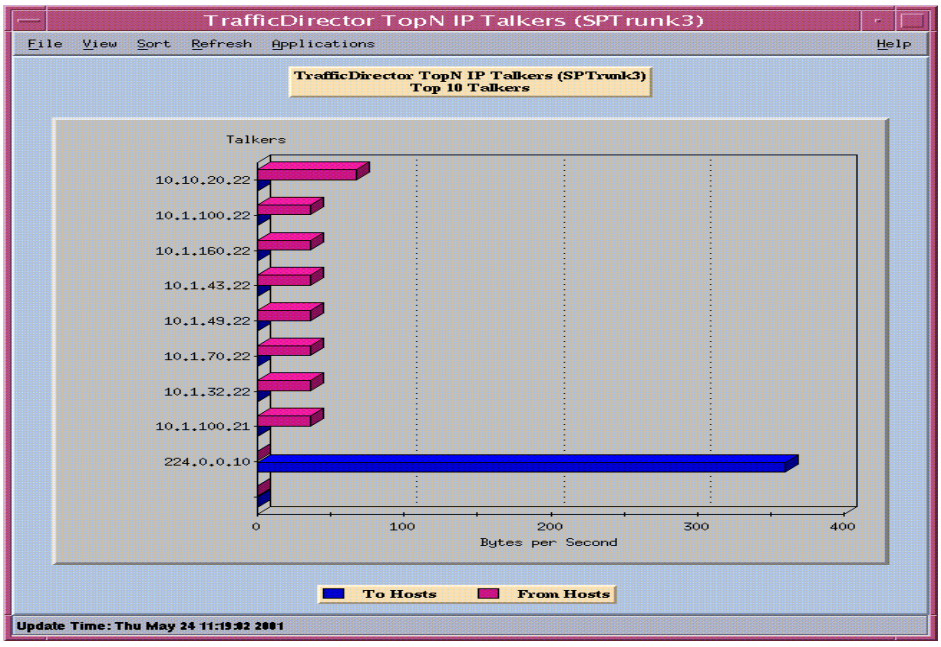


Figura 6.27 Análisis de las 10 Conversaciones IP mas activas.

A partir de los resultados obtenidos, se logró confirmar la utilidad que tiene la opción de software para la administración del desempeño que tiene los enlaces troncales en una red *enterprise*. Es importante destacar que ya sea el *SwitchProbe* o el módulo NAM, ambos pueden decodificar cualquiera de los protocolos de troncal ISL o bien 802.1Q y obtener la información de los encabezados del paquete.

6.1.1.3 Escenario #3 Administración de Servidores

Introducción:

Muchos de los ambientes LAN conmutados usan puertos de alta velocidad para las conexiones de los servidores Como consecuencia, los problemas en el enlace del servidor afectan la organización. Los enlaces a los servidores requieren supervisión diligente para el tratado de problemas. Uno de los problemas más frecuentes a los que están expuestos los servidores es el del aumento en tráfico. Esto puede ser simplemente por que es un día muy ocupado o bien por la intrusión de un *hacker*. La seguridad de la red es aumentada de buena manera por el uso de los SwitchProbes.

Objetivo:

Demostrar que el *SwitchProbe* puede detectar el aumento repentino de tráfico al configurar el umbral de aumento de utilización del puerto conectado al servidor.

Así, cuando la utilización del puerto alcanza el umbral máximo estipulado por un periodo específico de tiempo, una condición de alarma es desencadenada. El S*witchProbe* puede ser configurado para el envío de un *trap* SNMP hacia una estación de administración especificada. Y además de eso, capturar paquetes (hasta 16MB) para su posterior análisis si la situación fue realmente una intrusión y violación en la red.

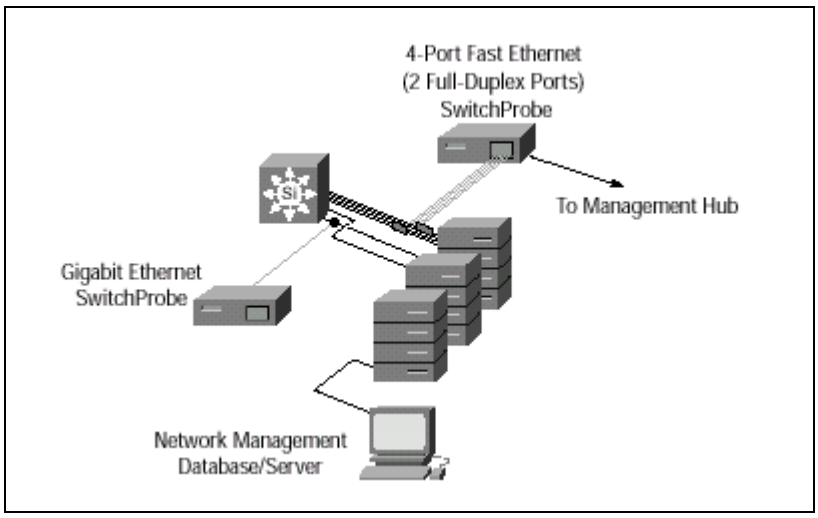


Figura 6.28 Escenario para la administración de servidores

Al implementar el escenario mostrado en la figura, se pueden alcanzar la administración de la cantidad de tráfico que tiene el servidor; además de supervisar los tiempos de respuesta de las aplicaciones que se corren en el mismo..

Dispositivos Necesarios:

- 2 Conmutadores de la familia Catalyst (5000, 5500, 6500)
- SwitchProbe GE.
- Consola Central de Administración
- Demás recursos del laboratorio conectados a los conmutadores para la simulación de la carga.

Configuración Previa.

La ejecución de este escenario requiere la configuración de alarmas (traps) en la aplicación *TrafficDirector*, de manera que se definan valores umbrales para el aumento/descenso de tráfico en el enlace del servidor que se desee administrar.

Inicialmente, es necesario entrar a la ventana del *Configuration Manager* ; y escoger el agente conectado físicamente al enlace del servidor.

Luego, se debe hacer click en el botón de "*Property*" para desplegar la ventana del editor de propiedades; donde se definen los valores umbrales para el *trap* que se definirá (ver figura 6.29).

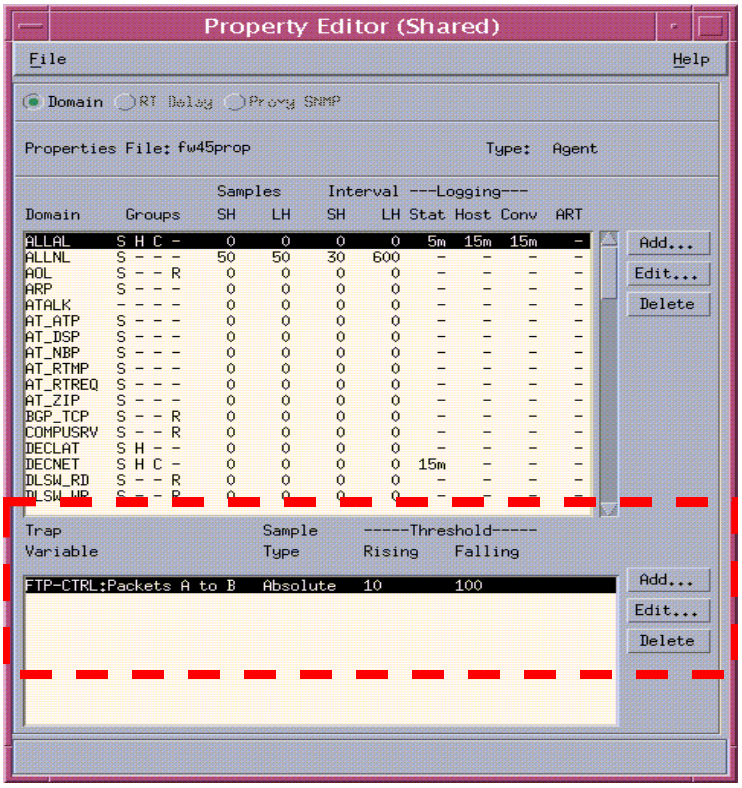


Figura 6.29 Ventana del editor de propiedades

El siguiente paso es el de definir los valores umbrales para definir el *trap*. Partiendo de la ventana del editor de propiedades, hay que hacer click en el botón *Add* de la parte inferior de la ventana. La siguiente figura presenta la ventana donde se brindan los parámetros para definir el *trap*.

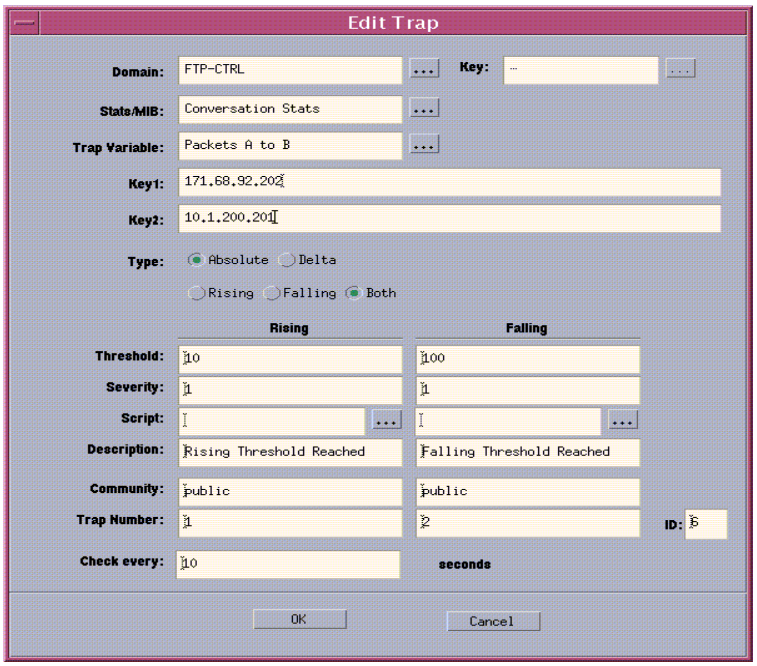


Figura 6.30 Ventana para la definición de alarmas (traps)

Es necesario definir los siguientes parámetros:

Domain: Protocolo o aplicación que se desea sondear

Stats/MIB: Tipo de estadística que se desea sondear.

TrapVariable: Aquí se define la variable a sondear.

Key1: Aquí se especifica la dirección origen del tráfico a analizar.

Key2: Aquí se especifica la dirección destino del tráfico a analizar

Type: En este campo se escoge el tipo de "disparador" de umbral que se definirá. Puede escoger entre revisar los umbrales como valores absolutos o delta; y si se desea que el evento se desencadene en el umbral de ascenso, en el de descenso o en ambos.

Thershold: Aquí se definen los valores umbrales a sondear.

Community: Aquí se definen la palabra clave de solo lectura.

Check Every: Aquí se define el tiempo de muestreo de los valores umbrales.

Resultados.

Para simular este escenario; se utilizó una de las estaciones SUN para que funcionara como servidor, al servicio de toda la red campus del laboratorio regional de Costa Rica.

El tráfico que se sondeó fue nuevamente tráfico FTP; pues éste es uno de los más pesados por la transmisión de datos en ráfagas y tiempo prolongado. La figura 6.31 presenta la notificación recibida por la consola de administración, anunciando que se alcanzaron los umbrales estipulados.

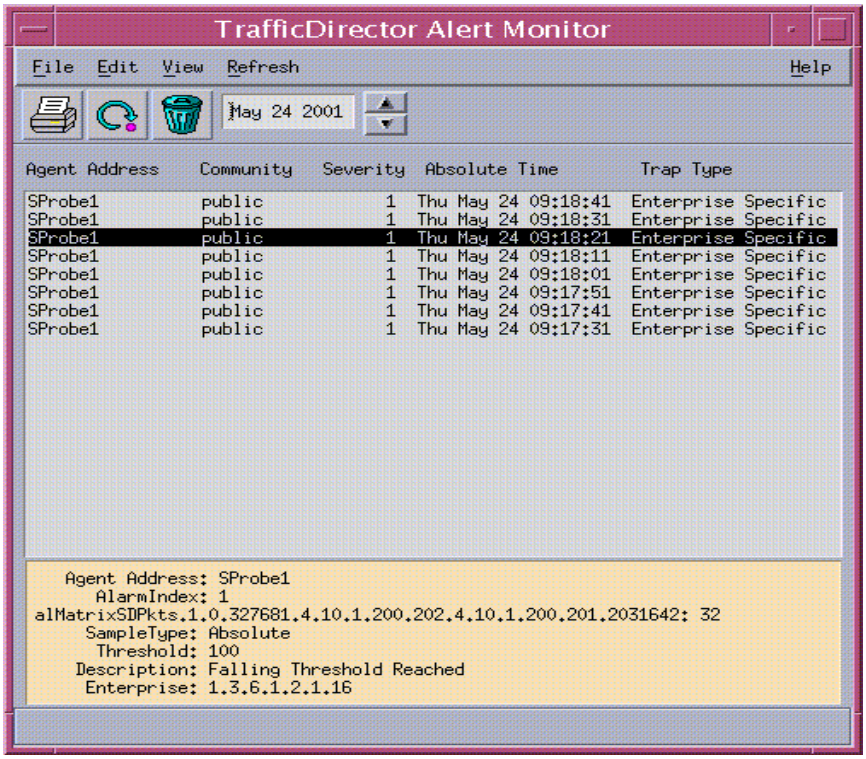


Figura 6.31 Ventana de recepción de alarmas "Alarm Monitor"

Otro de los objetivos que se planeó alcanzar, fue el de utilizar la función de captura de datos; apara luego analizarlos; ya que esta función es útil en el caso de posibles intrusiones a la red que se está administrando. La figura 6.32 muestra la ventana de configuración para iniciar la captura de los datos; mientras que la figura 6.33, muestra la ventana de análisis de estos datos.

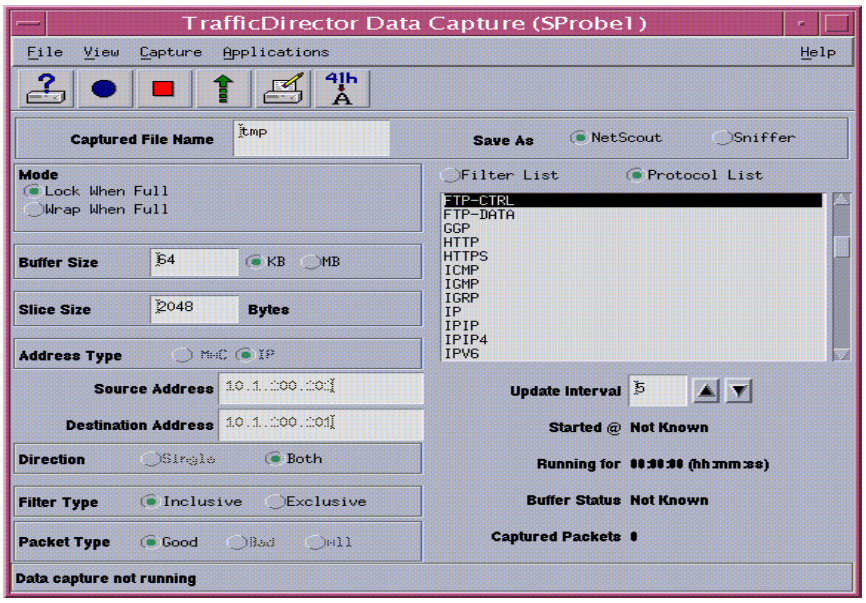


Figura 6.32 Aplicación de Captura de Datos

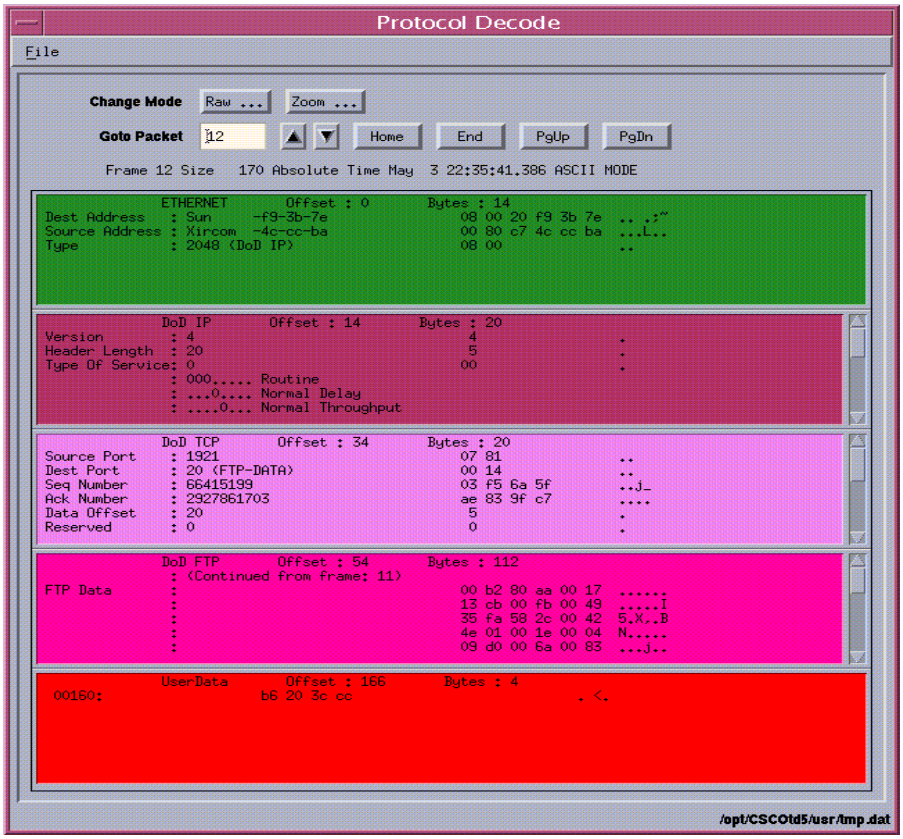


Figura 6.33 Aplicación de decodificación de protocolos

Finalmente, ya alcanzados los objetivos; cabe destacar la importancia de estas herramientas; para lograr un control exacto de las variables que podrían causar una sobrecarga de los servidores en una red *enterprise*; y de igual manera capturar y analizar la información a la que se puede tener acceso desde los servidores. Por supuesto, la captura de datos toma mayor importancia si el servidor al que se accesa debe ser protegido de intrusiones no autorizadas.

6.1.1.4 Escenario #4 Alertas y notificación de eventos

Introducción:

Quizá no sea la mejor estrategia de administración, el tener una estación administradora haciendo *ping* a dispositivos críticos de la red, para comprobar la disponibilidad de los mismos, sus tiempos de respuesta o bien consultar las variables MIB de los dispositivos tales como el uso del CPU; especialmente, si esos dispositivos están en lugares remotos accesibles por enlaces de ancho de banda muy bajo.

Objetivo:

Demostrar la utilidad del *SwitchProbe* como dispositivo de administración para localidades remotas y como, si éste fuera colocado cerca del dispositivo remoto que va a ser sondeado, podría realizar *pings* para comprobar la disponibilidad y la demora en el viaje de ida y vuelta (*round-trip delay)* del dispositivo. De igual manera, demostrar, como el *SwitchProbe* se encargaría de sondear el dispositivo por las variables MIB estipuladas y sus valores umbrales, para que un evento de alarma se desencadene cada vez que el límite umbral sea alcanzado. Así, todo el tráfico que se utilizaba para esta misma función sin el *SwitchProbe* se reduce a un paquete *trap* SNMP a través de lo que podría ser un enlace de bajo ancho de banda y de alto costo.

Dispositivos Necesarios:

- Conmutadores de la familia Catalyst (5000, 5500, 6500)
- SwitchProbe GE.
- Enrutadores (3600, 7500)

- Consola Central de Administración

Configuración previa.

Para comprobar los objetivos especificados para este escenario; es necesario configurar las funciones de medición de disponibilidad, retraso de ida y vuelta (*round trip relay*) y de administración *proxy* SNMP.

Antes de configurar estas funciones en el *TrafficDirector*, debe de habilitarse la opción de software de sondeo de recursos (*Resource Monitor*); además, se debe de configurar las propiedades de manera personalizada (*Custom Properties*).

Las propiedades personalizadas se configuran en la ventana del *Config Manager*, como se muestra en la siguiente figura.

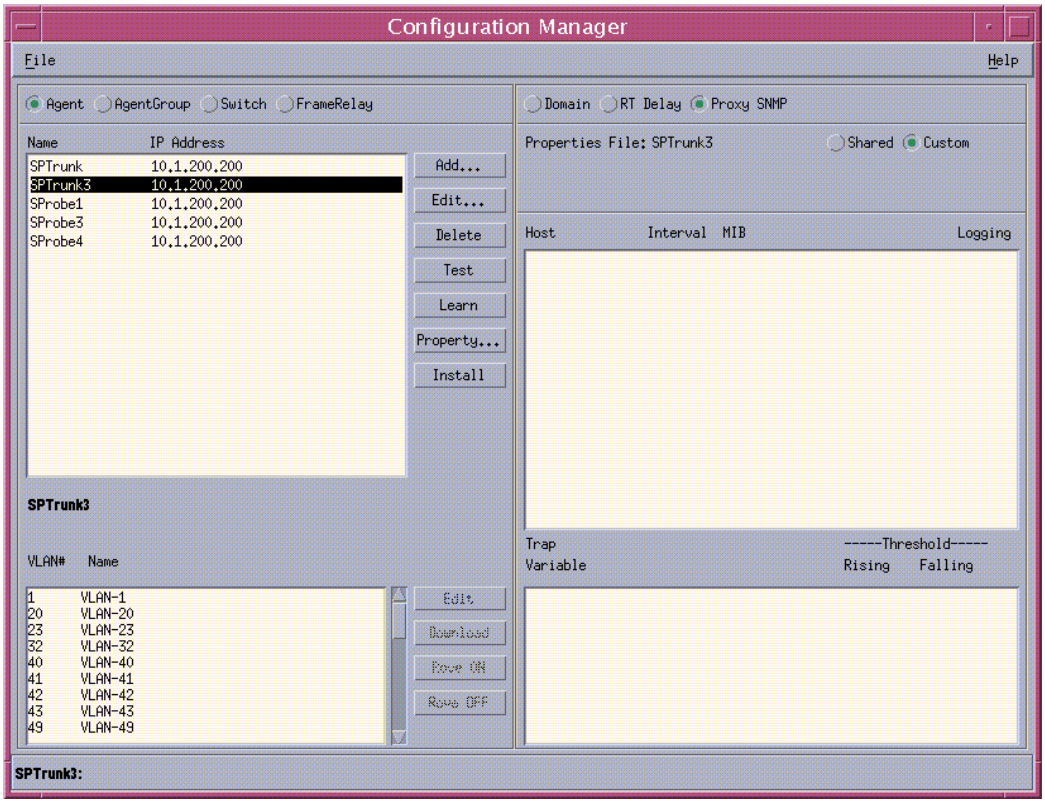


Figura 6.34 Ventana del *configuration manager*

Posteriormente, se debe de escoger la opción del *property manager*. Ésta le presentará la ventana de configuración de propiedades; y ahí se debe de escoger nuevamente el botón de *proxy* SNMP o bien *round trip delay* según lo que quiera configurar; además, del botón de agregar. La ventana de configuración del agente *proxy* SNMP se muestra en la siguiente figura.

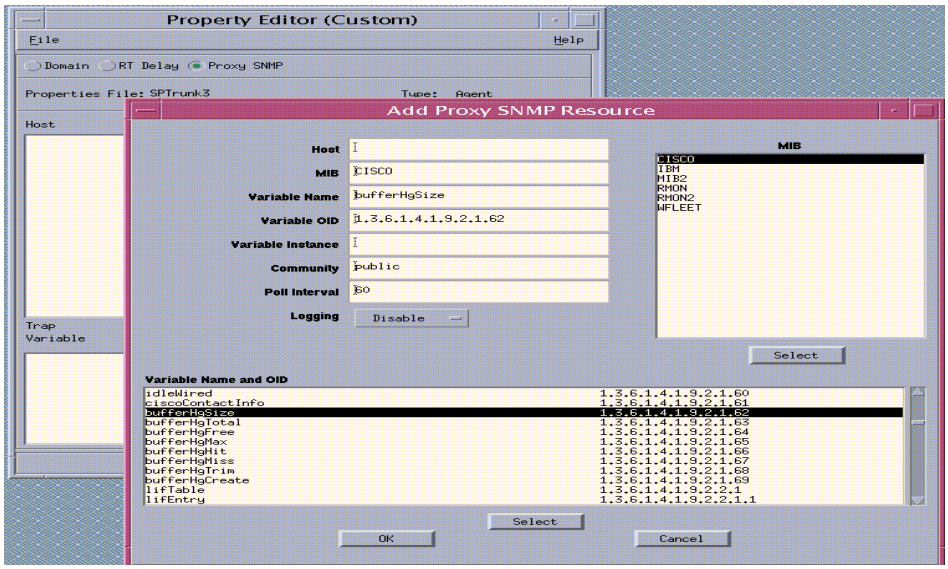


Figura 6.35 Ventana de configuración de agente proxy SNMP

Para configurar ésta herramienta, debe tener muy claro si el dispositivo que va a administrar soporta las variables y tablas MIB que pretende implementar. Inicialmente;

- debe de escoger la tabla MIB que utilizará,
- el nombre de la variable y OID,
- luego la instancia (usualmente esto corresponde al número de la interfaz con la cual el objeto MIB que se supervisará está asociada) y la variable, que la sonda estará preguntando al dispositivo que se indique.
- Posteriormente si se desea se puede habilitar la bitácora (*logging*).

De manera similar se realiza la configuración de la herramienta de sondeo de disponibilidad y de medición del retraso de ida y vuelta. La figura 6.36 presenta la ventana de configuración.

Los únicos parámetros que se deben de definir son la dirección del dispositivo que se administrará, el intervalo de muestreo, y si se debe hacer un archivo bitácora (*logging*) para almacenar los resultados.

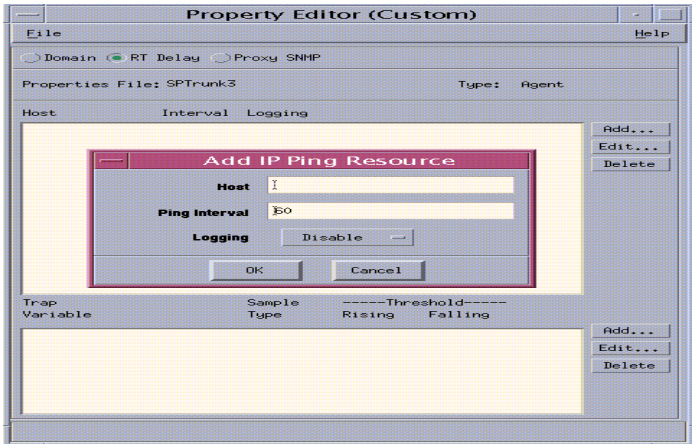


Figura 6.36 Ventana de configuración de aplicación RT delay

Resultados.

Como era de esperarse, los objetivos se cumplieron completamente, las figuras 6.37 y 6.38 presentan los resultados del sondeo de variables MIB especificas usando la herramienta *proxy* SNMP y las mediciones de disponibilidad y *round trip delay*, respectivamente.

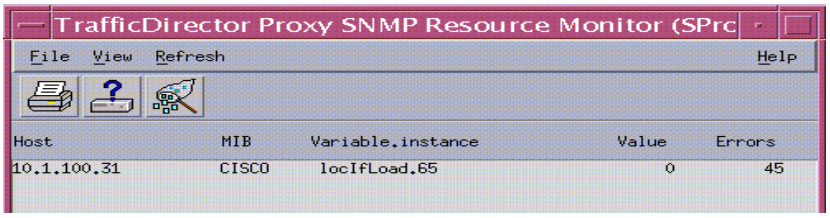


Figura 6.37 Resultado del sondeo proxy SNMP

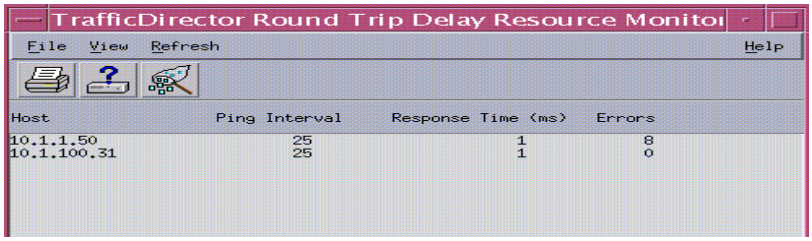


Figura 6.38 Resultado del sondeo *round trip delay*

El resultado obtenido con la prueba de sondeo *proxy* es muy importante; ya que como se puede observar en la figura 6.37 la variable sondeada no existe para el dispositivo que se estaba encuestando. Como se mencionó anteriormente, es de suma importancia que conozca que es lo quiere sondear, que MIB y que variable utilizará para hacerlo y si el dispositivo o el entorno de red soportan esa variable.
La explicación acerca de los errores mostrados en la figura capturada de pantalla corresponde a que esta variable, es específica para el sondeo de entornos donde se utilice el protocolo IGRP. El siguiente extracto del documento ***MIB Quick Reference Guide*** (refiérase a la bibliografía) donde se definen las variables que se pueden sondear y su significado se presenta a continuación:

> **locIfLoad**
> Provides the loading factor of the interface. The load on the interface is calculated as an exponential average over 5 minutes and expressed as a fraction of 255 (255/255 is completely saturated). Used by Interior Gateway Routing Protocol (IGRP).
> Syntax: Integer
> Access: Read-only

Finalmente, los resultados de la medición de disponibilidad y tiempos *round trip delay*, demostraron que esta herramienta es muy útil para que el administrador se mantenga al tanto de la disponibilidad de dispositivos que se encuentran en localizaciones remotas y darse una idea de la manera en que este dispositivo está respondiendo a las encuestas de la consola central de administración. Esta característica, en conjunto con el sondeo de variables MIB de manera remota, permiten la administración del desempeño de la red de manera proactiva

6.1.7.5 Escenario #5 Supervisión ART (Aplication Response Time)

Introducción:

La supervisión de aplicaciones críticas, es una prioridad alta en redes *enterprise*. Cuando los usuarios de la red y el departamento de IT establecen *Service Level Agreements (SLAs)* para las aplicaciones, muy a menudo éstos y el departamento IT se encuentran en desacuerdo el uno con el otro.

Los usuarios pueden exigir disponibilidad de las aplicaciones un 100 % del tiempo, además de un tiempo de reacción instantáneo de las aplicaciones, y el uso libre e ilimitado de la red. Satisfacer esas demandas es difícil, consecuentemente, el departamento IT pierde credibilidad, la productividad del negocio sufre debido al comportamiento ingobernable del usuario, y los costos del ancho de banda crecen fuera de control. Esto implica el surgimiento de preguntas acerca de a qué puede atribuirse el retraso en el tiempo de respuesta.

Objetivo:

Usualmente, las medidas para asegurar los SLAs se resuelven usando la disponibilidad y el tiempo de reacción de las aplicaciones de la red; de esta manera, el objetivo es el de demostrar como el *SwitchProbe* puede de gran utilidad en determinar y vigilar los SLAs usando la opción ART MIB. Esto se puede lograr, ubicando sondas a lo largo del *backbone*, cerca de los clientes y cerca de los servidores. El ART MIB, es una opción en los *SwitchProbes/WANProbes*, y proporciona datos detallados e información utilizada para medir el tiempo de respuesta en el intercambio solicitud-respuesta del protocolo (TCP) entre los clientes y los servidores. El ART MIB acumulará los tiempos transcurridos en milisegundos para todos los pares solicitud-respuesta que un agente observa durante cada intervalo de reporte.

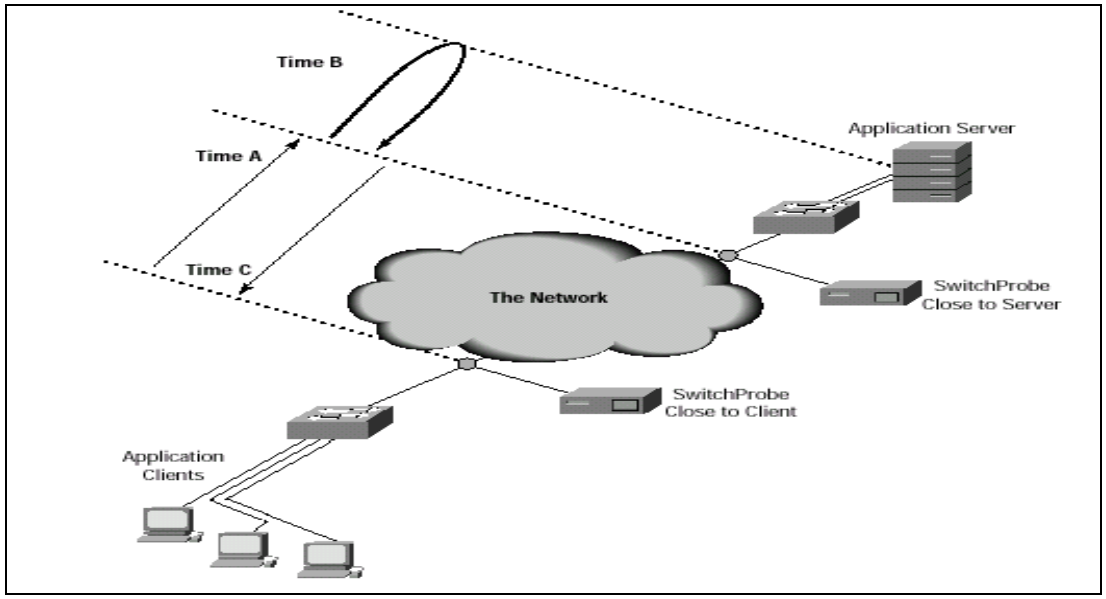


Figura 6.39 Escenario para la supervisión de los tiempos de respuesta de las aplicaciones

El posicionamiento estratégico de los *SwitchProbes* habilitados con el ART MIB incrementa en gran medida el valor de la información vista a través de la red. Cuando se mide el desempeño de los tiempos solicitud-respuesta del flujo de aplicaciones especificas, el tiempo de "viaje" redondo es la suma de los tiempos A, B y C.

- El tiempo A es el que toma la solicitud del cliente en atravesar la red para llegar al servidor de aplicaciones.
- El tiempo B es el tiempo que toma al servidor para procesar la solicitud del cliente y dar una respuesta.
- El tiempo C es el tiempo que toma a la respuesta del servidor en atravesar la red para llegar al cliente.

Como se muestra en la figura anterior, los *SwitchProbes* trabajan juntos para medir los tiempos de respuesta de los pares solicitud-respuesta, el uso de éstos agentes permite una mayor precisión en la medición de éstos tiempos.

Dispositivos Necesarios:

- 2 Conmutadores de la familia Catalyst (5000, 5500, 6500)
- SwitchProbe GE, WANProbe (con la opción ART MIB habilitada)
- Consola Central de Administración
- Demás recursos del laboratorio conectados a los conmutadores para la simulación de la carga.

Configuración previa.

Para obtener un análisis de tiempos de respuesta en la aplicación *TrafficDirector* es necesario tomar en cuenta, que el *switchprobe* debe poseer la capacidad de hacer este análisis; además, de que esta opción de software debe de igual manera estar habilitada dentro de la sonda. Inclusive, la definición de la aplicación que se va a sondear debe de tener habilitado la función ART (ver fig. 6.40).

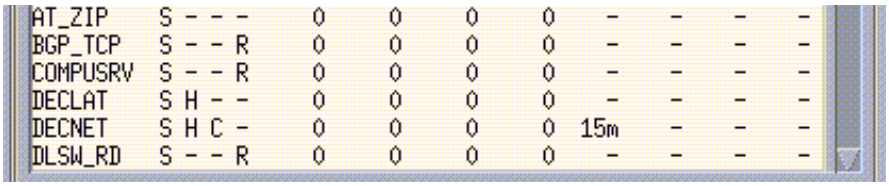


Figura 6.40 Dominios con función ART habilitada

La herramienta que se encarga de hacer esta función se encuentra en la ventana de análisis de aplicaciones, y se denomina *ART monitor*. Para que la función se despliegue correctamente, debe seleccionarse una de las aplicaciones en la caja de *domain name* y hacer click en el botón *ART monitor*.

Resultados.

Las figuras 6.41 y 6.42 exponen las mediciones que se llevaron a cabo utilizando el *SwitchProbe* para medir el tiempo de respuesta de las aplicaciones Telnet y FTP respectivamente.

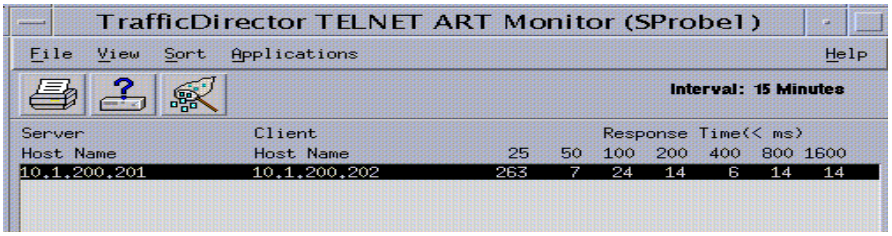


Figura 6.41 Resultado de la medición de tiempo de respuesta de aplicación telnet

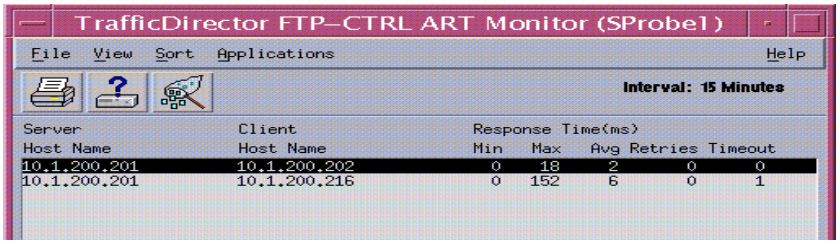


Figura 6.42 Resultado de la medición de tiempo de respuesta de aplicación FTP

Esta herramienta de medición permite conocer de manera acertada y rápida si los tiempos de respuesta en la red están dentro de los limites de desempeño razonables para los administradores y más importante, para los usuarios de la red. Inclusive, si los valores base de partida para juzgar la rapidez o lentitud de los tiempos de respuesta no se encuentran establecidos; esta herramienta permite hacerlo.

6.1.8 Escenarios de desarrollo en redes WAN.

6.1.8.1 Escenario #1. Administración y *Trobleshooting* de redes Frame Relay.

Introducción:

Muchas organizaciones están migrando de enlaces punto a punto a enlaces Frame Relay pues éstos son mas confiables y efectivos en costos. Así, cuando se administra un enlace WAN, un sonda inteligente colocada en el sitio corporativo, puede decodificar el paquete encapsulado y proveer datos de tiempo real e históricos acerca de los Circuitos Virtuales Permanentes (*Permanent Virtual Circuits* PVCs), *hosts* y protocolos más activos.

Para un administrador de redes, es importante tener la habilidad de "observar" el uso del DTE y DCE de un enlace Frame Relay y cada identificador de conexión individual de enlace de datos(*data link connection identifier DLCIs*) individual. Los *WANProbes* proveen ésta capacidad para reportar el tráfico en el troncal por DTE, DCE o DLCIs.

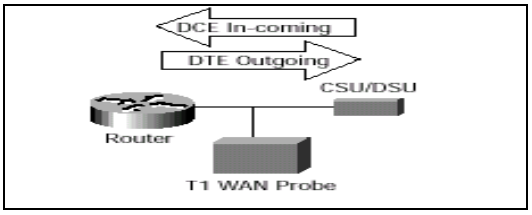


Figura 6.43 Conexión *WANProbe* para la administración y t*robleshooting* de redes Frame Relay

Objetivo:

El objetivo de éste escenario es el de utilizar el *WANProbe* para descubrir todos los DLCI's junto con los *Committed Information Rates CIR's* (tasa convenida de información) que se utilizan en una conexión FR. Esto se hará usando la información de administración y configuración colocada en la red por los dispositivos FRAD's (*Frame Relay Access Devices*), utilizando la opción *PVC discovery* en la sonda. De esta manera, se puede medir la utilización del enlace WAN y compararla con el CIR contratado y de esta manera asegurar la óptima utilización del enlace y reducir los costos del enlace.

Como objetivo secundario, está el de utilizar los reportes de administración en el enlace; *FECN (Forward Explicit Congestion Notification)*, *BECN (Bacward Explicit Congestion Notification),* y *DE tags (Discharge Elegible)* ; para así mantener un seguimiento de los posibles errores que se puedan dar en el enlace Frame Relay.

Dispositivos Necesarios:

- Enrutadores series (3600 o 7500)
- Multiport Ethernet WANProbe
- Consola Central de Administración
- Demás recursos del laboratorio

Configuración Previa.

Para este escenario, fue necesario la emulación de una red WAN, como la que se presenta en la figura siguiente. Refiérase a la sección de anexos para encontrar las configuraciones de los dispositivos involucrados. La sonda WAN se colocó entre los enlaces FR y HDLC. Cada interfaz conectada a la sonda se hizo a través de un *tap kit* ; y se configuró con la encapsulación y velocidad correspondiente.

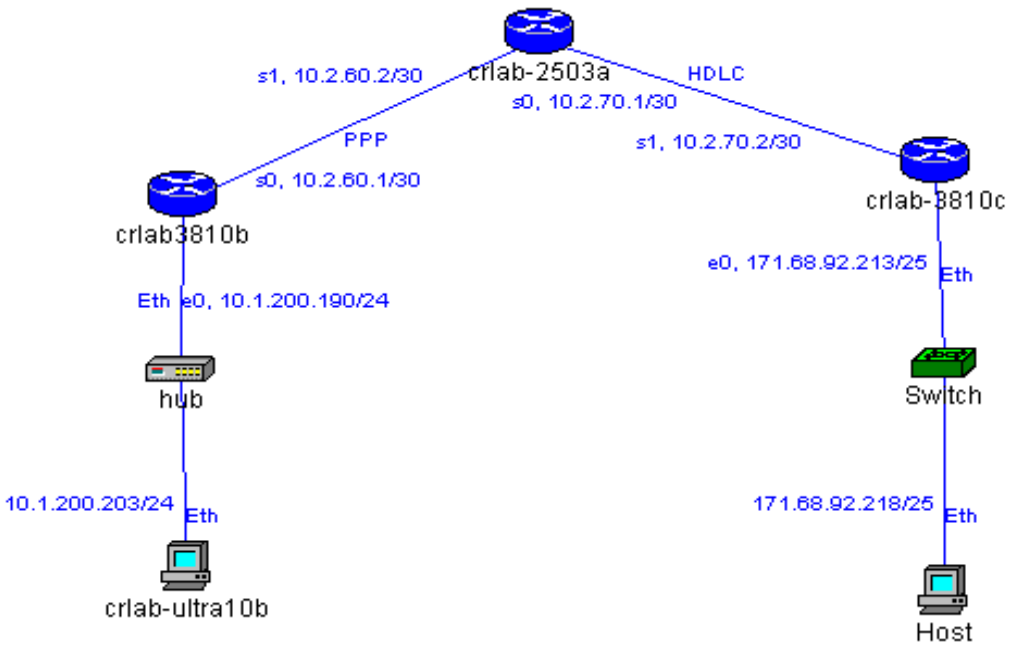


Figura 6.44 Diagrama de conexión para la emulación de la red WAN

El enlace FR se realizó de manera básica, y solamente definió el uso de DLCIs. Antes de empezar a observar todas las estadísticas en el enlace, se debe de definir la interfaz conectada como un agente (como se presenta en la fig. 6.44).

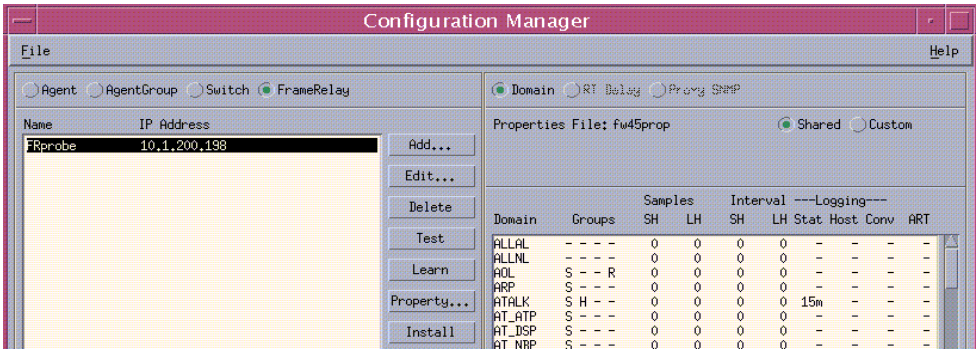


Figura 6.45 Definición del agente Frame Relay

Resultados.

De igual manera que como si fuera una conexión ethernet, es posible obtener datos estadísticos acerca del estado del enlace FR que esté administrando. Quizá la ventaja más importante que se tiene con la utilización de la definición de éste agente dedicado FR, es que las capacidades de análisis que éste presenta son sumamente atractivas. Las figuras 6.46 y 6.47 presentan algunas de las posibilidades que administración de desempeño del enlace FR. Como se puede observar, los datos se presentan por DTE y DCE (fig. 6.46) y es posible además, obtener información por DLCIs.

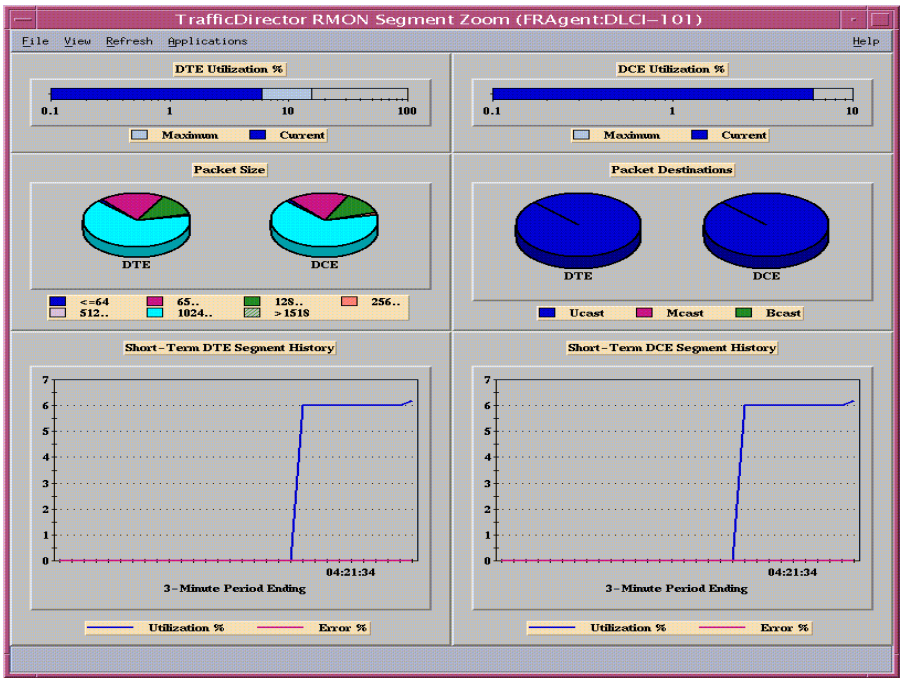
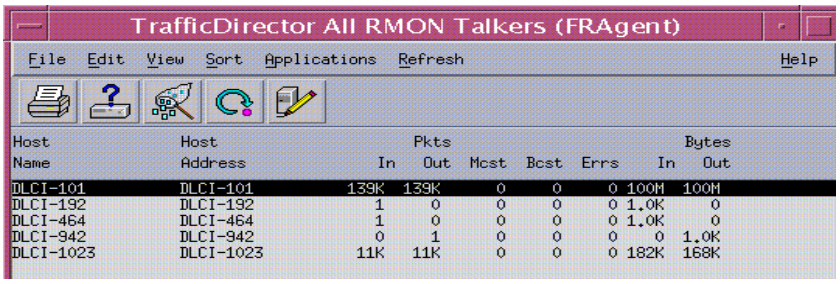


Figura 6.46 Estadísticas de enlace FR por DTE y DCE



Host Name	Host Address	Pkts In	Pkts Out	Mcst	Bcst	Errs	Bytes In	Bytes Out
DLCI-101	DLCI-101	139K	139K	0	0	0	100M	100M
DLCI-192	DLCI-192	1	0	0	0	0	1.0K	0
DLCI-464	DLCI-464	1	0	0	0	0	1.0K	0
DLCI-942	DLCI-942	0	1	0	0	0	0	1.0K
DLCI-1023	DLCI-1023	11K	11K	0	0	0	182K	168K

Figura 6.47 Información de enlace FR y las conversaciones por DLCI

De manera similar a como se ha hecho con los anteriores escenarios; la visibilidad de la red es aumentada, y es posible determinar los dispositivos mas activos y sus conversaciones(ver fig. 6.48). Mientras que utilizando la herramienta de tráfico *segment details* es posible obtener información acerca de los FECN, BECN y errores que pueden ocurrir en el enlace(ver fig. 6.49)

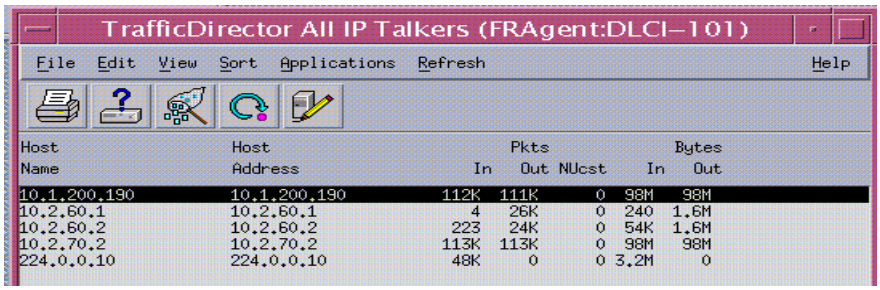


Figura 6.48 Estadísticas para las conversaciones de todos los dispositivos en el enlace

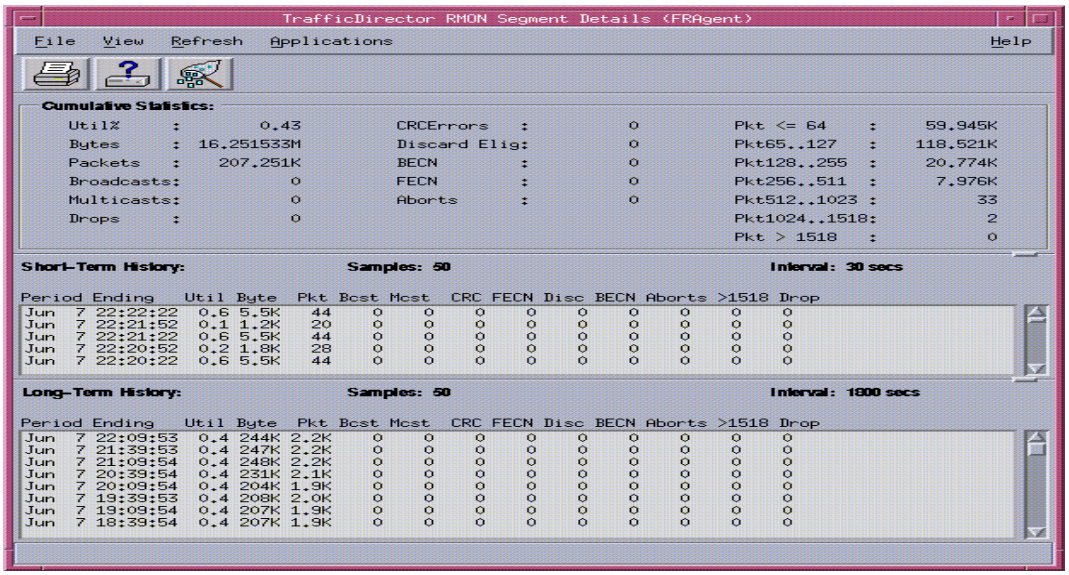


Figura 6.49 Información básica del enlace FR

Llevar el mantenimiento y administración de los enlaces WAN es de suma importancia para las empresas. Las posibilidades que esta herramienta brinda cobran suma importancia debido a que le permiten conocer en tiempo real el estado del enlace que utiliza para comunicarse con el resto de sus operaciones en el mundo; y evitar de manera proactiva problemas potenciales con el ancho de banda y planear la capacidad a largo plazo de su crecimiento. Los resultados anteriores comprueban la utilidad de la combinación *WANProbe/ TrafficDirector* para cumplir lo requerimientos de mantenimiento y administración de enlaces WAN.

6.1.8.2 Escenario #2. Administración de tráfico WEB o de Aplicaciones

Introducción:

La cantidad de tráfico web a través de la red crece enormemente día a día; este incremento, implica la necesidad de supervisión para la WAN hasta para satisfacer la necesidad de conocer qué aplicaciones web están corriendo en su red. Éste tipo de supervisión es logrado con los *WANProbes* RMON II

Objetivo:

Utilizar las capacidades del *WANProbe* para supervisión en la capa de aplicación y recoger estadísticas acerca de los *Top Talkers, Top Conversations;* y supervisión de puertos TCP y UDP

Dispositivos Necesarios:

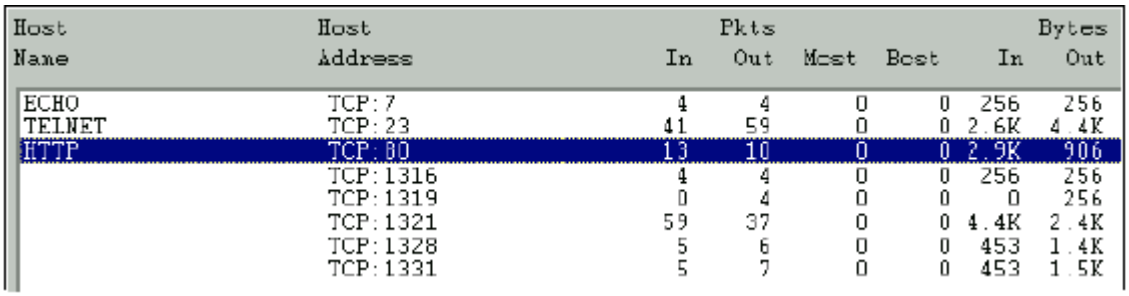
- Enrutadores de las familias (3600 o 7500)
- Multiport Ethernet WANProbe
- Consola Central de Administración
- Demás recursos del laboratorio

Configuración previa.

De la misma manera en que se realizó el escenario de sondeo de aplicaciones en ambientes LAN, este escenario utilizó una de las estaciones SUN como servidor web. Este escenario no tiene aspectos de configuración adicionales a los ya tratados a lo largo de la descripción de la mayoría de las pruebas realizadas hasta el momento.

Resultados.

Quizá el resultado más importante es el de demostrar que la sonda WANProbe es capaz de: sondear los dispositivos mas activos en la red; brindar información acerca de las aplicaciones más activas y descubrir de manera automática todos los puertos TCP y UDP en uso por cualquier enlace. La siguiente figura muestra un ejemplo de lo que es este análisis de tráfico por puerto.



Host Name	Host Address	Pkts In	Pkts Out	Pkts Most	Pkts Best	Bytes In	Bytes Out
ECHO	TCP:7	4	4	0	0	256	256
TELNET	TCP:23	41	59	0	0	2.6K	4.4K
HTTP	TCP:80	13	10	0	0	2.9K	906
	TCP:1316	4	4	0	0	256	256
	TCP:1319	0	4	0	0	0	256
	TCP:1321	59	37	0	0	4.4K	2.4K
	TCP:1328	5	6	0	0	453	1.4K
	TCP:1331	5	7	0	0	453	1.5K

Figura 6.50 Análisis de tráfico por puerto

La utilidad más importante que esta herramienta presenta es que permite organizar políticas para el uso del tráfico web y sustentarlas con estadísticas en tiempo real e históricas.

6.1.8.3 Escenario #3. Supervisión de Recursos Remotos

Introducción:

Este escenario es igual al utilizado para la alerta y notificación de eventos en redes LAN. Pero en este caso, es de una importancia mucho mayor debido a la importancia del ancho de banda en los enlaces WAN. De acuerdo a esta necesidad, la estrategia de administración no permite tener una estación administradora haciendo *ping* a dispositivos críticos para comprobar la disponibilidad de los mismos, sus tiempos de respuesta o bien consultar las variables MIB tales como el uso del CPU. Esto implicaría un costo enorme especialmente, si esos dispositivo están en lugares remotos accesibles por enlaces de ancho de banda muy bajo.

Objetivo:

Demostrar la utilidad del *WANProbe* como dispositivo de supervisión para localidades remotas y cómo, si éste fuera colocado cerca del dispositivo remoto que va a ser sondeado, podría realizar *pings* para comprobar la disponibilidad y el *round-trip delay* del dispositivo. De igual manera, demostrar como éste se encargaría de sondear el dispositivo por las variables MIB estipuladas y sus los valores umbrales, para que un evento de alarma se desencadene cada vez que el limite umbral sea alcanzado.

Así, todo el tráfico que se utilizaba para ésta misma función sin el WANProbe se reduce a un paquete *Trap SNMP* a través de lo que podría ser un enlace de bajo ancho de banda y de alto costo.

Dispositivos Necesarios:

- Multiport Ethernet WANProbe.
- Enrutadores (3810, 2600)
- Consola Central de Administración

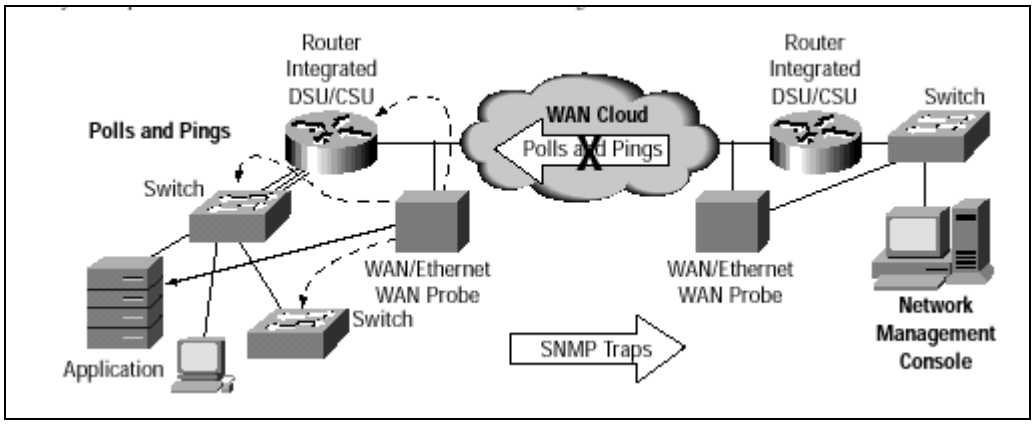


Figura 6.51 Diagrama del escenario para el administración de recursos remotos

Configuración previa

Este escenario no es más que la aplicación del escenario de alertas y notificación de eventos que se realizó en ambientes LAN. Todos los pasos para configurar el *TrafficDirector* se aplican aquí también. Sin embargo, para este escenario, se definieron *traps*, que permitieron conocer el estado de las variable MIB sobre los dispositivos remotos que se supervisaron.

La idea central; como se dijo en el escenario de redes LAN, es conocer qué es lo que se quiere supervisar en el dispositivo remoto, y por supuesto, cómo definir esta variable en la aplicación *TrafficDirector*.

La configuración de la propiedades personalizadas y la definición del dispositivo y la variable MIB a supervisar se realiza de la misma manera en que se configuró en el escenario para redes LAN.

La definición del *trap* es lo que se tratará a continuación. La siguiente figura muestra la ventana del editor de propiedades donde se muestran las variable MIB que se supervisaron; y la definición del *trap* para los resultados del sondeo de la variable *locIfLineProt*.

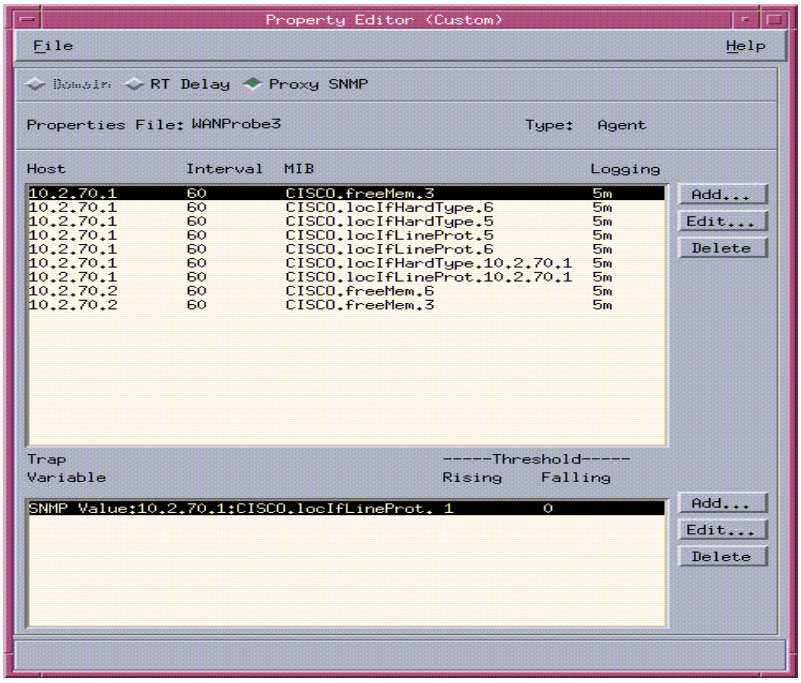


Figura 6.52 Ventana para definición de sondeo proxy SNMP

La definición del *trap* se realiza seleccionando el MIB que se supervisará, y haciendo click en el botón de agregar (add). La figura 6.53 muestra la ventana donde se especifican los valores umbrales que desencadenaran el *trap* en caso de ser alcanzados. La definición del *trap* no es diferente de la que se configuró en el escenario LAN, por lo tanto se omitirán los pasos para lograrlo. Tome en cuenta que al seleccionar la variable MIB para la que va a sondear, y luego agregar un *trap* para la misma, la mayoría de los campos en la definición del *trap* se generan automáticamente; por lo que los únicos campos a rellenar son los umbrales y el tipo de “disparador” que desencadenará la alarma.

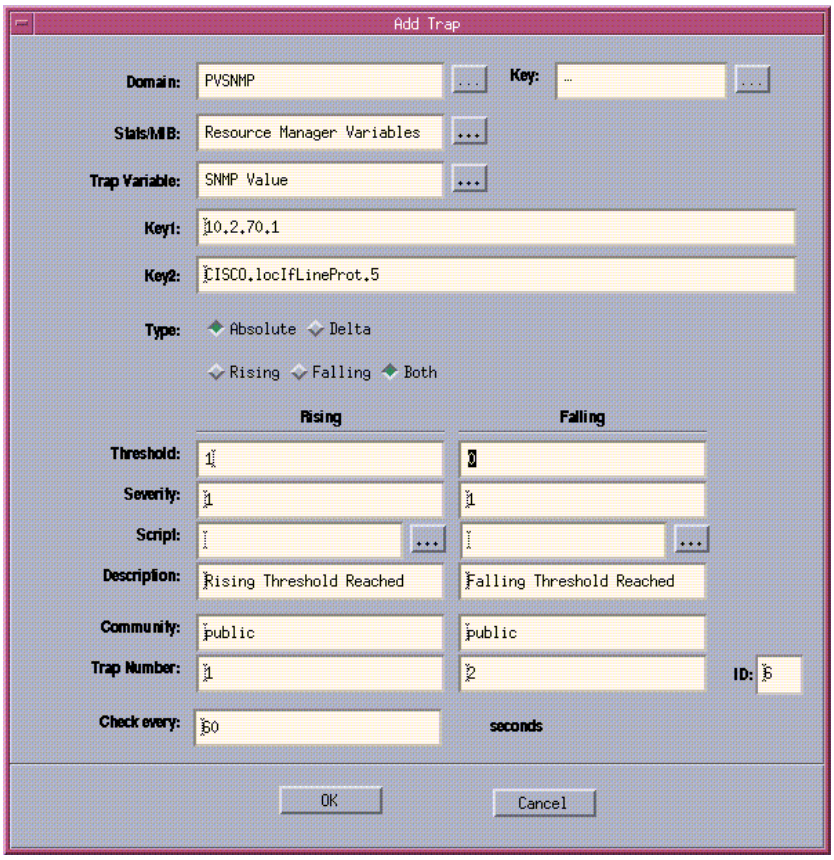


Figura 6.53 Definición de variables a supervisar en sondeo proxy SNMP

Resultados.

Los resultados obtenidos para esta prueba concuerdan totalmente con los obtenidos en las pruebas de ambientes LAN. Las mediciones del tiempo *round trip delay* se muestran en la siguiente figura. Mientras que los obtenidos en la aplicación del sondeo *proxy* SNMP en la figura 6.54

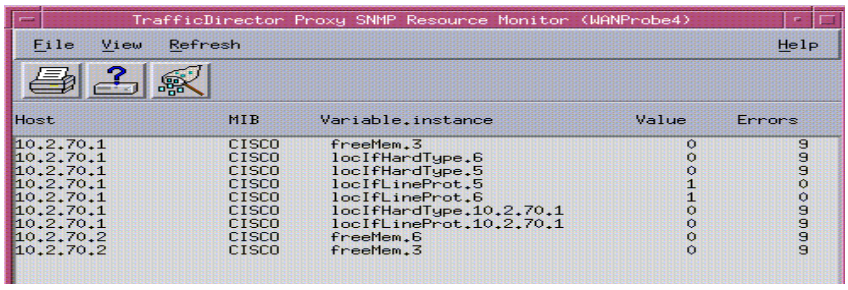


Figura 6.54 Resultado del sondeo proxy SNMP

La siguiente figura muestra el resultado obtenido para el *trap* definido en el escenario; es importante notar que la variable *locIfLineProt* permite conocer el estado de una interfaz en un dispositivo Cisco. Esta variable retorna un 1 si la interfaz está arriba, y un 0 si la interfaz está abajo. Por supuesto, la interfaz estaba abajo desde un principio; así que el resultado del *trap*, indica que la interfaz subió en determinado momento en el experimento.

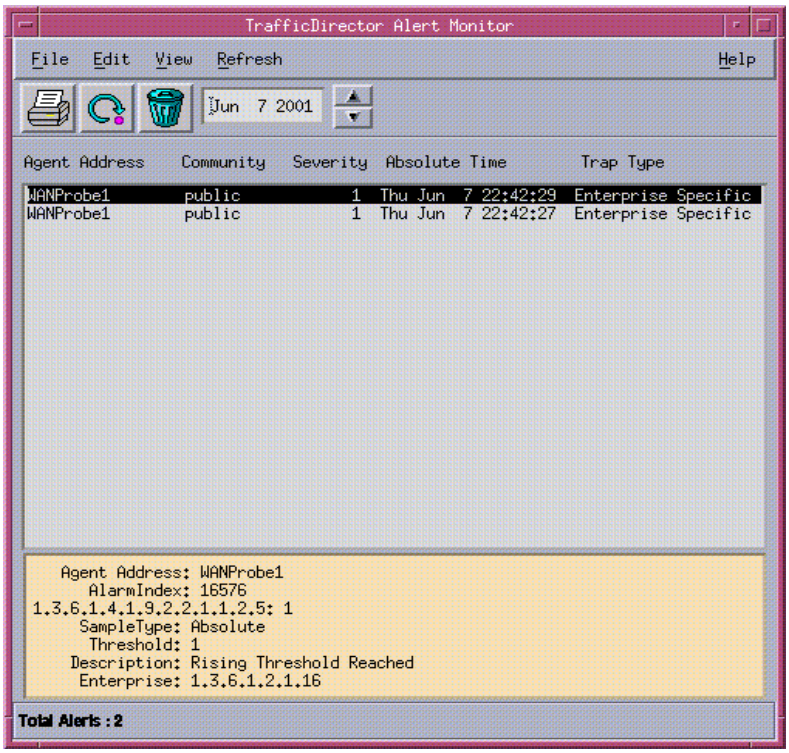


Figura 6.55 Resultado del sondeo de la variable locIfLineProt

El resultado de la prueba de medición del tiempo de retraso de ida y vuelta, se muestra en la figura 6.56

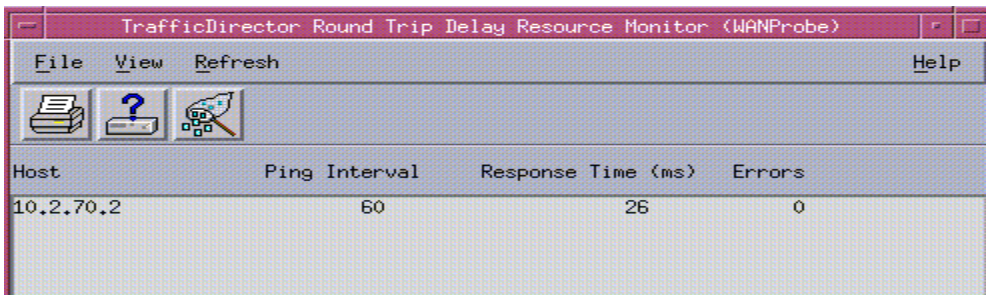


Figura 6.56 Resultado del sondeo *round trip delay*

De igual manera de como se explicó en los escenarios LAN, éstas herramientas permiten una administración proactiva de los dispositivos en cualquier tipo de ambiente. Sin embargo, para ambientes WAN cobran especial importancia debido a lo costosos que son los enlaces; y esta herramienta en conjunto con la sonda, permite reducir el tráfico de administración por un *trap* cuando ocurra algún problema.

6.1.8.4 Escenario #4. Administración de cuentas. (Billing and Accounting)

Introducción:

Todas las organizaciones reconocen que la óptima utilización de los recursos del al inversión realizada en su red es imperativa. Los enlaces WAN (enlaces alquilados o circuitos FR), a diferencia de los LAN son gastos recurrentes y además de alto costo. Así, una de las responsabilidades de los administradores de la red es la de supervisar y en lo posible reducir los costos operativos de la WAN; además de obtener la información necesaria para verificar y garantizar la calidad de servicio QoS (Quality of Service) por la que es cobrado por el proveedor de servicio. De igual manera, el proveedor de servicio también necesita de recolectores de información para generar reportes de cuenta acertados en base al uso de sus servicios.

Objetivo:

De manera similar al desarrollo del escenario anterior, se pretende demostrar la manera en que al colocar una sonda *WANProbe* al final de la red, el administrador de la red puede obtener la información necesaria acerca de la utilización de circuitos lógicos y físicos. Y cómo esta información puede ser convertida por el software de administración CW2000 (*TrafficDirector* específicamente) en un reporte de cuenta del uso del enlace.

Dispositivos Necesarios:

- Multiport Ethernet WANProbe.
- Enrutadores (3810, 2600)
- Consola Central de Administración

Configuración previa.

Antes de generar algún reporte especifico con la herramienta *TrendReporter*, es necesario que las bitácoras (*logging*) estadísticas estén inicializadas en los dominios que se pretende usar para generar el reporte. Esto se hace directamente en la opción del editor de propiedades; se elige el dominio que se quiere editar, luego el botón editar y se habilita el *logging* para las estadísticas, historiales, eventos y sondeo ART.

La siguiente figura muestra la forma en que se presenta el editor de propiedades si el *logging* está habilitado en un dominio.

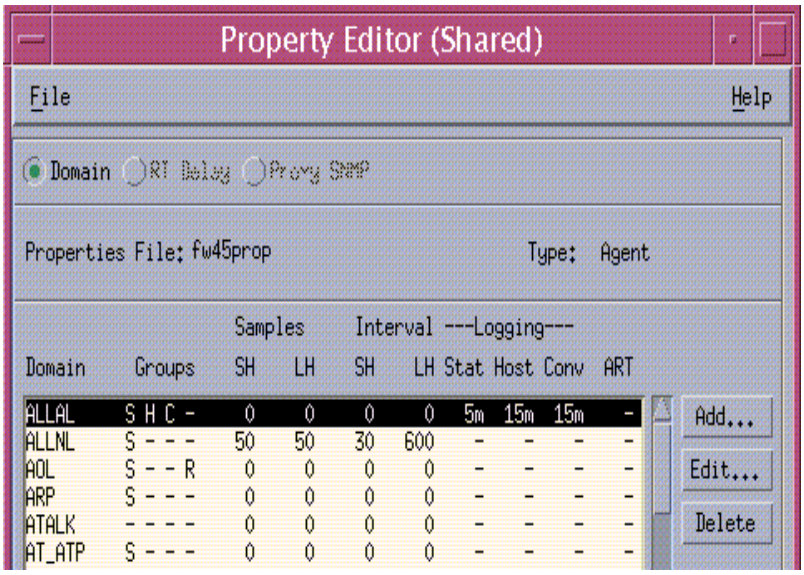


Figura 6.57 Presentación de los intervalos de *logging* en el editor de propiedades

La herramienta *Trend Reporter* se presenta en la siguiente figura; es simple de utilizar; y los parámetros que se requieren son: escoger el agente, el dominio y el lapso de tiempo en que se realizará el análisis.

NOTA: Tome en cuenta que si se estipula un análisis de un tiempo mayor al que la base de datos tiene registrado, el analizador no trabajará correctamente, para solucionarlo, escoja una cantidad de tiempo menor, donde esté seguro que la base de datos posee información y estadísticas.

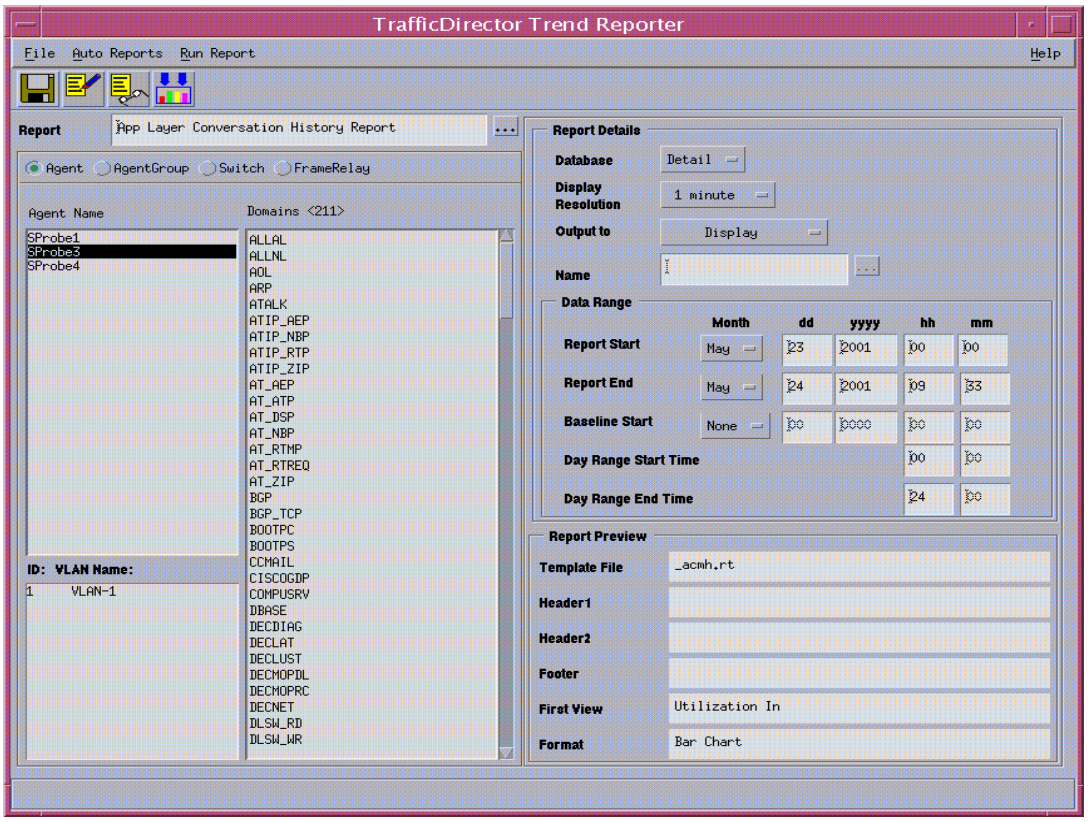


Figura 6.58 Ventana del TrendReporter

Resultados.

La recolección de datos, ya sean de tráfico, protocolo o aplicaciones; no sirve solamente para el análisis de tendencias sobre el comportamiento de una red; sino que además, permite reconocer la calidad de servicio que se está obteniendo del proveedor. Y aun más importante, se puede analizar los costos que estos servicios implican.

Las siguientes capturas de reportes presentan un breve ejemplo de la manera en que estos reportes podrían servir para la administración de costos y cuentas de enlaces alquilados a algún proveedor de servicio.

```
Billing Summary Report - Sorted by: Octets In and Out (All Hosts)
Agent: FRAgent, Domain: IP
From: Thu May 31, 2001 09:00,   To: Thu May 31, 2001 16:00,   Summary

Host                                | Octets| Octets|   Cost|   Cost
                                    |    Out|     In|    Out|     In
=============================================================================
10.2.70.2                           |   26M |   26M |  0.26 |  0.26
10.1.200.190                        |   26M |   26M |  0.26 |  0.26
224.0.0.10                          |     0 |  822K |  0.00 |  0.01
10.2.60.2                           |  424K |   13K |  0.00 |  0.00
10.2.60.1                           |  431K |     0 |  0.00 |  0.00
=============================================================================
Sub Total:                          |   54M |   54M |  0.54 |  0.54
Total:                              |       107M |       1.07
=============================================================================


Octets  Out    : Octets Out             Octets  In     : Octets In
Cost    Out    : Cost Out               Cost    In     : Cost In

Billing Rate = 0.010000 (per MBytes)


Billing Summary Report - Sorted by: Octets In and Out (All Hosts)
Agent: WANProbe1, Domain: FTP-DATA
From: Mon Apr 30, 2001 00:00,   To: Thu May 24, 2001 00:00,   Summary

Host                                | Octets| Octets|   Cost|   Cost
                                    |    Out|     In|    Out|     In
=============================================================================
10.1.200.201                        |  643M |  1.6B |  6.43 | 15.65
10.1.200.202                        |  899M |  232M |  8.99 |  2.32
10.1.200.226                        |  596M |  321M |  5.96 |  3.21
crlab-ultra10a                      |   20M |   26M |  0.20 |  0.26
10.1.200.200                        |   23M |   13M |  0.23 |  0.13
10.1.200.190                        |   10M |     0 |  0.10 |  0.00
10.1.1.16                           |  5.5M |     0 |  0.05 |  0.00
10.1.100.31                         |     0 |  3.8M |  0.00 |  0.04
10.1.200.199                        |  645K |  1.9M |  0.01 |  0.02
10.10.20.22                         |     0 |  1.7M |  0.00 |  0.02
10.1.200.255                        |     0 |  1.0M |  0.00 |  0.01
=============================================================================
Sub Total:                          |  2.2B |  2.2B | 21.98 | 21.64
Total:                              |       4.3B |       43.62
=============================================================================

Octets  Out    : Octets Out             Octets  In     : Octets In
Cost    Out    : Cost Out               Cost    In     : Cost In

Billing Rate = 0.010000 (per MBytes)
```

La siguiente figura muestra otro tipo de reporte que es posible generar, éste es de tipo gráfico y muestra el uso del enlace FR a través de un período de siete horas en un día común.

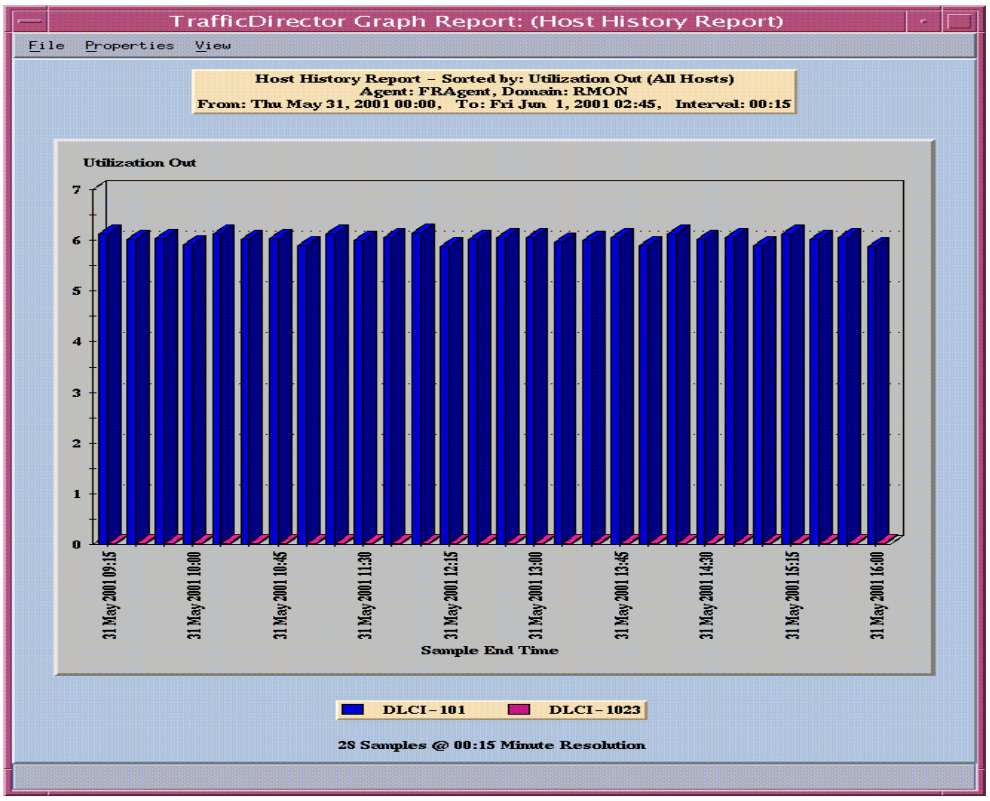


Figura 6.59 Resultado gráfico del análisis de utilización del enlace FR

Como se mencionó anteriormente, los enlaces WAN son gastos recurrentes y de alto costo. Los reportes generados por esta herramienta, ofrecen una gran ayuda a los administradores de la red cuya responsabilidades es la de supervisar y en lo posible reducir los costos operativos de la red WAN; y la posibilidad de verificar y garantizar la calidad de servicio QoS (*Quality of Service*) que es cobrado por el proveedor de servicio. Pero, el sistema también funciona de la manera inversa; pues el proveedor de servicio también necesita de recolectores de información para generar reportes de cuenta acertados en base al uso de sus servicios.

6.1.9 Funciones básicas de administración utilizando CiscoWorks2000

En este apartado, se discutirán algunas de las tareas básicas para la administración de una red que son posibles gracias a las múltiples funciones que tiene el software Ciscoworks2000. Estas funciones estarán enfocadas en las restantes áreas del modelo ISO para la administración de redes; a saber, administración de configuración, cambios, fallas y seguridad.

El sistema de trabajo utilizando CiscoWorks2000 se basa inicialmente en la selección del módulo que desea utilizar en la barra del lado izquierdo del *browser*; luego, se navega entre las funciones (algunas organizadas dentro de carpetas) y se selecciona la que sea necesaria. Esta correrá, ya sea en una ventana de *browser* adicional, o en la ventana principal. Debe notar, que en una gran mayoría de los casos, se deben escoger los dispositivos que se desean administrar antes de que la aplicación haga su trabajo. La figura 6.60 muestra la ventana de selección de dispositivos.

6.1.9.1 Administración centralizada de funciones de configuración, cambios y fallas.

La mayoría de estas áreas mencionadas están cubiertas por el *Resource Manager Essentials*. Éste modulo se puede ver como si fuera "una gran base de datos " donde se registran todos los sucesos relativos a la red ya sea ésta LAN o WAN.

Como se sabe, en el capítulo 5 en la descripción del software del sistema; esta aplicación es la que se encarga de llevar el control de los cambios que se den en las configuraciones de los dispositivos, programar las actualizaciones de software de los mismos, conocer sus características más importantes etc.

Todas estas funciones se encuentran en versiones separadas en la barra de navegación del módulo RME. Sin embargo, existe una que le permite tener completo dominio de gran parte de ellas; y además es la herramienta ideal para tener una administración centralizada

A continuación se describe la manera de administrar todos estos tópicos bajo una misma herramienta.

Inicialmente, debe de colocarse en la barra de navegación del modulo RME como muestra la siguiente figura.

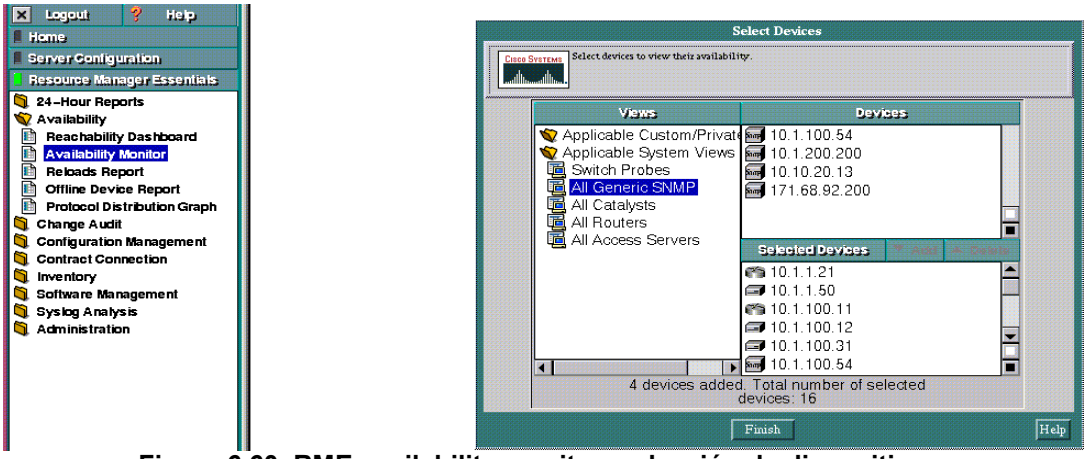


Figura 6.60 RME availability monitor; selección de dispositivos.

Desde esta aplicación es posible escoger los dispositivos con los que desea trabajar; éstos se encuentran categorizados por su función. Una vez seleccionados, proceda a agregarlos para su análisis y avance a la siguiente ventana.

La aplicación se encargará de encuestar a todos los dispositivos por su disponibilidad; y le presentará un resumen del análisis de los mismos (ver figura 6.61).

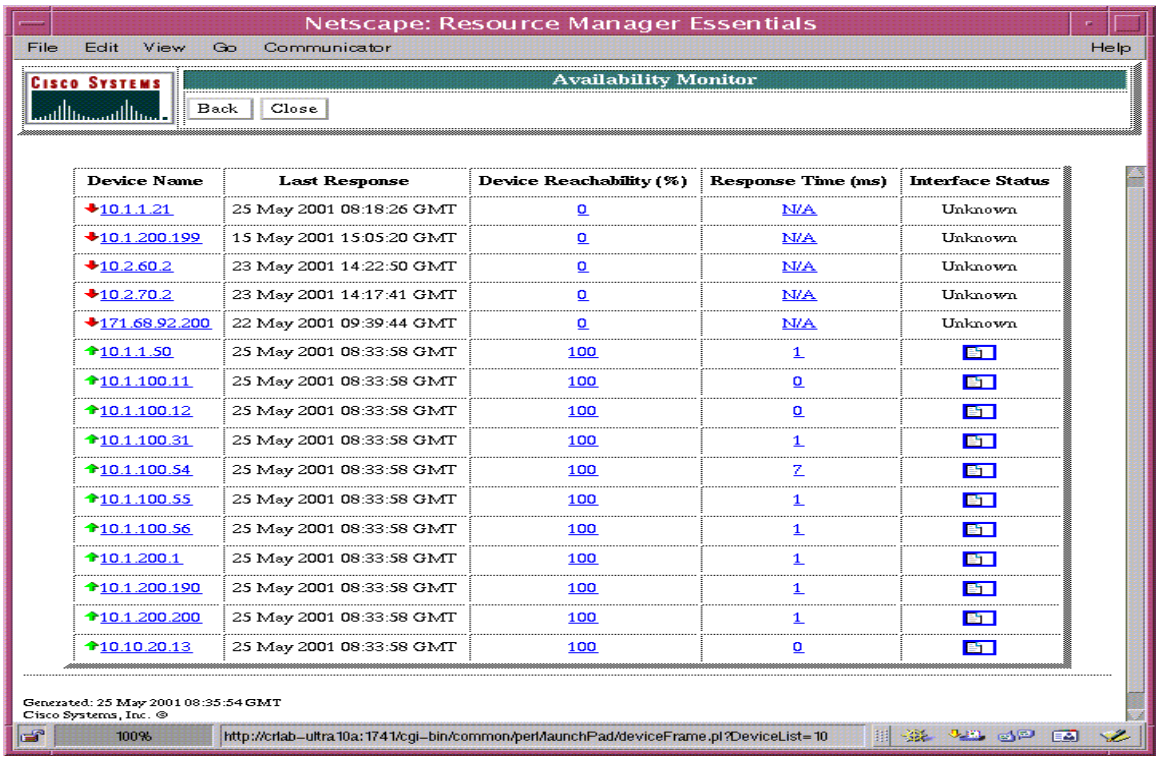


Figura 6.61 Ventana de resultados RME availability monitor

Desde esta ventana, y con solo hacer click en el dispositivo que necesite administrar, estará llamando a la aplicación *Device Center* (ver figura 6.62); donde podrá llevar a cabo labores de administración del dispositivo; además de crear reportes acerca de la configuración, tendencia de utilización de protocolos etc. La figura 6.62 muestra el gráfico de la disponibilidad del dispositivo en las últimas horas.

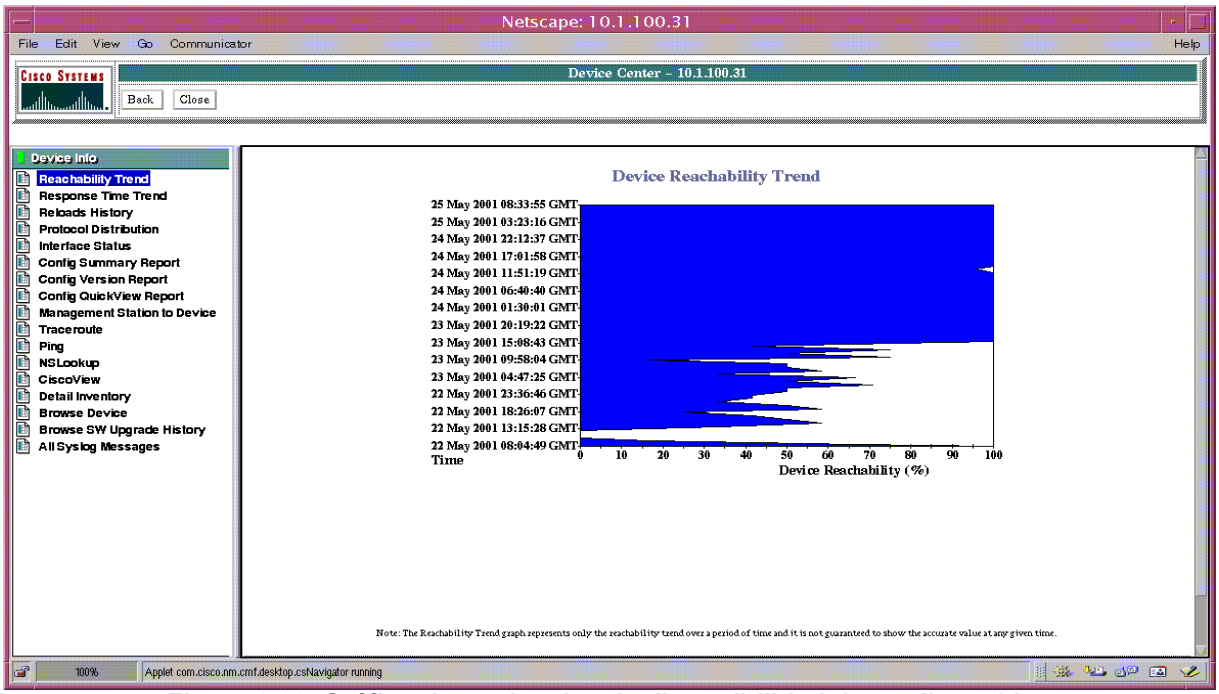


Figura 6.62 Gráfico de tendencias de disponibilidad de un dispositivo

La administración de la configuración de los dispositivos es muy importante; desde la aplicación del *device center*, el administrador de la red puede solicitar un resumen de los cambios en las configuraciones que este dispositivo ha recibido. La figura 6.63 muestra el resultado de esta solicitud.

Ahora; si se está interesado en ver exactamente que cambios específicos fueron realizados en la última actualización de la configuración; simplemente escoja la configuración que desee ver, y se le desplegará un reporte de comparación entre la configuración actual y la que escogió. Éste reporte le muestra en una interfaz gráfica las diferencias entre ambas configuraciones. Esta herramienta es de gran utilidad para enfrentar posibles situaciones de crisis ante una eventual caída de la red. Ver figura 6.64

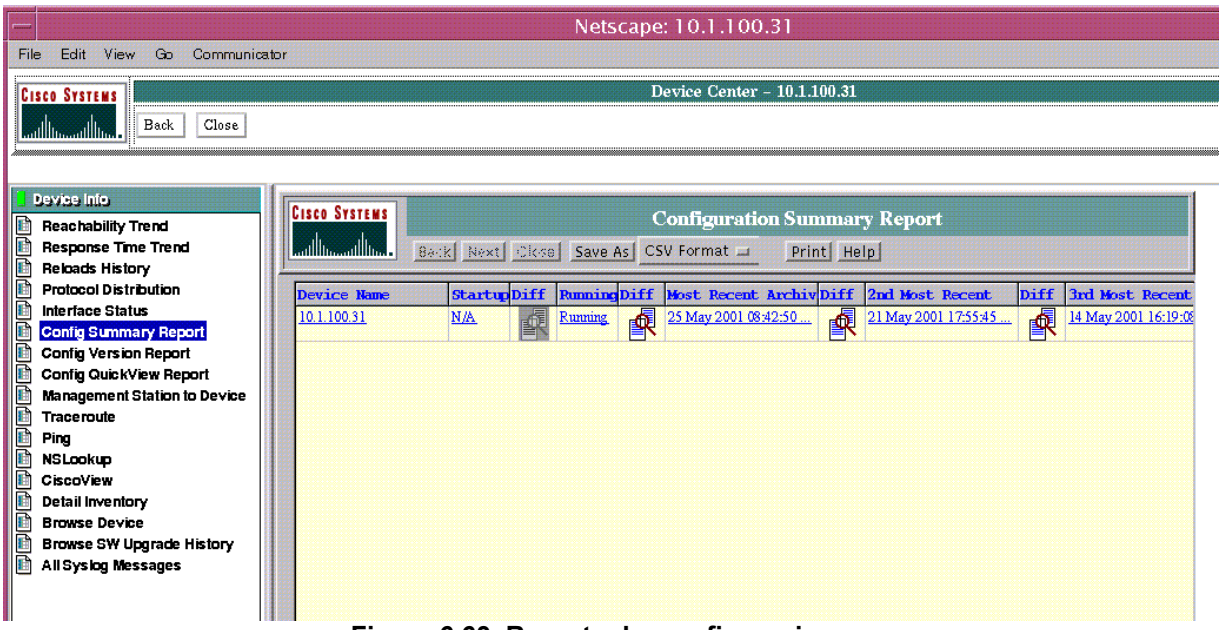


Figura 6.63 Reporte de configuraciones.

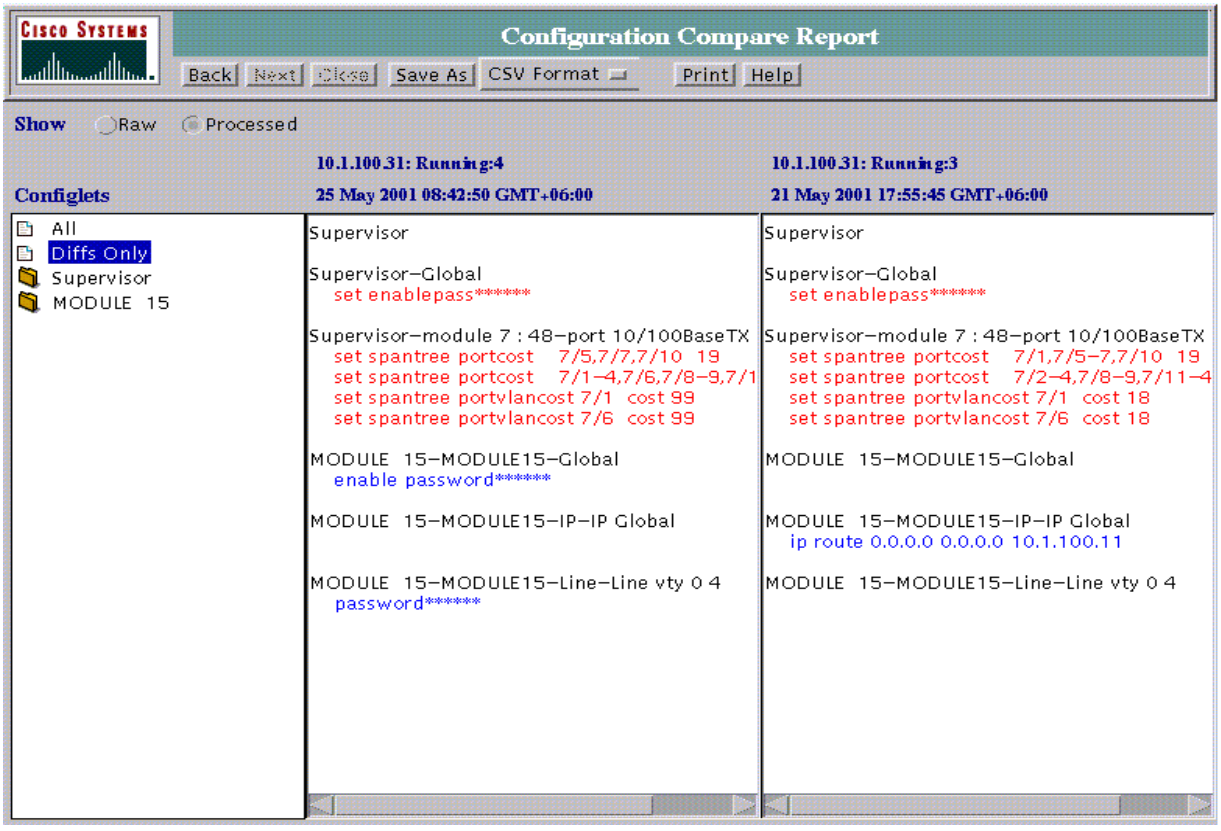


Figura 6.64 RME reporte de comparación de configuraciones

Otra de las funciones de administración que es posible realizar desde estas aplicaciones; es la de obtener un inventario detallado del dispositivo; tal que, se puede obtener información acerca de la imagen de software que posee, el número de *slots* disponibles y utilizados, también la cantidad de memoria que el dispositivo posee; inclusive, el numero de serie de los módulos que tiene(ver figura 6.65)

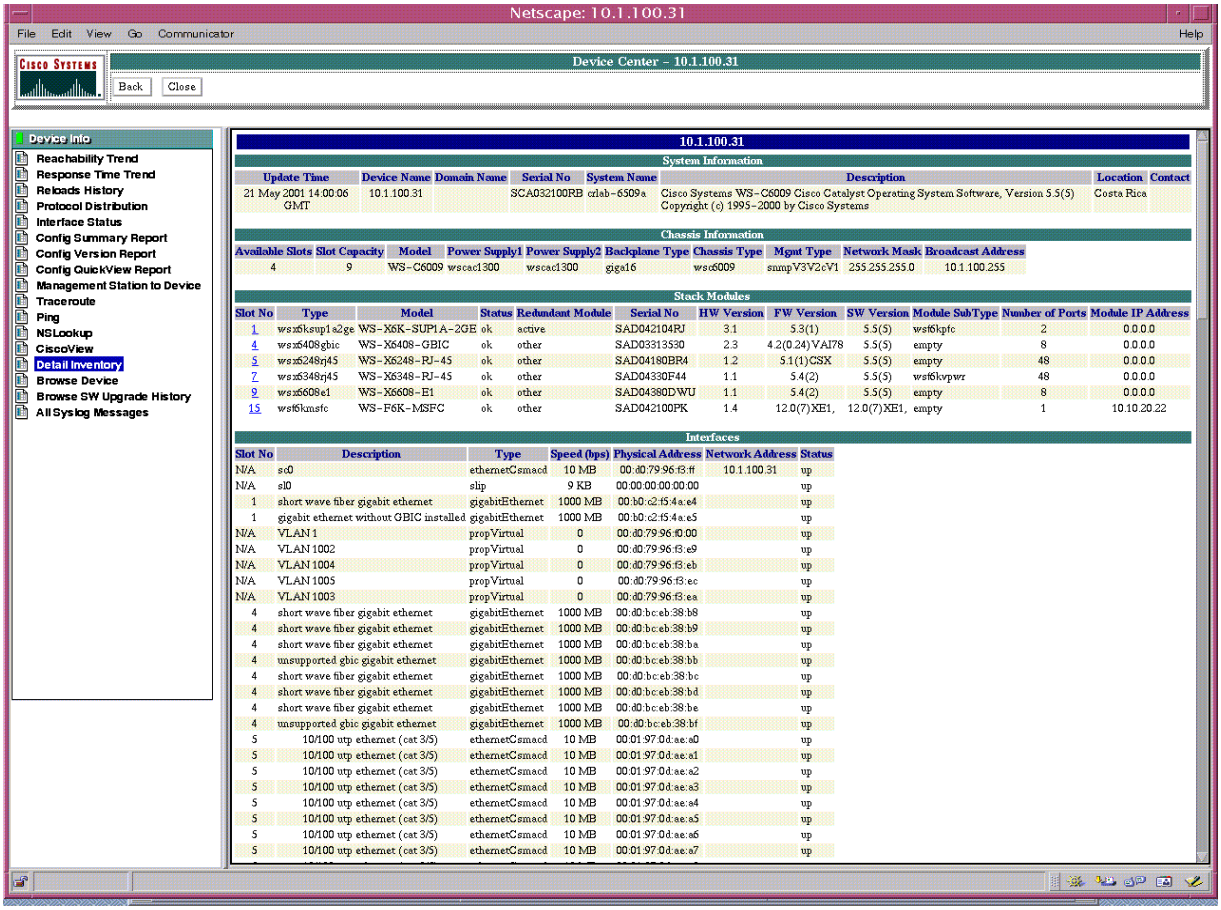
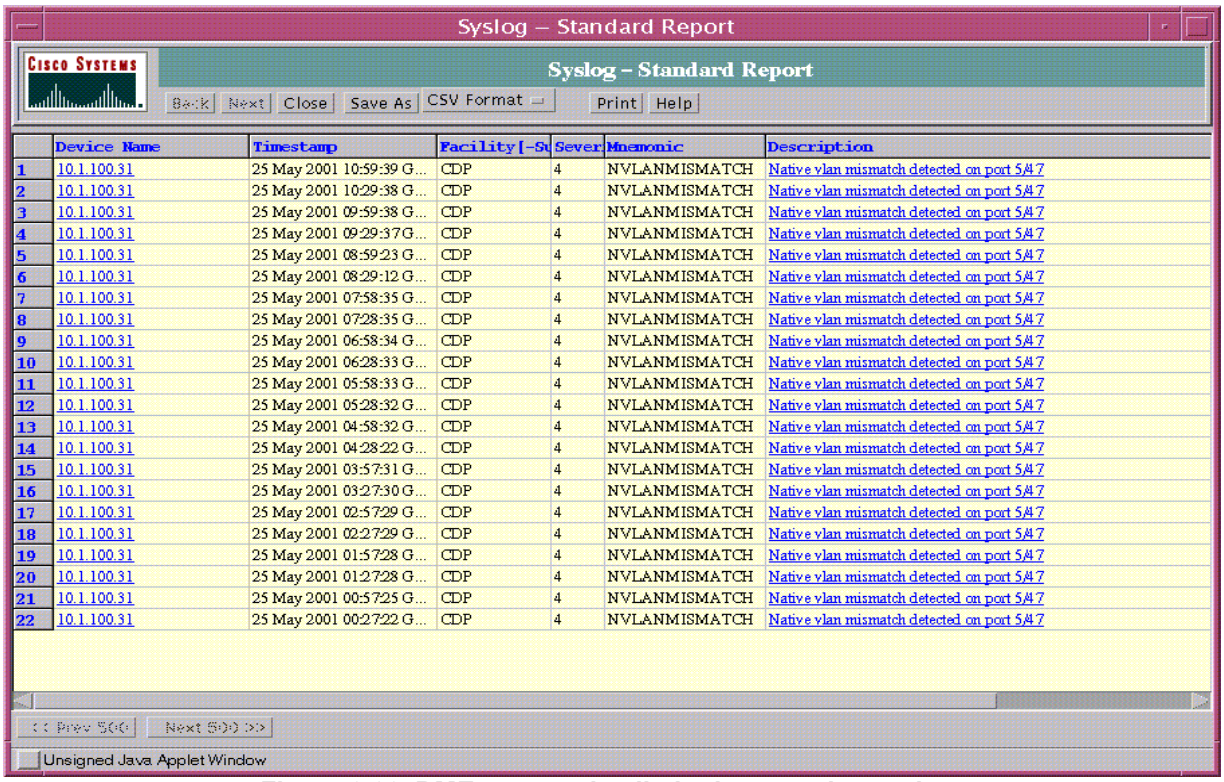


Figura 6.65 RME reporte detallado de inventario

La parte del área de administración de faltas, se encuentra representada aquí por la aplicación visualizadora de los mensajes *syslog*. Ésta se encarga de mostrar los mensajes que el dispositivo le envía a la consola central de administración; informándole de su estado, y posibles problemas lógicos o de configuración. Ver figura 6.66.



	Device Name	Timestamp	Facility[-Su	Sever	Mnemonic	Description
1	10.1.100.31	25 May 2001 10:59:39 G...	CDP	4	NVLANMISMATCH	Native vlan mismatch detected on port 5/47
2	10.1.100.31	25 May 2001 10:29:38 G...	CDP	4	NVLANMISMATCH	Native vlan mismatch detected on port 5/47
3	10.1.100.31	25 May 2001 09:59:38 G...	CDP	4	NVLANMISMATCH	Native vlan mismatch detected on port 5/47
4	10.1.100.31	25 May 2001 09:29:37 G...	CDP	4	NVLANMISMATCH	Native vlan mismatch detected on port 5/47
5	10.1.100.31	25 May 2001 08:59:23 G...	CDP	4	NVLANMISMATCH	Native vlan mismatch detected on port 5/47
6	10.1.100.31	25 May 2001 08:29:12 G...	CDP	4	NVLANMISMATCH	Native vlan mismatch detected on port 5/47
7	10.1.100.31	25 May 2001 07:58:35 G...	CDP	4	NVLANMISMATCH	Native vlan mismatch detected on port 5/47
8	10.1.100.31	25 May 2001 07:28:35 G...	CDP	4	NVLANMISMATCH	Native vlan mismatch detected on port 5/47
9	10.1.100.31	25 May 2001 06:58:34 G...	CDP	4	NVLANMISMATCH	Native vlan mismatch detected on port 5/47
10	10.1.100.31	25 May 2001 06:28:33 G...	CDP	4	NVLANMISMATCH	Native vlan mismatch detected on port 5/47
11	10.1.100.31	25 May 2001 05:58:33 G...	CDP	4	NVLANMISMATCH	Native vlan mismatch detected on port 5/47
12	10.1.100.31	25 May 2001 05:28:32 G...	CDP	4	NVLANMISMATCH	Native vlan mismatch detected on port 5/47
13	10.1.100.31	25 May 2001 04:58:32 G...	CDP	4	NVLANMISMATCH	Native vlan mismatch detected on port 5/47
14	10.1.100.31	25 May 2001 04:28:22 G...	CDP	4	NVLANMISMATCH	Native vlan mismatch detected on port 5/47
15	10.1.100.31	25 May 2001 03:57:31 G...	CDP	4	NVLANMISMATCH	Native vlan mismatch detected on port 5/47
16	10.1.100.31	25 May 2001 03:27:30 G...	CDP	4	NVLANMISMATCH	Native vlan mismatch detected on port 5/47
17	10.1.100.31	25 May 2001 02:57:29 G...	CDP	4	NVLANMISMATCH	Native vlan mismatch detected on port 5/47
18	10.1.100.31	25 May 2001 02:27:29 G...	CDP	4	NVLANMISMATCH	Native vlan mismatch detected on port 5/47
19	10.1.100.31	25 May 2001 01:57:28 G...	CDP	4	NVLANMISMATCH	Native vlan mismatch detected on port 5/47
20	10.1.100.31	25 May 2001 01:27:28 G...	CDP	4	NVLANMISMATCH	Native vlan mismatch detected on port 5/47
21	10.1.100.31	25 May 2001 00:57:25 G...	CDP	4	NVLANMISMATCH	Native vlan mismatch detected on port 5/47
22	10.1.100.31	25 May 2001 00:27:22 G...	CDP	4	NVLANMISMATCH	Native vlan mismatch detected on port 5/47

Figura 6.66 RME reporte detallado de mensajes syslog.

6.1.9.2 Administración de funciones de configuración especializadas.

Las funciones de los módulos que conforman el sistema CiscoWorks2000 son muy variadas; y en algunos casos redundantes; pero debe tomar esto como una manera de hacer las cosas de distintas formas. Éste es el caso de funciones como el mantenimiento y configuración de VLANs;

Existen diversas maneras de hacer la configuración de VLANs en un conmutador; sin embargo, las aplicaciones Campus Manager y Cisco View permiten hacerlo, y de manera gráfica. Ambas lo realizan desde un enfoque diferente; pues el CiscoView no es mas que una herramienta gráfica para la configuración de dispositivos de red, que hace esta tarea más simple y rápida. Mientras tanto, el enfoque que presenta la aplicación Campus Manager, es mucho más especializado; pues ésta es una de las funciones por la que fue concebido.

La figura 6.65 muestra la manera en que el mantenimiento y creación de VLANs es realizada en la aplicación CM. Ésta función se encuentra dentro de las que realiza la aplicación *topology services* en el CM.

El proceso de creación inicial se muestra en la figura 6.67, inicialmente, es necesario escoger un *VTP domain* en el cual se va a crear la VLAN; luego escoger en el menú de herramientas la creación de una nueva VLAN (ethernet en este caso; ver figura 6.67a); para después rellenar los campos necesarios en la ventana de definición VLANs (fig. 6.67b). **NOTA:** no es necesario entrar un numero *VLAN index* ; pues la aplicación asigna uno automáticamente.

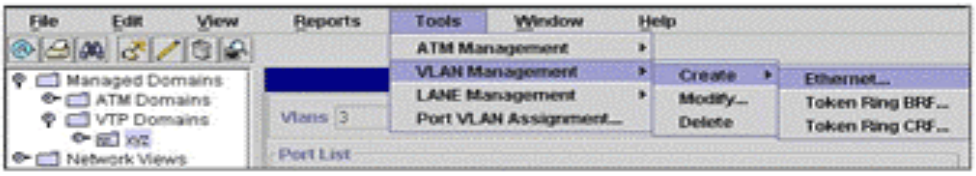


Fig. A

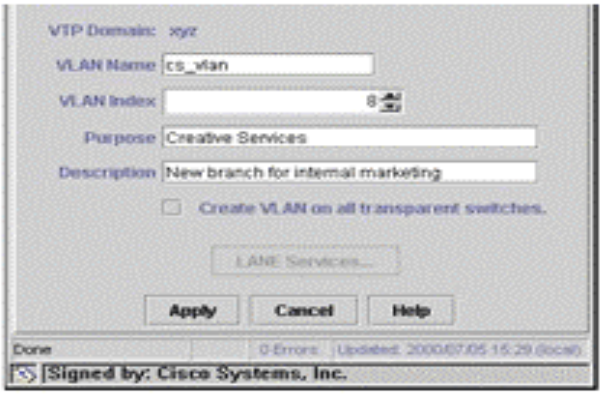


Fig. B

Figura 6.67 CM Administración de VLANS

El último paso, es el de asignar los puertos necesarios a la VLAN creada; como muestra la figura 6.68; se debe llamar a la función de asignación de puertos (fig. 6.68a); cuando la ventana para esta asignación se despliegue en pantalla(fig. 6.68b); simplemente escoja que puertos va a asignar, la VLAN a la cual los va a asignar, y haga click en el botón *move.*

Si la asignación fue satisfactoria, un mensaje indicándolo así se desplegará. Si selecciona el dominio VTP en que creó la VLAN, podrá observar su definición y los puertos que la conforman.

Fig. A

Fig. B

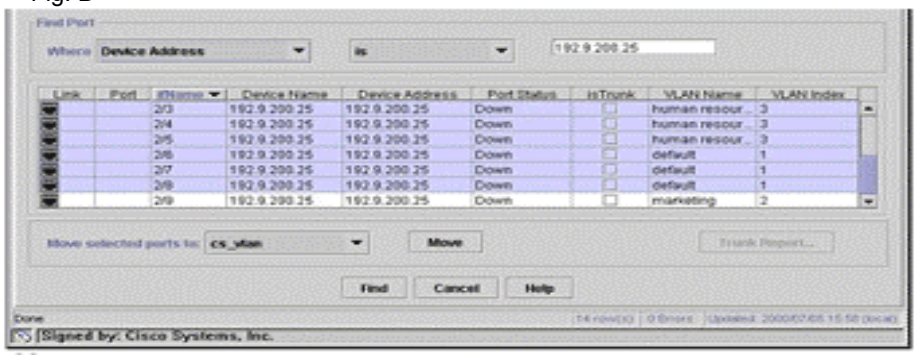


Figura 6.68 CM Asignación de puertos para VLANS

La función análoga a ésta en la aplicación CiscoView es la de configuración (*configure device*). Lo único que se debe hacer es escoger todo el "*chasis"* del conmutador en la interfaz gráfica del dispositivo (el dispositivo entero se ve resaltado con un borde amarillo), hacer clik derecho y escoger la opción de configurar. De ahí, debe navegar entre las diferentes opciones que se presentan en el menú "*category*"; y escoger **VLAN & Bridge**. La siguiente figura muestra la ventana de configuración de VLANs.

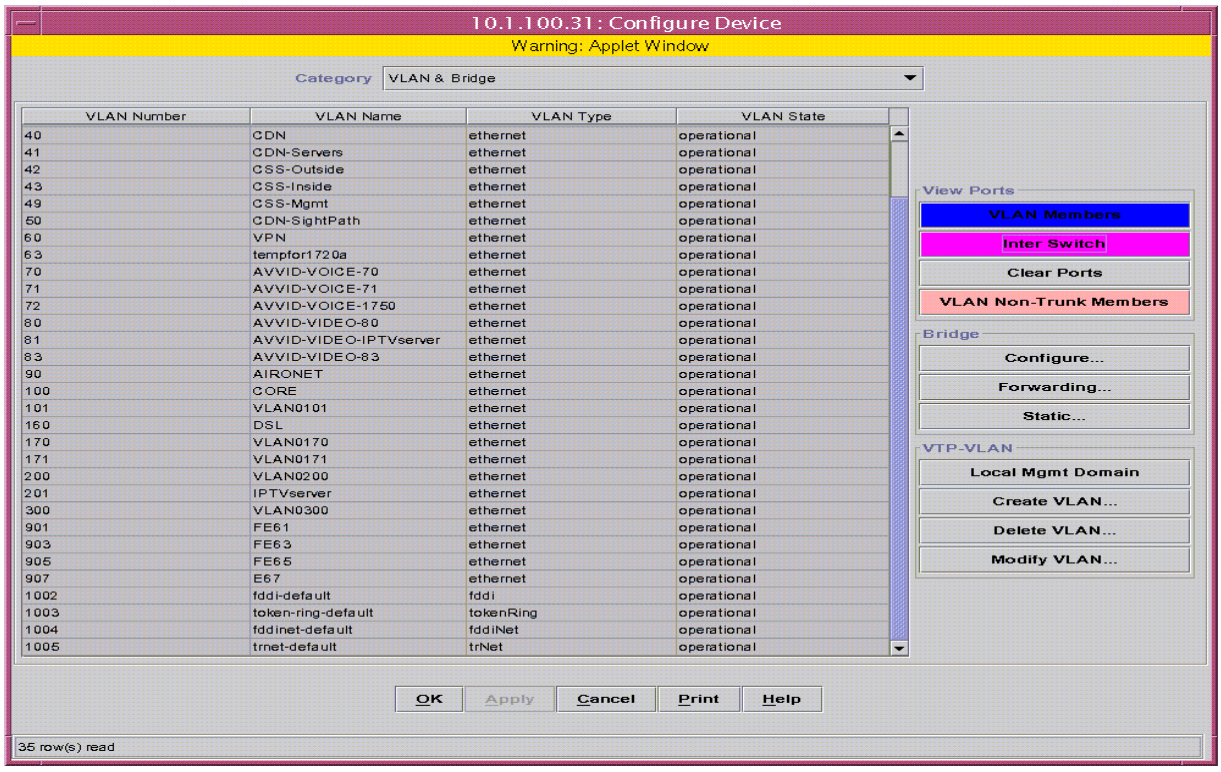


Figura 6.69 CiscoView Administración de VLANS

Ahora bien; asumiendo que el conmutador Catalyst ya está configurado y tiene (por lo menos) un dominio VTP, es posible llevar a cabo la tarea de crear nuevas VLANs; pues esto es un requisito imprescindible.

Partiendo de la ventana que se muestra en la figura 6.69, se debe seleccionar el botón "*create VLAN*". La figura 6.70a muestra la ventana que le permitirá definir la nueva VLAN. Rellene los campos necesarios (número, estado, tipo, nombre, MTU según sus necesidades); haga click en OK y si la nueva VLAN se creó satisfactoriamente, su definición aparecerá en la tabla de VLANs como se muestra en la figura 6.70b.

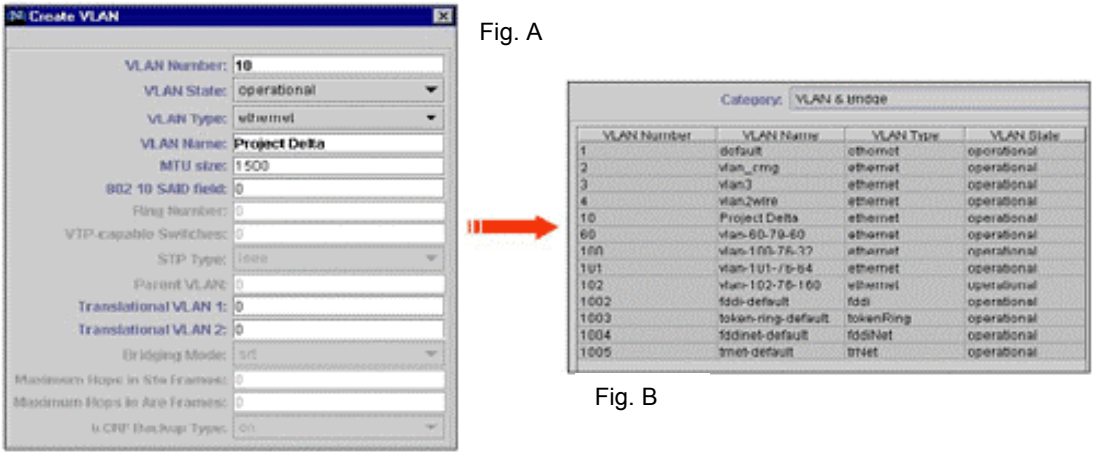


Fig. A

Fig. B

Figura 6.71 Ventana de definición de VLANS CiscoView

Para efectos de este ejemplo, se configurarán 6 puertos ethernet a la VLAN 10 (*project delta*). Para hacer esto, seleccione los 6 puertos (puede seleccionar mas puertos si presiona la tecla CTRL) desde la ventana principal del CiscoView como muestra la figura 6.72a y accese el menú de configuración. Una tabla es desplegada para configuración de interfaces múltiples (fig. 6.72b); donde lo único que tiene que hacer es cambiar el número de VLAN a la que pertenecen los puertos; y la VLAN ha sido creada.

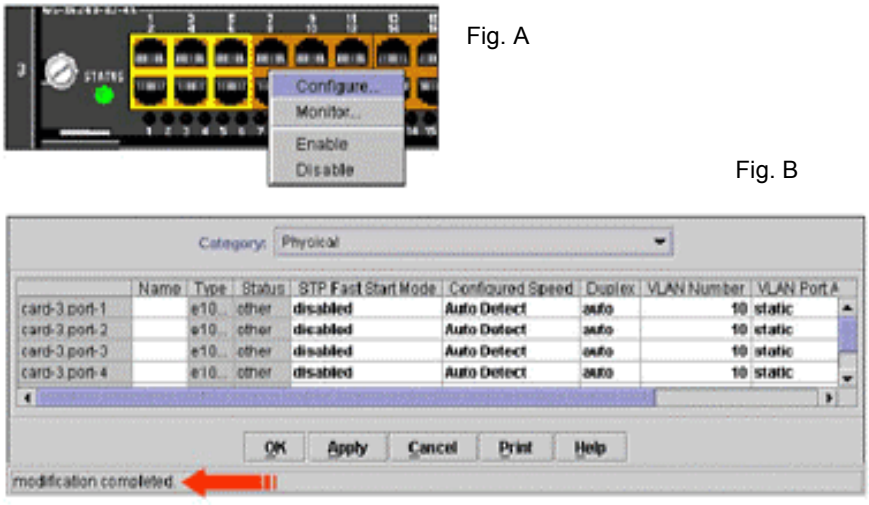


Fig. A

Fig. B

Figura 6.72 Asignación de puertos para VLANS CiscoView

NOTA: Para este ejemplo, se implementó una VLAN estática; si se desea crear una dinámica, es necesario cambiar el campo "*VLAN PortAdmin Status*" a modo dinámico. Además, se debe configurar el *VLAN Membership Policy Server* para asignar dinámicamente la interfaz a una VLAN basado en la dirección MAC conectada a la misma. Esto se puede lograr cambiándose a la categoría VMPS en la ventana de configuración del *chasis*

6.1.9.3 Resolución de problemas de conectividad.

En el dado caso, que sea necesario determinar por qué algún usuario no puede accesar al servidor de archivos, o que alguna de las estaciones de trabajo muestra signos de fallas de conectividad; el módulo Campus Manager ofrece una herramienta para rastrear donde se da el problema de conectividad entre dos dispositivos. *Path Analysis*, es la herramienta que permite realizar este tipo de rastreo. El proceso para realizar el rastreo puede tomar varios minutos; lo único que tiene que tener en cuenta es que debe tener el servidor *ANI (Asynchronous Network Interface*) al día (esto implica haber realizado un descubrimiento de la red recientemente) lo cual se puede lograr utilizando la aplicación **Action→Discover all.**

El paso siguiente es el de rellenar los campos de la fuente y el destino de los dispositivos que se van a analizar. La figura siguiente muestra la ventana donde se realiza esta tarea.

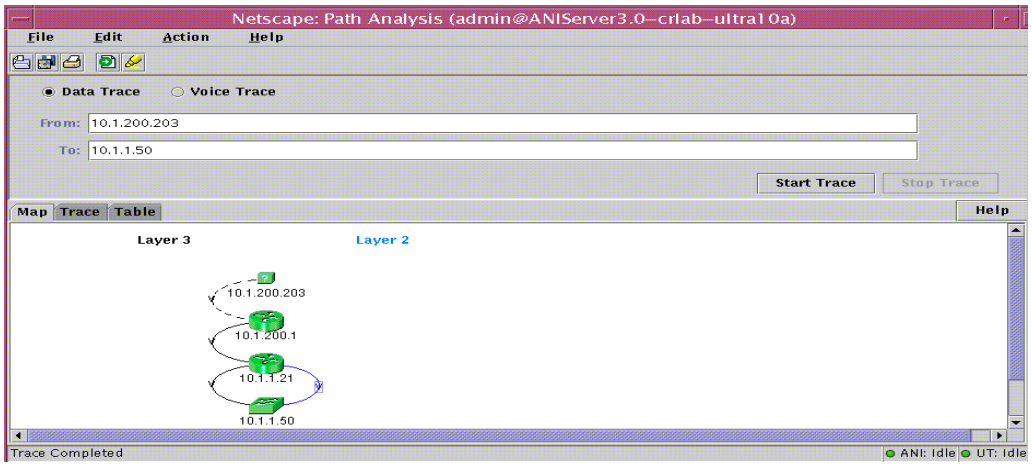


Figura 6.73 CM Ventana de análisis de conectividad

Si el rastreo de la conectividad entre ambos dispositivos es satisfactorio, el mapa de los dispositivos que se encontraron entre los que se estaban supervisando aparece en pantalla; con información de capa 3 y capa 2. Esta información puede observarse de manera tabular en con solo escoger la etiqueta *table*.

Si por el contrario, el análisis no es satisfactorio; el mensaje "*Could no reach source*" esto indicaría la existencia de problemas conectividad de capa 3 entre los dispositivos. Para descubrir cuál es el dispositivo que está fallando, tiene las siguientes opciones:

- Si en el rastreo anterior, este falló solo en la porción final; el problema está en las cercanías del dispositivo destino o en el mismo
- Si por el contrario, el rastreo no paso del dispositivo fuente, el problema se encuentra en el mismo.

Para asegurarse de que esta es la situación, es posible realizar el rastreo de manera inversa con la opción **Action→Reverse Trace**. Obtenida la información, ahora es posible concentrarse en el problema, solo de un lado de la red; por lo que se reducirá el tiempo en que el problema esté latente.

6.1.9.3 Administración de la seguridad en redes WAN enrutadas

El tópico de la seguridad puede ser sumamente denso; la siguiente descripción, se enfocará en el alcance que tiene el módulo *ACL Manager* en cuanto a la seguridad que es posible alcanzar utilizando listas de control de acceso en redes enrutadas.

Para realizar esta función, es necesaria la creación de un *escenario* en el administrador ACL. Inicialmente, debe asegurase de estar en la consola de administración CW2000 con privilegios de administrador; y por supuesto, haber instalado el módulo administrador de ACLs.

El primer paso para lograr la definición de una lista de control de acceso es el de iniciar la aplicación. Esto se logra en la opción **RME→ACL Management→Edit ACLs**. La figura 6.74 muestra la manera en que se debe crear el *escenario* para luego definir la lista ACL.

Debe rellenar los siguientes campos para definir correctamente el escenario:

Scenario Name: Nombre clave que desee utilizar.

Read Config from Device: Marcado.

Recover Scenario: Marcado.

Autosave period: 1 minuto; defina aquí el tiempo que crea conveniente.

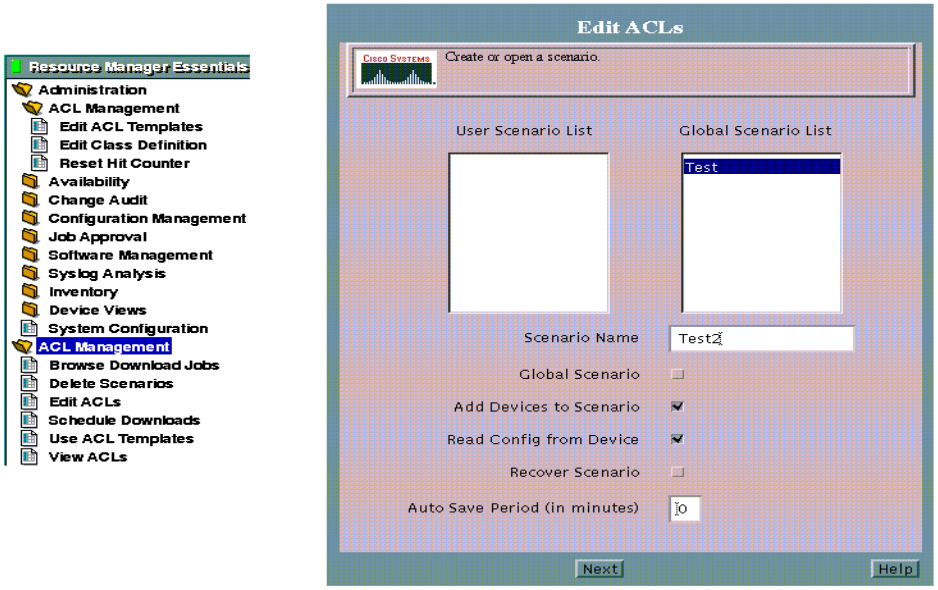


Figura 6.74 Ventana de edición de ACLs

Posteriormente, debe dar click en **next** para escoger en la siguiente ventana los dispositivos a los que desea configurar las listas de acceso. La ventana del *ACL Manager* se le presentará, en ésta, debe hacer click en el folder *ACL Definition* que se encuentra al lado izquierdo de la ventana como muestra la figura 6.xx.

El paso siguiente es el de definir concretamente el ACL que se necesite. Escoja la opción **ACL→New ACL** en la barra de menúes de la aplicación; o bien, haciendo click derecho en el folder *ACL Definition*. La ventana de definición de ACLs aparecerá, y para hacerlo debe de escoger (ver figura 6.75) :

- El tipo de ACL que quiere definir (en el caso de la figura IP)
- Si desea utilizar un número personalizado, o dejar que el administrador le asigne uno.
- Agregar un comentario.

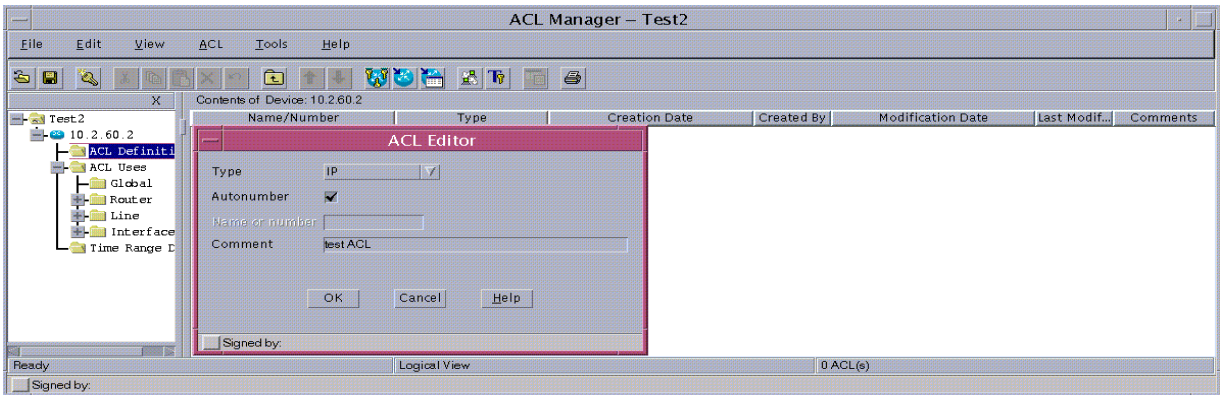


Figura 6.75 Ventana para definición de tipo de ACLs

Ahora bien, hasta el momento, se ha creado el escenario, y la definición del ACL en cuanto a su tipo; pero, no se ha definido qué y quiénes tienen los permisos en el ACL.

Para lograr esto, es necesario definir un ACE (*Access Control Entry*), esto se hace con la opción **ACL→New ACE** de la barra de menús del administrador ACL.

La figura 6.76 muestra la ventana donde se definen el tipo de permisos que se implementarán en la lista de acceso. Para definir el ACE, debe llenar los siguientes campos:

- Escoger el tipo de permiso.
- Dirección fuente y mascara si es necesario
- Comentario.
- Si se desea llevar bitácora (*Log).*

Haciendo click en el botón *Expand* le permitirá definir los parámetros para la creación de listas de control de acceso extendidas.

El siguiente paso es el de estipular que interfaces en el dispositivo donde se está definiendo el ACL, serán las que están protegidas por las mismas. Para lograr esto, haga click derecho en *ACL Definition* y escoja la opción **Use ACL**, una ventana aparecerá para definir las interfaces donde se aplicarán las listas. (Ver fig. 6.77)

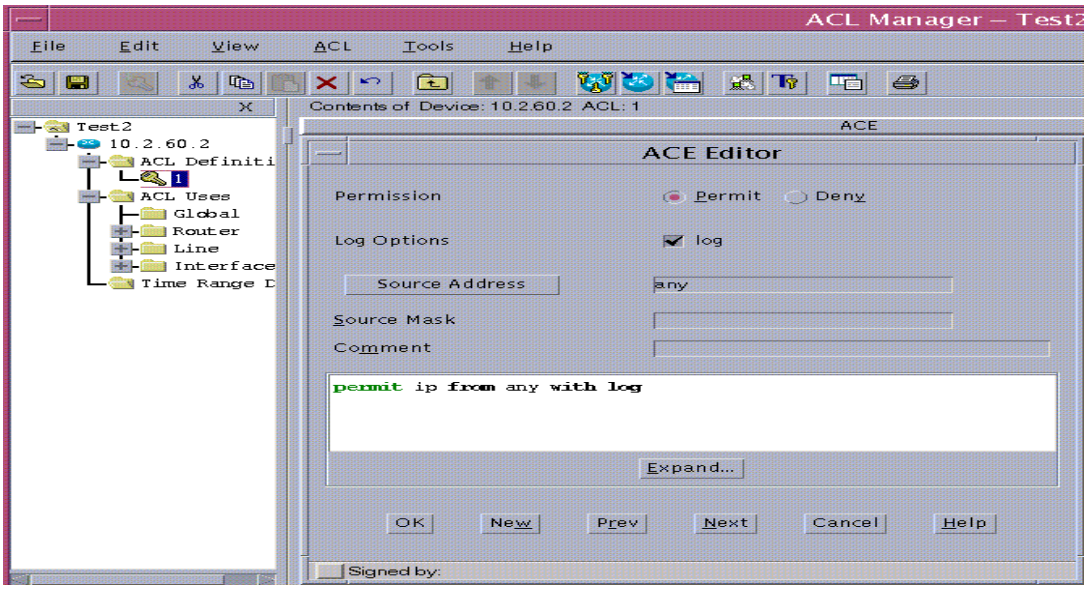


Figura 6.76 Ventana de definición de ACEs

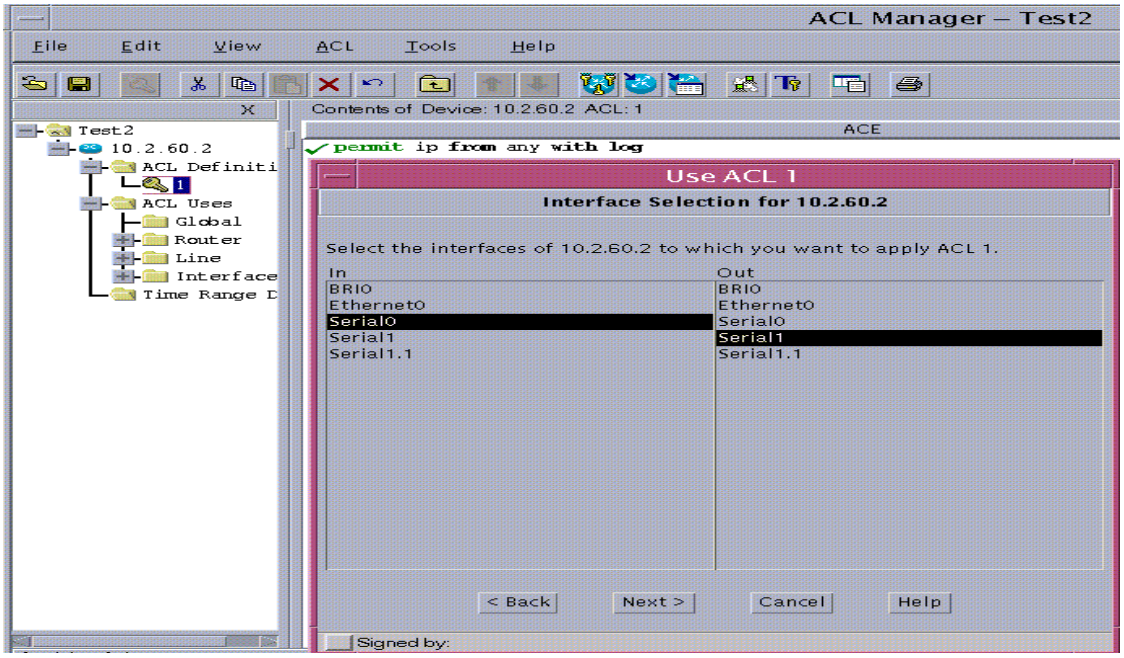


Figura 6.77 Especificación para el uso de ACLs en interfaces especificas

Finalmente, para bajar el ACL al dispositivo, puede hacerlo de varias maneras; usando la opción **Tools→ ACL Downloader**, o bien desde el RME, **RME→ACL Management→ Schedule downloads**.

En ambos casos, es necesario que se definan parámetros; como los dispositivos a los que desea descargar el ACL, la fecha y hora (si desea que sea programado) y los siguientes parámetros de seguridad:

- *Download in Parallel*: para realizar la tarea en paralelo, sin importar el orden de descarga
- *Write to NVRAM*: después de la descarga, se realiza la copia del "running config" a la memoria no volátil.
- *Rollback*: para asegurarse que en caso de falla de la descarga, los cambios realizados antes del error sean removidos.
- *Abort on error*: la configuración original se restablece en caso de error en la descarga.

La siguiente figura presenta la ventana de configuración de descarga. Para el final de ésta, la ACL debe de estar totalmente funcional y trabajando en su equipo.

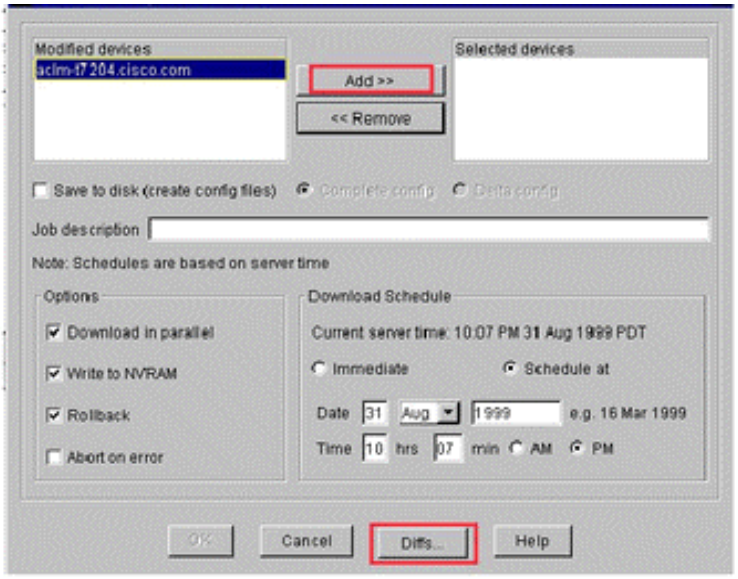


Figura 6.78 Ventana de programación para la descarga de las listas de acceso.

6.2 Alcances y limitaciones

El alcance que éste proyecto tiene se basa en la necesidad de llenar un vacío respecto a la experiencia que se tiene en cuando al tema de la administración de redes en los últimos tiempos. El proyecto consistió de varias etapas con el fin de crear conocimiento práctico sobre las diferentes herramientas que Cisco Systems provee para una correcta administración de sus equipos. Estas herramientas basadas en el modelo ISO de administración de redes, permiten a los administradores tener visibilidad completa de todas las capas de red; mantener una base de datos para análisis de tendencias, mantener un inventario detallado de la red, un registro de configuraciones, en fin un mantenimiento de tipo proactivo.

Sin embargo, el tema de la administración de redes es muy amplio, y varios de los tópicos acerca del mismo fueron excluidos de éste trabajo (por razones de tiempo y del enfoque que se planteo desde el inicio); ya que lo que se espera es un manual que permita desarrollar soluciones integrales para la administración de redes tipo *enterprise.* Por ejemplo, la administración de la seguridad en una red se tocó desde el punto de vista de la implementación de las listas de control de acceso; mientras que se dejaron de lado los VPN (*virtual private network*); igual sucedió con respecto a la administración de arquitectura *Content*, el IPM y las muchas funciones que posee el módulo RME; pues el proyecto tuvo un enfoque directo a la administración de desempeño, faltas y configuración

Inclusive, aunque se pretendió abarcar de manera diligente las bondades del software de administración CW2000; explotar todas las características que éste ofrece, significaría entrar muy de fondo y en detalle a cada una de éstas.

Como se dijo anteriormente, este trabajo pretende ser un punto de partida para informar y formar un criterio más amplio ante la necesidad de mantener un control proactivo de los dispositivos que conforman una red de trabajo y como se debe de llevar a cabo este control.

CAPITULO 7
CONCLUSIONES.

1. La administración de desempeño para una red es una de las claves mas importantes para el éxito y óptimo funcionamiento de la misma; y a la vez de una organización.
2. La planificación es clave importante para una administración exitosa de cualquier red.
3. Mientras más información se tenga de la red que se administra, es mucho más fácil enfrentar los problemas de un posible fallo en la misma.
4. El uso de dispositivo de supervisión externa presenta grandes ventajas respecto a la utilización de supervisión por agentes internos en los dispositivos.
5. La utilidad del NAM está comprobada cuando se necesita una supervisión y control integrada RMON 1 y 2, sin embargo, los dispositivos *switchprobe* son mucho mas flexibles en cuanto a su desarrollo dentro de una organización.
6. La estrategia de la empresa Cisco Systems en cuanto a la administración de redes es muy acertada, pues permite conocer los datos necesarios para la solución de problemas de manera rápida y efectiva.
7. Los paquetes de software para administración de redes de Cisco Systems son una gran herramienta para el mantenimiento constante e inteligente de los dispositivos de red.
8. Es importante el balanceo de carga que se haga para la administración de una red; la segmentación y el uso de servidores con funciones de administración especificas es una buena estrategia.
9. La supervisión de enlaces críticos es una buena estrategia de administración; pues éstos son de mucha mayor importancia para su organización y le facilitarán el desarrollo de soluciones de administración y mucho dinero.
10. Es importante dejar una opción de crecimiento para las herramientas de administración tomando en cuenta el crecimiento de su red.

Recomendaciones

- Es recomendable crear una red enrutada o VLAN solamente para el tráfico administrativo.
- Busque medios lógicos de segmentación de su red (*VTP domains*, *IP address ranges*, *LAN/WAN boundaries*); pues una red segmentada es mucho mas fácil de administrar.
- Busque la separación de funciones en la administración. Por ejemplo; HPOV en un servidor de administración; CW2K en otro y *TrafficDirector* en un servidor aparte. Esto le permitirá que las herramientas que utilice para administrar su red, trabajen al 100% y con recursos dedicados e idóneos para su ejecución.
- Tenga en cuenta los límites de escalabilidad de cualquier producto cuando haga la distribución de funciones.
- Hasta los mejores productos de NM pueden ser inútiles si se utilizan malas prácticas; además, las herramientas le ayudarán a hacer su trabajo, pero no lo harán por ud.
- Asegúrese de entender las tecnologías con las que trabaja en su red y los requerimientos de los usuarios a quienes brinda servicio; ésto le permitirá establecer niveles base para trabajar y mantener.
- Entienda su organización, ésto le servirá para evitar problemas por atribución de funciones que no corresponden.
- Prepare sus dispositivos para la administración; utilice al máximo las características que éstos poseen para ser administrados
- Utilice los *community strings* para accesar sus dispositivos.
- Utilice las opciones de notificación de los dispositivos que administra: ej. *Syslog* y *Traps*.
- Mantenga siempre a mano un inventario del equipo que administra y sus características; ésta información le podría ahorra mucho tiempo y dinero en una eventual caída de su red.

- Realice periódicamente una etapa de recolección de datos de desempeño; ésto le permitirá estar al tanto de la “salud de su red”.
- Mantenga una base de datos de las configuraciones, esto le ayudara a enfrentar conflictos por cambios hechos en la red de manera mas rápida; use herramientas que automaticen esta tarea.
- Implemente un proceso de control de cambios; para que éstos sean planeados y supervisados.
- Investigue el *release* de *software* para el soporte y la compatibilidad de su hardware con las plataformas de administración de red.
- El número de ACLs es un límite crítico para el desempeño de su red.
- Para la utilización del *TrafficDirector*; se recomienda no habilitar el *logging* cuando se supervisen muchos puertos; ya que ésto puede crear muchos procesos que a su vez crearán un aumento en la utilización del CPU del NMS y por supuesto un uso muy alto del disco duro. Los límites de su habilitación dependerán de la frecuencia de *polling* y el número de agentes que se administrarán.

BIBLIOGRAFÍA.

Documentos de internet:

White Papers Públicos de Cisco
http://www.cisco.com/warp/public/cc/pd/nemnsw/sips/tech/
Remote Monitoring Solutions for Wide-Area Networks: A Comprehensive WAN Monitoring Strategy for Enterprise Networks 1998 Cisco Systems.
Network Monitoring in an Enterprise LAN Environment 2000 Cisco Systems.
Network Monitoring in an Enterprise WAN Environment 2000 Cisco Systems.
Remote Monitoring Solutions for Switched Internetworks: A Comprehensive Strategy for Monitoring Enterprise Networks 1998 Cisco Systems.
Remote Monitoring for Switched Internetworks (RMON and RMON2) 2000 Cisco Systems.

Data Sheets Network Management Products
http://www.cisco.com/warp/public/752/ds/english/nm.html
Configuring Network Management
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/rel_4_2/config/netmg.htm
Understanding the Catalyst Switched Port Analyzer Feature.
http://www.cisco.com/warp/public/473/41.html
Using TrafficDirector to manage RMON I/II devices
http://www.cisco.com/warp/public/477/TD/tdir-agent.html
Configuring the TrafficDirector to use NAM card in a Catalyst Switch
http://www.cisco.com/warp/public/477/TD/37.html
Configuring the Network Analysis Module.
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/rel_5_2/config/nam.htm
MIB Quick Reference Guide
http://www.cisco.com/univercd/cc/td/doc/product/software/ios11/mbook/mtext.htm
SwitchProbe support page
http://www.cisco.com/pcgibin/Support/PSP/psp_view.pl?p=Hardware:Switchprobe&s=Documentation#Product_Documentation
Network Management Basics
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/nmbasics.htm

Documentos públicos del foro SNMP http://www.snmp.com
Siegel Manfred ***Hierarchical Network Management***
Siegel Manfred ***What is Network Management***
Goldsmith German ***Distributed Network Management***

Otros documentos:
Northeats Consulting ***Building the Management Intranet*** http://www.ncri.com
Documentos sobre RFC's http://moon.act.uji.es/~jcasani/rfc.htm
SNMPV3 http://www.ibr.cs.tu-bs.de/ietf/snmpv3/

APENDICES

APÉNDICE 1:
NETWORK MANAGEMENT

Introducción.

La administración de redes (Network Management) significa cosas diferentes para personas diferentes, en algunos casos envuelve a un consultor de redes solitario supervisando la actividad de la red con un analizador de protocolos obsoleto. En otros casos, la administración de redes envuelve una base de datos distribuida, dispositivos de red auto-supervisados y estaciones de trabajo de alto perfil generando visualizaciones gráficas en tiempo real de los cambios en la topología de red y el tráfico. En general, network management es un servicio que emplea gran variedad de herramientas, aplicaciones y dispositivos para asistir a los administradores de red a supervisar y mantener la red.

Desde la explosión de las telecomunicaciones y la Internet en los últimos 15 años, ha sido evidente la necesidad de un planeamiento en cuanto a la manera en que se debe administrar las operaciones de una red y su crecimiento vertiginoso. Precisamente, el crecimiento de las redes a nivel privado y público; las nuevas tecnologías de redes y la falta de expertos dedicados al manejo y administración de las crecientes y heterogéneas redes, fueron los factores que permitieron el advenimiento de los protocolos de manejo y administración de redes; para la realización de éstas tareas de manera sencilla y centralizada.

A.1 Arquitectura de Administración de Redes.

Muchas arquitecturas de administración de redes usan la misma estructura y conjunto de relaciones. Las *Estaciones Finales* (dispositivos administrados), como lo son las computadoras y otros dispositivos de red, corren software que los habilita para enviar alertas cuando reconocen problemas (por ejemplo, cuando uno o más umbrales determinados por el usuario se han excedido).

Una vez recibidas las alertas las *Entidades de Administración* están programadas para reaccionar ejecutando una, varias, o un grupo de acciones, que incluyen: la notificación al operador, registro de eventos, apagado del sistema, e intentos de reparación automática del sistema.

Las entidades de administración pueden "encuestar" a las Estaciones Finales para revisar los valores de ciertas variables. Las encuestas pueden ser automáticas o iniciadas por usuario, pero los *agentes* en las estaciones finales responden a todas las encuestas. Los *Agentes* son módulos de software que primero compilan información de los dispositivos administrados en los cuales residen, y almacenan la información en una *Tabla MIB* (*Base de Datos de Administración)*, y finalmente la proveen a las entidades de administración dentro del *sistema de administración de redes (Network Management Systems NMS)* por medio de un *protocolo de administración de redes.* Los protocolos mas conocidos incluyen al Protocolo Simple de Administración de Redes (*SNMP Simple Network Management Protocol*), y al Protocolo Común de información de administración (*CMIP Common Management Information Protocol*). Los *proxies* de administración son entidades que proveen información de administración en lugar de otras entidades.

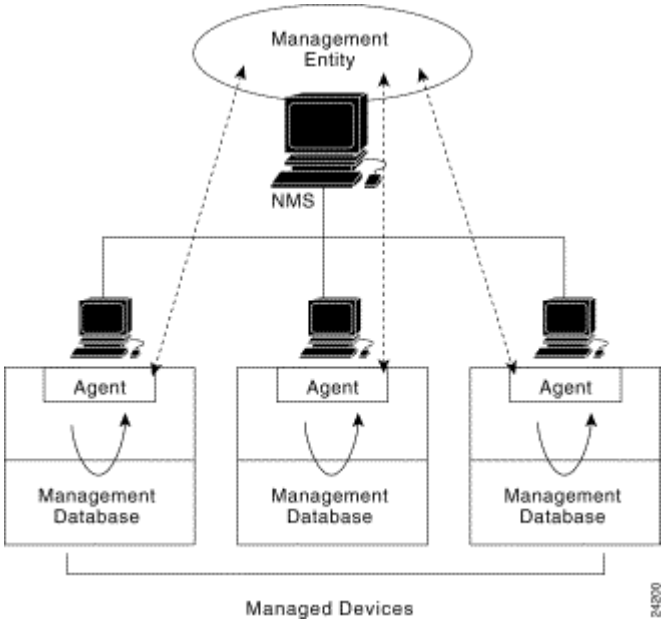


Figura A1.1 Arquitectura básica de administración de redes

A.1.1 Modelo ISO de Administración de Redes

La ISO ha contribuido de gran manera a la estandarización de las redes. Su modelo de administración de redes es un medio primario para el entendimiento de las grandes funciones de los sistemas de administración de redes. Éste modelo consiste de cinco áreas conceptuales:

- Administración de Desempeño (*Performance Management*)
- Administración de Configuración (*Configuration Management*)
- Administración de Cuentas (*Accounting Management*)
- Administración de Fallas (*Fault Management*)
- Administración de Seguridad (*Security Management*)

Administración de Desempeño.

Su objetivo es el de medir y hacer disponible varios aspectos del desempeño de la red para que ésta pueda ser mantenida a un nivel aceptable. Ejemplos de variables de desempeño que pueden ser proveídas incluyen el *throughput* de la red, tiempos de respuesta al usuario y utilización de la línea.

Éste tipo de administración envuelve tres pasos; primero, los datos del desempeño de la red son recolectados en variables de red que interesan al administrador. Segundo, los datos son analizados para determinar los niveles normales (*baseline*). Finalmente, los umbrales apropiados son determinados para cada variable importante; así, cuando éstos umbrales son excedidos se indica que existe un problema digno de atención.

Las entidades de administración supervisan continuamente las variables de desempeño, y cuando un umbral es excedido, una alerta es generada y enviada al sistema de administración de redes.

Cada uno de éstos pasos descritos, es parte del proceso de respuesta para sistemas reactivos.

Cuando el desempeño se torna inaceptable porque se excedió una variable definida, el sistema reacciona enviando un mensaje. La administración del desempeño también permite la utilización de métodos proactivos. Por ejemplo, la simulación de la red puede ser utilizada para proyectar como el crecimiento de la red puede afectar las medidas de desempeño. Tal simulación puede alertar a los administradores para impedir problemas, y así medidas correctivas pueden ser tomadas.

Administración de Configuración.

El objetivo de ésta, es supervisar la red y la información de configuración del sistema; para que así, los efectos de las varias posibles versiones de los elementos de hardware y software tengan seguimiento y sean administrados.

Cada dispositivo de red posee una variedad de versiones de información asociadas a él. Los subsistemas de la administración de *configuración* almacenan ésta información en una base de datos para fácil acceso. Así, cuando un problema ocurre, ésta base de datos puede ser investigada por pistas que puedan ayudar a resolver el problema.

Administración de Cuentas.

Su objetivo es el de medir los parámetros de utilización de la red, para poder así, regular apropiadamente el uso individual o grupal de la red. Tal regulación minimiza los problemas de la red (porque los recursos pueden ser proporcionados basados en las capacidades) y maximiza la justicia en el acceso entre todos los usuarios.

Como en la administración de desempeño, el primer paso hacia una apropiada administración de cuentas, es medir la utilización de todos lo recursos importantes de la red. El análisis de los resultados provee un vistazo a los patrones de uso y de ahí las “cuotas de uso” pueden ser estimadas. Algunas correcciones pueden ser requeridas para alcanzar las practicas de acceso optimo; y proveer una utilización de recursos optima.

Administración de Fallas.

Su objetivo primordial es detectar, registrar, notificar a los usuarios, y (en la medida de lo posible) corregir automáticamente los problemas que ocurran para mantener la red funcionando efectivamente. Debido a que las fallas pueden causar la caída o una degradación inaceptable de la red, la administración de fallas es la mas ampliamente implementada del modelo ISO.

La administración de fallas envuelve primeramente, la determinación de síntomas, el reconocimiento de los problemas; luego, el problema es solucionado y está probada en todos los subsistemas importantes. Finalmente, la detección y resolución del problema es registrada.

Administración de Seguridad.

Su función fundamental, es la de controlar el acceso a los recursos de la red de acuerdo con las pautas estipuladas localmente; para que la red no pueda ser saboteada (intencionalmente o no) y que la información importante no pueda ser accesada por aquellos que no tienen la autorización apropiada. Un subsistema de administración de seguridad; por ejemplo, puede sondear a los usuarios accesando un recurso de la red, impidiéndole el acceso a aquellas que ingresan códigos de acceso inapropiados.

Los subsistemas de seguridad trabajan particionando los recursos de red, en áreas autorizadas y no autorizadas. Éstos subsistemas, llevan a cabo varias funciones. Identifican recursos importantes de la red y determinan la relación entre esos recursos importantes de la red y grupos de usuarios. Éstos también supervisan los puntos de acceso de éstos recursos y registran el acceso inapropiado de los mismos.

A.1.2 Modelo IBM de administración de redes.

La administración de redes IBM se refiere a cualquier arquitectura que se use para administrar redes IBM SNA (*Sistems Network Arquitecture*) o bien redes APPN (*Advanced Peer to Peer Networking*). La administración de redes IBM es parte de la arquitectura de redes abiertas ONA (*Open Network Arquitecture*) y es desempeñada de manera centralizada por el uso de plataformas de administración tales como NetView y otras. De manera similar al modelo ISO, se divide en cinco áreas especificas las cuales son:

- Administración de Configuración (*Configuration Management*)
- Administración de Desempeño y Cuentas (*Performance and Accounting management*).
- Administración de Problemas (*Problem Management*).
- Administración de Operaciones (*Operations Management*).
- Administración de Cambios (*Change Management*).

Administración de Configuración IBM

La administración de configuración controla información describiendo las características lógicas y físicas de los recursos de red, como también de las relaciones entre éstos recursos. Un sistema central de administración almacena la información en bases de datos de configuración, y pueden incluir información tal como el software del sistema, los números de las versiones del micro código, números seriales de hardware o software, localización física de los dispositivos de red, nombres, direcciones, y números de teléfono de los contactos. Como era de esperar, ésta especificación es muy similar a la de la administración de configuración del modelo ISO.

Las facilidades de ésta área ayudan a mantener un inventario de los recursos de red y aseguran que los cambios en la configuración de la misma se reflejen en la base de datos. Ésta función de administración provee información que es usada por la administración de fallas (para comparar diferentes versiones y localizar, identificar, y revisarlas características de los recursos de red) y el área de administración de cambios de cambios (para analizar el efecto de los cambios y realizar los cambios en momentos que haga menos impactos en la red).

Administración de Desempeño y Cuentas IBM

Ésta área de administración provee información acerca del desempeño de los recursos de red. Sus funciones incluyen supervisar el tiempo de respuesta de los sistemas, medir la disponibilidad y uso de los recursos; además del seguimiento, control y mantenimiento de los mismos. La información reunida en las funciones de ésta área, es importante para conocer si las metas de desempeño de la red están siendo cumplidas y si se deben iniciar los procedimientos de "reconocimiento de problemas" basados en las mediciones.

Administración de Problemas IBM.

Ésta área es similar a la administración de fallas del modelo ISO en que se encarga de las condiciones de error que causan la pérdida para los usuarios del desempeño óptimo de los recursos de red. La administración de problemas consta de 5 pasos: determinación del problema, diagnóstico del problema, paso y recuperación del problema, resolución del problema, seguimiento y control del problema. La determinación del problema consiste en detectarlo y completar los pasos necesarios para el inicio del diagnóstico del mismo; como lo es, el aislamiento del problema a una subsistema particular. El diagnóstico en si consiste en la determinación precisa de la causa de problema y la acción requerida para resolverlo. El paso y recuperación del problema consiste en los intentos de sobreponerse al problema, parcial o completamente aunque sea temporalmente.

La resolución del problema se refiere a los esfuerzos para eliminar el problema y muchas veces requiere de acciones correctivas como el reemplazo de *hardware* y *software*. El seguimiento y control del problema consiste en seguir los problemas hasta que una solución definitiva sea alcanzada; además, información vital acerca de esto debe ser registrada.

Administración de Operaciones IBM.

Ésta consiste en la administración de los recursos distribuidos de la red desde un sitio central, usando dos conjuntos de funciones: Servicios de administración de operaciones y Servicios comunes de operaciones.

Los servicios de Administración de operaciones se encargan de proveer el control de recursos remotos de manera centralizada, usando operaciones como: activación y desactivación de recursos, cancelación de ordenes, etc. Éstos servicios pueden ser iniciados automáticamente en respuesta a alguna notificación de problemas en el sistema.

Los servicios comunes de operación permiten que la administración de los recursos sea explícitamente dirigida por otras áreas de administración, usando comunicación a través de aplicaciones especializadas. Los servicios de operación común ofrecen dos importantes servicios; el de ejecución de comandos (provee medios estandarizados para la ejecución de comandos remotos) y el servicio de administración de recursos (el cual provee un medio para el transporte de información de manera independiente del contexto).

Administración de Cambios IBM

Ésta se encarga de dar seguimiento a los cambios de la red y mantiene archivos de cambio en nodos remotos. Los cambios en la red suceden principalmente por; el cambio en los requerimientos del usuario (incluye las actualizaciones de hardware y software, nuevas aplicaciones y servicios, etc.).

O bien, debido a la necesidad tratar los cambios inesperados resultado de hardware y software (daños etc.).

Arquitecturas de Administración de redes IBM

Dos de las más conocidas arquitecturas de administración de redes son: Arquitecturas de Redes Abiertas (*ONA Open Network Arquitecture*) y *SystemView*.

- *Open Network Arquitecture ONA*

La arquitectura ONA es una arquitectura de administración de redes ampliamente generalizada, que define cuatro entidades de administración claves: el punto focal, el punto de recolección, el punto de entrada y finalmente el punto de servicio.

El punto focal es una entidad de administración que provee soporte para las operaciones de administración de redes centralizadas. Éste, responde a las alertas de las estaciones finales, mantiene las bases de datos, y provee de una interfaz de usuario al administrador de la red. Existen tres tipos de puntos focales; primario, secundario y anidados.

Los puntos focales primarios cumplen con todas las funciones antes mencionadas. Los puntos focales secundarios actúan como un respaldo de los primarios y se usan cuando éstos fallan. Los puntos focales anidados proveen soporte de administración distribuido para redes grandes; y son responsables por direccionar información critica a as puntos focales globales.

Los puntos de recolección distribuyen información de sub redes SNA auto contenidas a los puntos focales. Éstos son comúnmente utilizadas para direccionar datos de redes *peer to peer* a la jerarquía ONA.

Un punto de entrada es un dispositivo SNA que puede implementar la arquitectura ONA por el mismo otros dispositivos. La mayoría de los dispositivos SNA son capaces de convertirse en puntos de entrada.

Un punto de servicio es un sistema que provee acceso a una arquitectura ONA para dispositivos que no son SNA y es esencialmente una puerta de entrada a la arquitectura ONA. Los puntos de servicio son capaces de enviar información de administración acerca de sistemas que no son SNA a los puntos focales, recibiendo comandos de los puntos focales, y traduciendo comandos a un formato aceptable para los dispositivos que no son SNA para su ejecución.

- *SystemView.*

SystemView es un esquema para la creación de aplicaciones de administración que permiten supervisión en sistemas multi-vendedor. *SystemView* describe como las aplicaciones administran redes heterogéneas que operan con otros sistemas de administración. Ésta es la estrategia oficial de administración de sistemas de la arquitectura Sistema - Aplicación de IBM.

A.2 Normas para la administración de redes.

El Comité Asesor de Internet (*Internet Advisory Board, IAB*) ha elaborado y adoptado varias normas para la administración de la red. En su mayoría, éstas se han diseñado específicamente para ajustarse a los requerimientos del protocolo TCP/IP, aunque, cuando es posible, cumplen con la arquitectura OSI. El *IETF (Internet Engineering Task Force*), responsable de las normas para la administración de la red, adoptó un enfoque de dos pasos para cubrir las necesidades actuales y futuras.

El primer paso comprende el uso del Protocolo Simple para Administración de la Red (*Simple Network Management Protocol, SNMP*), el cual fue diseñado y aplicado por el IETF. El protocolo SNMP se utiliza actualmente en muchas redes y por supuesto en Internet; y está integrado dentro de la gran mayoría de los productos comerciales que están disponibles. Conforme se ha mejorado la tecnología, SNMP ha evolucionado y se ha vuelto más completo.

El segundo paso comprende las normas OSI para administración de la red, llamados Servicios Comunes de Información sobre la Administración (*Common Management Information Services, CMIS*), y el Protocolo Común de Información sobre la Administración (*Common Management Information Protocol, CMIP*), el cual se utilizará en las futuras aplicaciones de TCP/IP.

Tanto SNMP como CMIP utilizan el concepto de *Network Management Systems* NMS, que intercambian información con los procesos que se encuentran dentro de los dispositivos de la red, como las estaciones de trabajo, *bridges*, enrutadores y conmutadores.

La estación primaria de administración se comunica con los diferentes procesos de administración, para analizar la información sobre el estado de la red.

A.2.1 ¿Qué es SNMP?

El Protocolo Simple para Administración de Redes (SNMP), fue diseñado originalmente para proporcionar un medio para manejar los enrutadores de una red. Así, SNMP, aunque es parte de la familia de protocolos TCP/IP, no depende del protocolo IP; pues fue diseñado para ser independiente del protocolo (de manera que pueda correr igual de fácil bajo IPX de SPX/IPX de Novell, por ejemplo); sin embargo, la mayor parte de las instalaciones SNMP utilizan IP en redes TCP/IP.

Algunas de las especificaciones en el diseño del protocolo SNMP fueron:

- Administración de red integrada: capacidad de administrar redes incorporando componentes que vinieran de una variedad de fabricantes con una simple aplicación.
- Inter-operabilidad: capacidad de tener un dispositivo de un proveedor administrado por otro dispositivo de diferente proveedor.
- Estándares: éstos definen métodos comunes de comunicación y estructuras de datos de manera que redes diferentes puedan ser integradas con una administración de red.

Los componentes esenciales del protocolo SNMP y sus papeles se muestran a continuación:

- Base de información de la administración (*Management Information Base MIB*)
- Estructura de identificación de la información sobre la *administración (Structure Management Information SMI*)
- Protocolo Simple para Administración de Redes (*Simple Network Management Protocol SNMP*)

La IAB ha designado al SNMP, SMI, y a la Internet MIB iniciales como "Protocolos Estándar", con *status* de "recomendado". Por medio de esta acción, la IAB recomienda que todas las implementaciones en IP y TCP sean administrables por web.

De acuerdo a las especificaciones; la arquitectura para la implementación de SNMP consta de 3 elementos o partes: el NMS o administrador, el agente y la tabla MIB.

A.2.1.1 Administrador NMS (Network Management System)

Es un nodo que activamente participa en la administración de la red. Éste solicita e interpreta los datos acerca de los dispositivos de red y el tráfico de la misma, y típicamente interactúa con los usuarios para llevar a cabo sus intenciones. Un administrador puede provocar cambios en un agente alterando el valor de una variable en el nodo agente. Los administradores o *managers* son frecuentemente implementados como aplicaciones de red.

El administrador se localiza en el host principal de la red. Su principal función es encuestar a los agentes acerca de cierta información solicitada. Existen muchos softwares compatibles, por ejemplo para *PC's Netguard* y sobre UNIX el *HP Open View.*

A.2.1.2 Agentes

Un agente SNMP es un software que reside en un nodo de red y es responsable de comunicarse con los *managers* o administradores considerando el nodo. El nodo es representado como un objeto administrado teniendo varios campos o variables que están definidas en el MIB apropiado.

El agente tiene dos propósitos:

- Responder a las solicitudes de los *managers*, suministrando o cambiando los valores de las variables de los objetos según se solicitaron.
- Generar *traps* para alertar a los *managers* de los eventos notables que ocurren en el nodo, tales como una falla.

El agente corre en cada nodo de la red. Colecciona información de red y terminal como esté especificado en el MIB.

No todos los dispositivos soportan SNMP directamente. Los dispositivos que no lo hacen pueden tener un apoderado (proxy) que les traduzca entre SNMP y él mismo.

A.2.1.3 Interacción entre *Administradores y Agentes*

El administrador, se comunica con el agente por mensajes de SNMP los cuales están en forma de solicitudes, éstos no necesitan saber ningún detalle interno acerca del objeto administrado por el agente. Además, un agente SNMP puede servir solicitudes de muchos administradores SNMP. El agente no necesita saber el contenido de la solicitud o la estructura del administrador que está haciendo la solicitud. El agente valida la solicitud, los servicios, y entra en estado pasivo, esperando la siguiente solicitud. Esta división de responsabilidades simplifica las soluciones de administración de red.

Los periféricos que tienen integradas las capacidades para SNMP corren un software agente para administración, cargado como parte de un ciclo de arranque o dentro de la memoria fija (*firmware*) del dispositivo. Éstos dispositivos que tienen agentes SNMP se dice que se tratan de dispositivos administrados.

Los dispositivos administrados por SNMP se comunican con el software servidor SNMP que está localizado en cualquier parte de la red. El dispositivo habla con el servidor de dos formas: por sondeo o por interrupción

Un dispositivo sondeado hace que el servidor se comunique con el dispositivo, preguntándole sobre su condición o sobre sus estadísticas actuales. El sondeo en ocasiones se hace en intervalos regulares, teniendo al servidor conectado a todos los dispositivos administrados de la red. El problema con el sondeo es que la información no siempre es actual, el tráfico de la red se incrementa con el número de dispositivos administrados y la frecuencia del sondeo.

Un sistema SNMP basado en la interrupción hace que el dispositivo administrado envíe mensajes al servidor cuando algunas condiciones lo garanticen. De ésta forma, el servidor conoce inmediatamente cualquier problema (a menos que el dispositivo falle, en cuyo caso la notificación debe hacerse desde otro dispositivo que haya tratado de comunicarse con el dispositivo que falló).

Los dispositivos basados en la interrupción tienen sus propios problemas. En primer lugar, está la necesidad de ensamblar un mensaje para el servidor, lo que puede requerir de una gran cantidad de ciclos del CPU, todos los cuales se toman de la tarea normal del dispositivo. Esto puede provocar cuellos de botella y otros problemas en el dispositivo. Si el mensaje que va a enviarse es extenso, como sucede cuando contiene una gran cantidad de estadísticas, la red puede padecer de una notable degradación mientras el mensaje se ensambla y transmite.

Si existe una falla mayor en cualquier parte de la red, como cuando falla la corriente eléctrica y se activan las fuentes de energía, cada dispositivo administrado por SNMP tratará de enviar al mismo tiempo, mensajes controlados por interrupción hacia el servidor, para reportar el problema. Esto puede congestionar la red y producir una información errónea en el servidor.

A menudo se utiliza una combinación de sondeo y de interrupción para sobreponerse a todos éstos problemas. La combinación se llama sondeo dirigido por *traps*, e implica que el servidor haga un sondeo de las estadísticas a intervalos regulares o cada vez que lo ordene el administrador de sistema. Además, cada dispositivo administrado por SNMP puede generar un mensaje de interrupción cuando se presenten ciertas condiciones, pero éstos mensajes tienden a estar más rigurosamente definidos que en un simple sistema controlado por interrupción. Por ejemplo, sí se utiliza SNMP sólo mediante interrupción, un enrutador puede reportar un incremento de la carga cada 10 por ciento. Si utiliza un sondeo por *traps*, usted conoce la carga del sondeo regular y puede dar instrucciones al enrutador para enviar una sola interrupción cuando se experimente un incremento significativo en la carga. Después de recibir un mensaje de interrupción con sondeo por *traps*, el servidor puede seguir sondeando al dispositivo para mayores detalles, en caso de ser necesario.

La computadora del administrador no necesita conectarse directamente hacia todas las redes físicas que contiene entidades administradas.

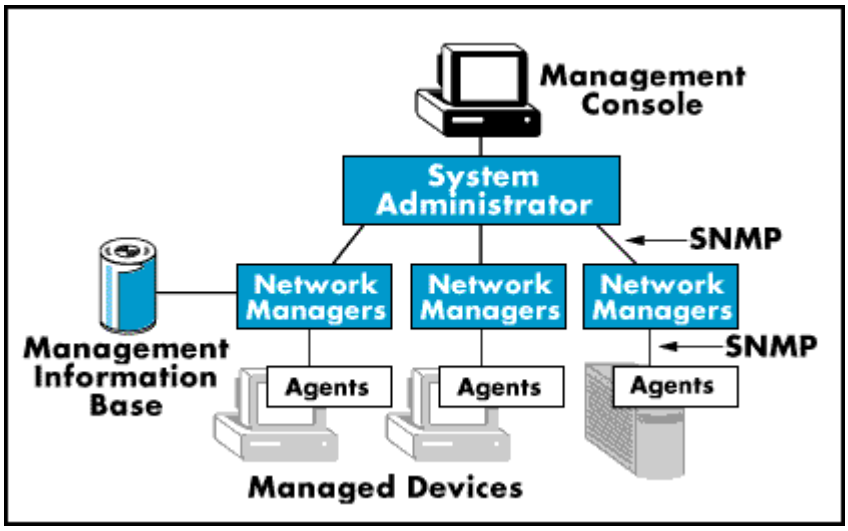


Figura A1.2 Interacción entre NMS, MIB y Agents, a través el protocolo SNMP

El software servidor SNMP puede comunicarse con los agentes SNMP y transferir o solicitar diferentes tipos de información. Generalmente, el servidor solicita las estadísticas del agente, incluyendo el número de paquetes que se manejan, el estado del dispositivo, las condiciones especiales que están asociadas con el tipo de dispositivo (como las indicaciones de que se terminó el papel o la pérdida de la conexión en un módem) y la carga del procesador.

El servidor también puede enviar instrucciones al agente para modificar las entradas de su base de datos MIB; además, puede enviar los límites o las condiciones bajo las cuales el agente SNMP debe generar un mensaje de interrupción para el servidor, como cuando la carga del CPU alcanza el 90 por ciento.

Las comunicaciones entre el servidor y el agente se llevan a cabo de una forma un tanto sencilla, aunque tienden a utilizar una notación abstracta para el contenido de sus mensajes. El agente nunca envía datos hacia el servidor a menos que se genere una interrupción o se haga una solicitud de sondeo. Esto significa que pueden existir algunos problemas constantes sin que el servidor SNMP sepa de ellos, simplemente porque no se realizó un sondeo ni se generó interrupción.

A.2.1.3 *Management Information Base MIB*

Ésta especifica los elementos de los datos que un anfitrión o un enrutador deben conservar y las operaciones permitidas en cada uno.

Cada dispositivo administrado por SNMP mantiene una base de datos que contiene estadísticas y otro tipo de información. Estas bases de datos se llaman Base de información sobre administración, o MIB. Las entradas de MIB tienen cuatro datos: un tipo de objeto, una sintaxis, un campo de acceso y un campo de estado. Las entradas MIB; generalmente siguen reglas estrictas para el formato, definidas por la Notación para Sintaxis Abstracta Uno (*Abstract Syntax Notation One, ASN. I*).

El tipo de objeto es el nombre de la entrada específica, generalmente a manera de un simple nombre. La sintaxis es el tipo de valor, como una cadena o un entero. No todas las entradas una MIB tienen un valor. El campo de acceso se utiliza para definir el nivel de acceso de la entrada, comúnmente está definida por los valores de sólo lectura, lectura-escritura, sólo escritura y no accesible. El campo de estado contiene una indicación de que la entrada de la MIB es obligatoria (lo que significa que el dispositivo administrado debe aplicar la entrada), opcional (el dispositivo administrado puede aplicar la entrada), u obsoleta (que no se utiliza).

Existen muchos tipos de MIB, los mas conocidos son los llamados MIB-1 y MIB-2. Las estructuras de ambos son diferentes. MIB-1 se utilizó a principios de 1988 y tiene 114 entradas en la tabla, las cuales están divididas en grupos. Para que un dispositivo administrado pueda ser compatible con MIB-1, debe manejar grupos que son aplicables a ésta. Por ejemplo, una impresora administrada no tiene que aplicar todas las entradas que traten con el Protocolo para *Gateway* Exterior (*Exterior Gateway Protocol EGP*), el cual generalmente lo aplican solamente los enrutadores y los dispositivos similares.

MIB-2 es una ampliación a MIB- 1 hecha en 1990, está conformada por 171 entradas que están divididas en diez grupos. Las adiciones amplían algunas de las entradas de los grupos básicos de MIB-1 y agregan tres nuevos grupos. Al igual que con MIB-1, un dispositivo SNMP que pretenda ser compatible con MIB-2 debe adaptar todos los grupos que son aplicables a ese tipo de dispositivo. Es posible encontrar muchos dispositivos que son compatibles con MIB-1 pero que no lo son con MIB-2.

El MIB para TCP/IP divide la información de la administración en 8 categorías:

Tabla A1.1 Categorías del MIB para TCP/IP

Categoría MIB	Incluye información sobre
system	Sistema operativo del host o del enrutador
Interfaces	Interfaz de red individual
Addr.trans.	Dirección de traducción (por ejemplo, transformación ARP)
ip	Software de Protocolo de Internet
icmp	Software de Protocolo de Mensajes de Control de Internet
tcp	Software de Protocolo de Transmisión de Internet
udp	Software de Protocolo de Datagrama de Usuario
egp	Software de Protocolo de Compuerta Exterior

A.2.1.4 Structure of Management Information SMI (Estructura de la información de administración)

Además del estándar MIB, el cual especifica variables de administración de red y sus significados, un estándar separado especifica un conjunto de reglas utilizadas para definir e identificar variables MIB. Las reglas se conocen como especificaciones *Structure of Management Information SMI*.

Para mantener los protocolos de administración de red simples; SMI establece restricciones a los tipos de variables permitidas en MIB, especifica las reglas para nombrar tales variables y crea reglas para definir tipos de variables.

Por ejemplo, el estándar SMI incluye definiciones de términos como *IpAddress* (definiéndolo como una cadena de cuatro octetos) y *Counter* (definida como un

entero en el rango de 0 a 2^{32}-1) y especifica que son los términos utilizados para definir variables MIB. Algo muy importante, las reglas en SMI describen cómo se refiere MIB a las tablas de valores (por ejemplo, la tabla de enrutamiento IP).

A.2.1.5 SNMP Protocolo Simple para Administración de Redes.

SNMP ha pasado por varias iteraciones. La versión más utilizada se llama SNMP v1. Por lo general, SNMP se utiliza como una aplicación cliente/servidor asincrónica, lo que significa que tanto el dispositivo administrado como el software servidor SNMP pueden generar un mensaje para el otro y esperar una respuesta, en caso de que haya que esperar una. Ambos lo empaquetan y manejan el software para red (como el IP) como lo haría cualquier otro paquete. SNMP utiliza UDP como un protocolo de transporte de mensajes. El puerto 161 de UDP se utiliza para todos los mensajes, excepto para los traps, que llegan el puerto 162 de UDP. Los agentes reciben sus mensajes del administrador a través del puerto UDP 161 del agente.

La ventaja fundamental de usar SNMP es que su diseño es simple por lo que su implementación es sencilla en grandes redes y la información de administración que se necesita intercambiar ocupa pocos recursos de la red. Además, permite al usuario elegir las variables que desea sondear sin mas que definir:

- El título de la variable.
- El tipo de datos de las variables.
- Si la variable es de solo lectura o también de escritura.
- El valor de la variable.

Otra ventaja de SNMP, es que en la actualidad es el sistema más extendido. La popularidad la ha conseguido al ser el único protocolo que existió en un principio y por ello casi todos los fabricantes de dispositivos de red diseñan sus productos para soportar SNMP.

La posibilidad de expansión es otra ventaja del protocolo SNMP; debido a su sencillez es fácil de actualizar.

El SNMP es especialmente estable ya que sus definiciones se mantienen fijas aun, cuando nuevos elementos de datos se añadan al MIB y se definan nuevas operaciones como efectos del almacenamiento de esos elementos.

A pesar de su extenso uso, SNMP tiene algunas desventajas. La más importante es que se apoya en UDP. Puesto que UDP no tiene conexiones, no existe contabilidad inherente al enviar los mensajes entre el servidor y el agente. Otro problema es que SNMP proporciona un solo protocolo para mensajes, por lo que no pueden realizarse el filtrado de mensajes. Esto incrementa la carga del software receptor. Además, SNMP casi siempre utiliza el sondeo en cierto grado, lo que ocupa una considerable cantidad de ancho de banda.

SNMP ofrece más que las dos operaciones que se han descrito:

Tabla A1.2 Operaciones permitidas por SNMP

Operación	Significado
get-request	Obtener un valor desde una variable específica
Get-next-request	Obtener un valor sin conocer su nombre exacto
get-response	Obtener repuesta a una operación *fetch*
set-request	Almacenar un valor en una variable específica
Trap	Réplica activada por un evento

Ahora bien, el protocolo SNMP no es perfecto y tiene sus fallos que se han ido corrigiendo.

La primera deficiencia de SNMP es que tiene grandes fallos de seguridad que puede permitir a intrusos acceder a información sobre la red. Todavía peor, estos intrusos pueden llegar a bloquear o deshabilitar terminales.

La solución a este problema se ha incorporado en la versión SNMPv2. Básicamente, se han añadido mecanismos para resolver:

- Privacidad de los datos, los intrusos no puedan tomar información que va por la red.
- Autenticación, para prevenir que los intrusos manden información falsa por la red.

- Control de acceso, que restringe el acceso a ciertas variables a determinados usuarios que puedan hacer caer la red.

El mayor problema de SNMP es que se considera tan simple que la información está poco organizada, lo que le hace no muy acertado para administrar las grandes redes de la actualidad. Esto se debe en gran parte a que SNMP se creó como un protocolo provisional, pero fue tan aceptado que ha sido difícil de reemplazar.

La versión SNMPv2 permite una separación de variables con más detalle, incluyendo estructuras de datos para hacer más fácil su manejo. Además SNMPv2 incluye 2 nuevas PDU's orientadas a la manipulación de objetos en tablas *get-bulk e inform*.

Así, aunque SNMP es un sistema de administración algo anticuado los cambios que ha venido de la mano de la versión 2 del mismo le han brindado nueva vida, ya que para SNMP v2 se intento mejorar los problemas de seguridad que presentaba SNMP v1, evitando que los intrusos observen el estado o la condición de los dispositivos administrados. Tanto la encriptación como la autenticación están soportadas por SNMP v2.

La versión 3 del protocolo (SNMPv3) posee la misma estructura básica de las versiones anteriores (SNMPv1 y SNMPv2), hecho que ha facilitando su desarrollo y avance, además de su comprensión. Lo que busca ésta nueva versión es cubrir las deficiencias de las otras dos versiones, enriqueciendo todos sus componentes arquitectónicos para ofrecer nuevas capacidades de seguridad y facilidades de administración.

Ésta nueva versión ha introducido nuevos mecanismos que permiten incrementar la seguridad a nivel de la capa IP, debido a que en éste nivel es probable que se pueda efectuar la captura de algún tipo de tráfico que circula por la red, además de esto, puede que el mismo sea utilizado y/o repetido, falsificando su dirección IP, originando con ésto, datagramas no confiables. Por ésta razón SNMPv3, ha hecho especial énfasis en el proceso de identificación de los usuarios (Autenticación) de la red, en mantener la integridad de los datos y en asegurar la confidencialidad de la información.

Adicionalmente a esto, la versión tres ha mejorado considerablemente su proceso administrativo, en el cual se han agregado nuevas aplicaciones que permiten el fácil manejo de toda la información y además agilizan considerablemente todo el proceso.

A.2.1.6 SNMP: Especificaciones del protocolo

Elementos de procedimiento

Se describirán a continuación las acciones que realiza una entidad de protocolo en una implementación SNMP. Se definirá “dirección de transporte” como una dirección IP seguida de un número de puerto UDP (Si se está usando el servicio de transporte UDP).

Cuando una entidad de protocolo envía un mensaje, realiza las siguientes acciones:

1. Construye la PDU apropiada como un objeto definido con el lenguaje ASN.1
2. Pasa ésta PDU, junto con un nombre de comunidad y las direcciones de transporte de fuente y destino, a un servicio de autenticación. Éste servicio generará en respuesta otro objeto en ASN.1
3. La entidad construye ahora un mensaje en ASN.1 usando el objeto que le ha devuelto el servicio de autenticación y el nombre de comunidad
4. Este nuevo objeto se envía a la entidad destino usando un servicio de transporte.

Cuando una entidad de protocolo recibe un mensaje, realiza las siguientes acciones:

1. Hace un pequeño análisis para ver si el datagrama recibido se corresponde con un mensaje en ASN.1. Si no lo reconoce, el datagrama es descartado y la entidad no realiza más acciones.
2. Observa el número de versión. Si no concuerda descarta el datagrama y no realiza más acciones.
3. Pasa los datos de usuario, el nombre de comunidad y las direcciones de transporte de fuente y destino al servicio de autenticación. Si es correcto, éste devuelve un objeto ASN.1. Si no lo es, envía una indicación de fallo. Entonces la entidad de protocolo puede generar una trap, descarta el datagrama y no realiza más acciones.

4. La entidad intenta reconocer la PDU. Si no la reconoce, descarta el datagrama. Si la reconoce, según el nombre de comunidad adopta un perfil y procesa la PDU. Si la PDU exige respuesta, la entidad iniciará la respuesta ahora.

Estructura de un PDU

Los datos que incluye una PDU genérica son los siguientes:

- *ErrorStatus:* Entero que indica si ha existido un error. Puede tomar los siguientes valores, que se explicarán posteriormente:

noError *(0)*
tooBig *(1)*
noSuchName *(2)*
badValue *(3)*
readOnly *(4)*
genErr *(5)*

- *ErrorIndex:* entero que en caso de error indica qué variable de una lista ha generado ese error.
- *VarBindList:* Lista de nombres de variables con su valor asociado. Algunas PDU quedan definidas sólo con los nombres, pero aún así deben llevar valores asociados. Se recomienda para éstos casos la definición de un valor NULL.

Tipos de PDU's

- *GetRequest-PDU y GetNextRequest-PDU*

Son PDU's que solicitan a la entidad destino los valores de ciertas variables. En el caso de *GetRequest-PDU* estas variables son las que se encuentran en la lista *VarBindList*; en el de *GetNextRequest-PDU* son aquellas cuyos nombres son sucesores lexicográficos de los nombres de las variables de la lista. Como se puede observar, *GetNextRequest-PDU* es útil para confeccionar tablas de información sobre un MIB.

Siempre tienen a cero los campos *ErrorStatus* y *ErrorIndex*. Son generadas por una entidad de protocolo sólo cuando lo requiere su entidad de aplicación SNMP.

Estas PDU's siempre esperan como respuesta un *GetResponse-PDU*.

- *SetRequest-PDU*

Ordena a la entidad destino poner a cada objeto reflejado en la lista *VarBindList* el valor que tiene asignado en dicha lista. Es idéntica a *GetRequest-PDU*, salvo por el identificador de PDU. Es generada por una entidad de protocolo sólo cuando lo requiere su entidad de aplicación SNMP. Espera siempre como respuesta una *GetResponse-PDU*.

- *GetResponse-PDU*

Es una PDU generada por la entidad de protocolo sólo como respuesta a *GetRequest-PDU*, *GetNextRequest-PDU* o *SetRequest-PDU*. Contiene la información requerida por la entidad destino o bien una indicación de error.

Cuando una entidad de protocolo recibe una *GetRequest-PDU*, una *SetRequest-PDU* o una GetNextRequest-PDU, sigue las siguientes reglas:

1. Si algún nombre de la lista (o el sucesor lexicográfico de un nombre en el caso de *GetNextRequest-PDU*) no coincide con el nombre de algún objeto en la vista del MIB al que se pueda realizar el tipo de operación requerido ("set" o "get"), la entidad envía al remitente del mensaje una *GetResponse-PDU* idéntica a la recibida, pero con el campo *ErrorStatus* puesto a 2 (*noSuchName*), y con el campo *ErrorIndex* indicando el nombre de objeto en la lista recibida que ha originado el error.
2. De la misma manera actúa si algún objeto de la lista recibida es un tipo agregado (como se define en el SMI), si la PDU recibida era una *GetRequest-PDU*.
3. Si se ha recibido una *SetRequest-PDU* y el valor de alguna variable de la lista no es del tipo correcto o está fuera de rango, la entidad envía al remitente una *GetResponse-PDU* idéntica a la recibida, salvo en que el campo *ErrorStatus* tendrá el valor 3 (*badValue*) y el campo *ErrorIndex* señalará el objeto de la lista que ha generado el error.
4. Si el tamaño de la PDU recibida excede una determinada limitación, la entidad enviará al remitente una *GetResponse-PDU* idéntica a la recibida, pero con el campo *ErrorStatus* puesto a 1 (*tooBig*).

5. Si el valor de algún objeto de la lista no puede ser obtenido (o alterado, según sea el caso) por una razón no contemplada en las reglas anteriores, la entidad envía al remitente una *GetResponse-PDU* idéntica a la recibida, pero con el campo *ErrorStatus* puesto a 5 (*genErr*), y el campo *ErrorIndex* indicando el objeto de la lista que ha originado el error.

Si no se llega a aplicar alguna de estas reglas, la entidad enviará al remitente una *GetResponse-PDU* de las siguientes características:

- Si es una respuesta a una *GetResponse-PDU*, tendrá la lista *varBindList* recibida, pero asignando a cada nombre de objeto el valor correspondiente.
- Si es una respuesta a una *GetNextResponse-PDU*, tendrá una lista *varBindList* con todos los sucesores lexicográficos de los objetos de la lista recibida, que estén en la vista del MIB relevante y que sean susceptibles de ser objeto de la operación "*get*". Junto con cada nombre, aparecerá su correspondiente valor.
- Si es una respuesta a una *SetResponse-PDU*, será idéntica a ésta, pero antes la entidad asignará a cada variable mencionada en la lista *varBindList* su correspondiente valor. Ésta asignación se considera simultánea para todas las variables de la lista.

En cualquiera de éstos casos, el valor del campo *ErrorStatus* es 0 (*noError*), igual que el de *ErrorIndex*. El valor del campo *requestID* es el mismo que el de la PDU recibida.

- *Trap-PDU*

Es el PDU que indica una excepción o *trap*. Es generada por una entidad de protocolo sólo a petición de una entidad de aplicación SNMP. Cuando una entidad de protocolo recibe una *Trap-PDU*, presenta sus contenidos a su entidad de aplicación SNMP.

Los datos que incluye una *Trap-PDU* son los siguientes:

- *enterprise:* tipo de objeto que ha generado la trap.
- *agent-addr:* dirección del objeto que ha generado la trap.
- *generic-trap:* entero que indica el tipo de trap.

Puede tomar los siguientes valores:

coldStart *(0)*

warmStart *(1)*

linkDown *(2)*

linkUp *(3)*

authenticationFailure *(4)*

egpNeighborLoss *(5)*

enterpriseSpecific *(6)*

- *specific-trap:* entero con un código específico.
- *time-stamp:* tiempo desde la última iniciación de la entidad de red y la generación del trap.
- *variable-bindings:* lista tipo varBindList con información de posible interés.

La siguiente es una breve descripción de los tipos de *trap* que se especifican en el campo *generic-trap* de un PDU:

- *Trap* de arranque frío *(COLDSTART Trap)*: La entidad de protocolo remitente se está re-inicializando de forma que la configuración del agente o la implementación de la entidad de protocolo puede ser alterada. Por ejemplo, un *trap* podría ser mandado por un enrutador que recién ha sido configurado y requiere reiniciarse para que los cambios tengan efecto.
- *Trap* de arranque en caliente *(WARMSTART TRAP)***:** La entidad de protocolo remitente se está reinicializando de forma que ni la configuración del agente ni la implementación de la entidad de protocolo se altera.
- *Trap* de conexión perdida *(LINKDOWN TRAP)***:** La entidad de protocolo remitente reconoce un fallo en uno de los enlaces de comunicación representados en la configuración del agente. Éste *Trap-PDU* contiene como primer elemento de la lista variable-bindings el nombre y valor de la interfaz afectada. Por ejemplo, una interfaz en un enrutador que se ha dañado o un archivo en un servidor con un NIC fallo.

- *Trap* de conexión establecida *(LINKUP TRAP)***:** La entidad de protocolo remitente reconoce que uno de los enlaces de comunicación de la configuración del agente se ha establecido. El primer elemento de la lista variable-bindings es el nombre y el valor de la interfaz afectada.
- *Trap* de fallo de autenticación *(AUTHENTICATION FAILURE TRAP)***:** La entidad de protocolo remitente es la destinataria de un mensaje de protocolo que no ha sido autentificado.
- *Trap* de pérdida de vecino EGP *(EGPNEIGHBORLOSS TRAP)***:** Un vecino EGP con el que la entidad de protocolo remitente estaba emparejado ha sido seleccionado y ya no tiene dicha relación. El primer elemento de la lista variable-bindings es el nombre y el valor de la dirección del vecino afectado.
- *Trap* específica *(ENTERPRISESPECIFIC TRAP)***:** La entidad remitente reconoce que ha ocurrido algún evento específico. El campo *specific-trap* identifica qué *trap* en particular se ha generado.

A.2.2 SNMPv2

Uno de los propósitos del modelo administrativo para SNMPv2 es definir como la infraestructura administrativa se aplica para llevar a cabo una administración de red efectiva en diversas configuraciones y entornos.

El modelo implica el uso de diferentes identidades en el intercambio de mensajes. De ésta forma, representa abandonar el basado en comunidades del SNMPv1 original. Al identificar sin ambigüedad al emisor y al receptor de cada mensaje, ésta nueva estrategia mejora el esquema histórico de comunidades ya que permite un diseño del control de acceso a los datos más conveniente así como el empleo de protocolos de seguridad asimétricos(con llave pública) en el futuro.

A.2.2.1 PDUs

Ésta versión del protocolo SNMP incluye todos lo PDUs de la versión SNMPv1 pero incluye dos nuevas PDUs

- *GetBulkRequest*

El *GetBulkRequest* está definido en el RFC 1448 y forma por tanto parte de las operaciones del protocolo. Un mensaje *GetBulkRequest* se genera y se transmite como una petición de una aplicación SNMPv2. Su fin es solicitar la transferencia de una cantidad de datos potencialmente elevada, incluyendo, sin que ello le condicione, la rapidez y eficiencia en la recuperación de grandes tablas. GetBulkRequest es más eficiente que GetNextRequest en la recuperación de grandes tablas MIB de objetos.

- *InformRequest*

Un mensaje *InformRequest* se genera y se transmite como una solicitud de una aplicación (de una entidad *manager* SNMPv2) que desea notificar a otra aplicación, (que se ejecuta también en un *manager* SNMPv2) información en el ámbito del MIB(*MIB view*) para un entorno local a la aplicación que envía el mensaje. El paquete se utiliza para indicar al *manager* del otro entorno de la información accesible en el emisor. (comunicación *manager-manager* a través de los límites del entorno). Las dos primeras variables en la lista de asociaciones de variables de un mensaje *InformRequest* son *sysUpTime.0* y *snmpEventID.i* respectivamente. Les pueden seguir otras variables.

A.2.2.2 Entidad SNMPv2

Una entidad SNMPv2 es un proceso real que realiza operaciones de administración de red mediante la generación y/o respuesta a mensajes SNMPv2. Todas las posibles operaciones de una entidad se pueden restringir a un subconjunto de las operaciones que puede efectuar el entorno de administración("*SNMPv2 Party"*).

Las principales amenazas contra las que el protocolo SNMPv2 aporta protección son:

- Modificación de información
- Enmascaramiento
- Modificación del flujo de mensajes
- Intrusión en la información

Los siguientes servicios de seguridad proporcionan medidas contra las anteriores amenazas:

- Integridad de los datos

La proporciona el algoritmo de condensación de mensajes MD5. Se calcula un resumen o extracto de 128 bits de la porción indicada del mensaje SNMPv2 y se incluye como parte del mensaje enviado al receptor.

- Autentificación del origen de los datos

A cada mensaje se le añade un prefijo con un valor secreto que comparten el emisor del mensaje y el receptor, antes de calcular el extracto.

- *Replay* o retardo del mensaje

En cada mensaje se incluye un sello de tiempo,

- Confidencialidad de los datos

La proporciona el protocolo simétrico de privacidad que encripta una porción adecuada del mensaje de acuerdo con una llave secreta conocida sólo por el emisor y el receptor.

Éste protocolo se usa conjuntamente con el algoritmo simétrico de encriptación, en el modo de encadenamiento de cifrado de bloques, que forma parte del DES(*Data Encryption Standard*). La parte designada del mensaje se encripta y se incluye como parte el mensaje enviado el receptor.

A.2.3 SNMPv3

La principal novedad introducida en la versión 3 del protocolo SNMP es la modularidad. En dicha versión una entidad SNMP se considera compuesta por un motor y varias aplicaciones. A su vez el motor se divide en cuatro módulos: *dispatcher*, subsistema de proceso de mensajes, subsistema de seguridad y subsistema de control de acceso.

De ésta manera, la versión SNMPv3 se independizan los mecanismos utilizados para la seguridad (autentificación y privacidad) y para el control de acceso; utilizados en las versiones anteriores. De este modo, una misma entidad puede utilizar diferentes modelos de seguridad y control de acceso simultáneamente, lo que incrementa notablemente la flexibilidad y la interoperabilidad.

Se define un modelo estándar para seguridad basada en usuarios, USM (*User Security Model*) y otro para control de acceso basado en vistas, VACM (*View-based Access Control Model*). Se aprovechan los conceptos definidos en las versiones previas y al mismo tiempo la modularidad del protocolo permite la introducción de futuros modelos independientes de los actuales.

SNMPv3 es un protocolo de manejo de red interoperable, que proporciona seguridad de acceso a los dispositivos por medio de una combinación de autenticación y encripción de paquetes que trafican por la red.

Las capacidades de seguridad que SNMPv3 proporcionan son:

- Integridad del Mensaje: Asegura que el paquete no haya sido violado durante la transmisión.
- Autenticación: Determina que el mensaje proviene de una fuente válida.
- Encripción: Encripta el contenido de un paquete como forma de prevención.

SNMPv3 proporciona tanto modelos como niveles de seguridad. Un modelo de seguridad es una estrategia de autenticación que es configurada para los usuarios y los grupos en los cuales éstos residen. Los niveles de seguridad se refieren al nivel permitido a un usuario dentro de un modelo de seguridad.

La combinación de ambas cosas determinará que mecanismo de seguridad será el empleado cuando se maneje un paquete SNMP.

Es importante resaltar que SNMPv3 no es un reemplazo de SNMPv1 ó SNMPv2. SNMPv3 define una serie de nuevas capacidades a ser utilizadas en conjunto con SNMPv2 (preferiblemente) y SNMPv1. Es posible afirmar que "SNMPv3 es SNMPv2 sumándole administración y seguridad".

A.2.3.1 Arquitectura Utilizada

SNMPv3 incluye tres servicios:

- Autenticación.
- Privacidad.
- Control de Acceso.

Para dar éstos servicios de una forma eficiente, SNMPv3 introduce un nuevo concepto llamado "*Principal*", el cual no es más que una entidad en la que, la mayor parte de los servicios son proporcionados ó procesados. Un *Principal* puede actuar en forma individual en un rol particular, como aplicación o conjunto de aplicaciones ó bien como una combinación de todos ellos. Esencialmente un *Principal* opera desde una estación administradora y envía comandos SNMP hacía los agentes. La identidad del *Principal* y la del agente juntos determinan las capacidades de seguridad que serán invocadas, incluyendo autenticación, privacidad y control de acceso.

Es posible definir SNMPv3 en una forma modular. Cada Entidad SNMP incluye un simple *SNMP Engine*. Un *SNMP Engine* implementa funciones para enviar / recibir, autenticar y encriptar / desencriptar mensajes, además de controlar el acceso a los objetos manejados. Estas funciones son proporcionadas como servicios para una o más aplicaciones que son configuradas con el *SNMP Engine* para así formar la *SNMP Entity*. El papel del *SNMP Entity* es determinado por módulos que están implementados en esa entidad.

La estructura modular de las especificaciones permiten definir diferentes versiones de cada módulo, lo que hace posible que se puedan tomar ciertas capacidades y aspectos de SNMP sin la necesidad de ir a una nueva versión y tomar el estándar completo (por ejemplo SNMPv4), de éste modo se mantiene la coexistencia de varias versiones.

Elementos de un *SNMP Entity*

- *SNMP Engine*
- Despachador: Permite la concurrencia de múltiples versiones de mensajes SNMP en el SNMP Engine. Es responsable de:

    1) Aceptar los PDUs de las aplicaciones para que luego sean transmitidos a través de la red y de enviar los PDUs entrantes a las aplicaciones.
    2) Pasar los PDUs que salen al Subsistema de Procesamiento de Mensajes para que sean preparados y pasar los PDUs entrantes al mismo subsistema para que sean extraídos.
    3) Enviar y recibir mensajes SNMP sobre la Red.

- Subsistema de Procesamiento de Mensajes: Responsable de preparar mensajes para enviar y de extraer los datos de la información recibida.
- Subsistema de Seguridad: Proporciona los servicios de autenticación y privacidad del mensaje. Éste subsistema potencialmente contiene múltiples modelos de seguridad.
- Subsistema de Control de Acceso: Proporciona un conjunto de servicios de autorización que una aplicación puede utilizar para el chequeo de acceso de los mensajes.

•

A.2.3.2 Aplicaciones:

- Generador de Comandos*:* Recibe los PDUs SNMP *Get*, *GetNext*, *GetBulk* ó *SetRequest* y procesa la respuesta a una requisición que ha sido generada.
- Generador de Respuestas*:* Recibe los PDUs SNMP *Get*, *GetNext*, *GetBulk* ó *SetRequest* destinados al sistema local y luego desarrolla la operación de los protocolos apropiados, usando control de acceso y genera un mensaje de respuesta para ser enviada a la estación que hizo el requerimiento.
- Creador de Notificación*:* Monitorea un sistema para una condición o evento particular y genera un mensaje de *Trap* ó *Inform* basados en ellos. Un originador de Notificación debe de tener un mecanismo para determinar donde enviar el mensaje y cual es la versión de SNMP y los parámetros de seguridad a usar cuando se envíe el mensaje.
- Receptor de Notificación*:* Espera por los mensajes de notificación y genera respuestas cuando un mensaje recibido contenga un PDU tipo *Inform*.
- *Proxy Fowarders:* Adelanta los mensajes SNMP. Es una aplicación Opcional.

A.2.3.3 Procesamiento del Mensaje

El RFC2272 define en forma general el modelo para el procesamiento del mensaje en SNMPv3. Éste modelo es responsable de aceptar los PDUs del Despachador, encapsularlo entonces en mensajes, e invocar el USM (Modelo de Seguridad del Usuario) para insertar los parámetros relacionados con la seguridad en el encabezado del mensaje. El modelo de procesamiento del mensaje también se encarga de aceptar mensajes entrantes, invocar el USM para procesar los parámetros de seguridad que se encuentran en el encabezado del mensaje y entrega el PDU al Despachador.

En lo que a la estructura del mensaje se refiere. Los primeros cinco campos son generados por el modelo de procesamientos de mensajes entrantes / salientes. Los siguientes seis campos muestran los parámetros de seguridad usados por el USM.

Finalmente el PDU, junto con el *ContextEngineID* y *ContextName* constituyen el PDU a ser procesado.

Los siguientes son los campos del PDU

- *msgVersion*: Configurado para SNMPv3.
- *MsgID*: Un identificador único usado entre dos entidades SNMP para coordinar los mensajes de requisición y respuesta. Su rango es de 0 a 231 – 1.
- *MsgMaxSize*: Se refiere al tamaño máximo de un mensaje en octetos soportado por el que envía, con un rango de 484 a 231 – 1. Éste es el máximo tamaño que una entidad que envía puede aceptar de otra *SNMP Engine*.
- *MsgFlag*: Un arreglo de octetos que contiene tres banderas en los tres bits menos significativos:
- *ReportableFlag*: Utilizada igual a 1 para los mensajes enviados conteniendo una requisición o un *Inform*, e igual a 0 para mensajes conteniendo una Respuesta, *Trap* ó Reporte PDU.
- *PriorFlag y AuthFlag*: Son configuradas por el que envía para indicar el nivel de seguridad que le fue aplicado al mensaje.
- *MsgSecurityModel*: Es un identificador en el rango de 231 – 1 que indica que modelo de seguridad fue utilizado por el que envió el mensaje, para que así el receptor tenga conocimiento de que modelo de seguridad deberá usar para procesar el mensaje. Existen valores reservados:

  1 para SNMPv1

  2 para SNMPv2

  3 para SNMPv3.

Los seis campos siguientes relacionados con los parámetros de seguridad y generados por la USM incluyen:

- *MsgAuthoritativeEngineID*: Se refiere al valor de la fuente de un *Trap*, Response ó Report y al destino de un *Get, GetNext, GetBulk, Set ó Inform.*
- *MsgAuthoritativeEngineTime*: Es un valor entero en el rango de 231 – 1 que representa el número de segundos desde que el *snmpEngineBoots* del *SNMP Engine* fue incrementado.

- *MsgUserName*: Usuario principal desde el cual el mensaje ha sido enviado.
- *MsgAuthenticationParameters*: Parámetro de autenticación. Si la autenticación no es utilizada, éste valor es nulo. Éste parámetro es generado usando un algoritmo llamado HMAC.
- *MsgPrivacyParameters*: Parámetro de privacidad; si la privacidad no es utilizada, éste valor es nulo. Éste parámetro es generado usando un algoritmo llamado DES.

A.2.3.4 La Clave de Autenticación

El mecanismo de autenticación en SNMPv3 asegura que un mensaje recibido fue en realidad transmitido por la entidad principal fuente que aparece en el identificador del encabezado del mensaje. En adición, éste mecanismo asegura que el mensaje no fue alterado durante la transmisión y que no fue de alguna manera retardado ó capturado y luego reenviado por otra fuente.

En el proceso de autenticación cada *Engine* de SNMP, principal y remota que desee comunicarse deberá compartir una llave secreta de autenticación. La entidad que envía proporciona autenticación incluyendo en el mensaje un código. Éste código es una función del contenido del mensaje, de la identidad del *Engine SNMP* y del Principal, del tiempo de transmisión y de la llave secreta que sólo deberá de ser conocida por el que envía y el que recibe. La llave secreta debe ser configurada inicialmente por el administrador de la red, quien cargará estas llaves en las bases de datos de los agentes y los administradores. Esto puede hacerse manualmente ó utilizando una forma segura de transferencia de datos.

Cuando la entidad receptora recibe el mensaje, ésta utiliza la misma llave secreta para calcular el código de autenticación del mensaje. Si el código calculado en el lado receptor coincide con el valor incluido en el mensaje enviado, entonces el receptor conocerá que el mensaje fue originado de un administrador autorizado y que el mismo no fue alterado durante su transmisión.

A.2.3.5 Modelo de Control de Acceso VACM (View-Based Access Control Model)

Con el Modelo de Control de Acceso se hace posible configurar los agentes para proporcionar diferentes niveles de accesos a los MIB y a los diferentes adminstradores. Un agente puede restringir el acceso a sus MIBs a un administrador en particular de dos formas:

- Pueden restringir acceso sólo a ciertas porciones del MIB.
- El agente puede limitar la operación que un administrador puede usar en ciertas porciones del MIB.

El control de acceso a ser usado por un agente para cada administrador deberá ser pre-configurado. Esencialmente consiste de una tabla que detalla los privilegios de accesos de varios administradores autorizados. A diferencia de la autenticación la cual es hecha por el usuario, en el control de acceso es hecho por grupo, dónde un grupo puede estar compuesto por una serie de usuarios.

A.2.3.6 Transporte.

Pueden usarse mensajes de SNMP con una gran variedad de colecciones protocolares, dentro de las cuales se pueden nombrar IPX y UDP. Aunque se definen varías categorías se seleccionó UDP como el transporte preferido, ya que es simple y se puede implementar con poco código. Además de esto es la opción más fiable en caso de que el dispositivo esté dañado o sobrecargado.

A.2.3.7 Arquitectura, seguridad y administración.

La arquitectura de SNMPv3, se basa principalmente en el mejoramiento de la seguridad y de la administración, por éste hecho está enfocado en los siguientes puntos:

a. Los Instrumentos y Aplicaciones.

b. Las entidades (Proveedores de servicio como los instrumentos en agentes y gerentes).

c. Las Identidades (usuarios de Servicio)

d. La información de dirección, incluyendo apoyo para múltiple contextos lógicos.

A.2.3.8 Coexistencia y transición de SNMPv3.

SNMPv3 permite la transición y coexistencia de los diferentes documentos MIB generados en la versión 1 (SNMPv1) y la versión 2 (SNMPv2). Por otra parte, también permite la coexistencia de las entidades que soportan las diferentes versiones de SNMP en una red multi-lenguaje y además el procesamiento de operaciones protocolares en los múltiples lenguajes implementados.

En el modelo de procesamiento de mensajes de SNMPv1 y el Modelo de Seguridad de ésta misma versión, existen mecanismos para adaptar estas versiones y las de SNMPv2 al Modelo de Control de Acceso de Vista (*VACM- View Based Access Control Model*). El VACM puede simultáneamente asociarse con un solo instrumento de implementación, el cual puede procesar múltiples mensajes y múltiples modelos de seguridad.

A.2.3.9 Servicios de seguridad de SNMPv3

Tipos de servicios de seguridad.

Los servicios de seguridad que ofrece el modelo de SNMPv3 son los siguientes:

a. Integridad de los Datos.

b. Prevenir la alteración y/o destrucción de los datos por entes no autorizados.

c. Autenticación del origen de los datos.

d. Comprobar el origen de los datos exigiendo la identidad del usuario. Corrobora que los datos estarán en el lugar donde se originó la petición.

e. Confidencialidad de los datos.

f. Garantizar que los datos no serán accesados por usuarios no autorizados, entidades o procesos desconocidos.

g. Módulo de Tiempo (*Timeliness*) y protección de repetición limitada.

Permite proteger un mensaje de un determinado retraso e impide la repetición del mismo.

Organización del módulo de seguridad.

Los protocolos de seguridad están divididos en tres módulos diferentes y cada uno tiene sus responsabilidades específicas:

a. Módulo de Autenticación. Está encargado de la Integridad y de la Autenticación del origen de los datos. Cuando se efectúa el proceso de autenticación el mensaje completo es chequeado para garantizar su integridad en el módulo de autenticación.

b. Módulo de Tiempo (*Timeliness*). Ofrece protección contra el retraso o repetición del mensaje. El chequeo de tiempo solo se realiza si se ha concluido el proceso de autenticación.

e. Módulo de Reserva. Ofrece protección contra el descubrimiento de los datos, garantizando la confidencialidad de los mismos. En éste caso se necesita también que el mensaje sea autenticado.

A.2.3.10 Protección contra la repetición del mensaje, retraso y redirección.

Con el objeto de ofrecer protección contra el retraso, la repetición y la redirección de los mensajes, SNMP utiliza sus instrumentos y establece una serie de mecanismos, los cuales se resumen a continuación:

- Instrumento SNMP de autoridad. SNMP asigna uno de sus instrumentos para controlar el retraso, la repetición y la redirección, el cual está involucrado en cada proceso de comunicación y constituye o representa la autoridad. Cuando un mensaje de SNMP está en espera de una respuesta, el receptor de tales mensajes es autorizado para recibirla.
- Mecanismos. Los mecanismos utilizados contra la repetición del mensaje, retraso y redirección son los siguientes:

Para proteger un mensaje de la amenaza de repetición o retraso, se utiliza un juego de indicadores de tiempo (*Timeliness*) en el instrumento de autoridad de SNMP. El indicador de tiempo se utiliza para determinar si un mensaje fue recibido en forma reciente. Un instrumento de SNMP puede evaluar dichos indicadores y asegurarse que un mensaje recibido es más o menos reciente que otro que proviene del mismo origen. Éstos mecanismos detectan e identifican los mensajes que no son generados recientemente.

- Verificación de Mensajes enviados por un instrumento SNMP.

Cada uno de los mensajes enviados por un instrumento de autoridad, que en éste caso sería el Remitente, incluye una identificación única (identificador), la cual está asociada con su destinatario. Cada uno de los mensajes son chequeados de forma tal que se asegure que están en el destino correcto. Ningún instrumento de autoridad puede transferir el mensaje o ser reemplazado por otro instrumento de autoridad, pero puede suceder que lo haga un instrumentos no autoritario, al cual se transfieren también los datos del SNMP autoritario, sin embargo esto no se considera una amenaza ya que la respuesta será descartada por el módulo de procesamiento de mensajes, porque será un mensaje de demanda no excelente.

- Identificación de mensajes generados no recientemente.

Un juego de indicadores de tiempo es incluido en el mensaje, mostrando el tiempo de generación del mismo. Los mensajes que posean indicadores de tiempo no recientes, son considerados no auténticos, por lo que los instrumentos SNMP suspenden cualquier respuesta hasta que no se normalice la transmisión o no exista una demanda excelente. El receptor de un mensaje (destinatario) verifica la identificación del instrumento de autoridad y se asegura que verdaderamente ese es su destino final.

A.2.4 CMIP

A.2.4.1 Introducción al CMIP

Tras la aparición de SNMP como protocolo de administración de red, a finales de los 80, gobiernos y grandes corporaciones plantearon el Protocolo Común de Administración de Información CMIP (*Common Management Information Protocol*) que se pensó que podría llegar a ser una realidad debido al alto presupuesto con que contaba. En cambio, problemas de implementación han retrasado su expansión de modo que solo está disponible actualmente de forma limitada.

CMIP fue diseñado teniendo en cuenta a SNMP solucionando los errores y fallos que tenía SNMP y volviéndose un administrador de red mayor y más detallado.

Su diseño es similar a SNMP por lo que se usan PDU's (Protocol Data Unit) como variables para supervisar la red.

En CMIP las variables son unas estructuras de datos complejas con muchos atributos, que incluyen:

- **Variables de atributos:** representan las características de las variables.
- **Variables de comportamiento:** qué acciones puede realizar.
- **Notificaciones**: la variable genera una indicación de evento cuando ocurre un determinado hecho.

Tiene cinco puntos que son considerados importantes para una buena administración.

- Detección de fallas
- Administración de configuración
- Análisis del rendimiento
- Control de seguridad
- Conteo

A.2.4.2 Administracion en OSI

Como CMIP es un protocolo de administración de red implementado sobre OSI conviene introducir el marco de trabajo OSI en lo que respecta a administración, ya que será la base para CMIP. La administración OSI posibilita supervisar y controlar los recursos de la red que se conocen como "objetos administrados". Para especificar la estandarización de la administración de red se determina: Modelo o grupo de modelos de la inteligencia de administración, hay 3 principales:

- **Modelo de organización** que describe la forma en que las funciones de administración se pueden distribuir administrativamente. Aparecen los dominios como particiones administrativas de la red.
- **Modelo funcional** describe las funciones de administración (de fallos, de configuración, de contabilidad, de seguridad...) y sus relaciones.

- **Modelo de información** que provee las líneas a seguir para describir los objetos administrados y sus informaciones de administración asociadas. Reside en el MIB (Management Information Base).

A.2.4.3 Fundamentos de CMIP

CMIP es un protocolo de administración de red que se implementa sobre el modelo de Interconexión de Redes Abiertas OSI (*Open Systems Interconnection*) que ha sido normalizado por la ISO (*International Organization for Standardization's*) en sus grupos de trabajo OIW (*OSI Implementors Workshop*) y ONMF (*OSI Network Management Forum*). Además existe una variante del mismo llamado CMOT que se implementa sobre un modelo de red TCP/IP.

En pocas palabras, CMIP es una arquitectura de administración de red que provee un modo de que la información de control y de mantenimiento pueda ser intercambiada entre un administrador (*manager*) y un elemento remoto de red. En efecto, los procesos de aplicación llamados administradores (*managers*) residen en las estaciones de administración mientras que los procesos de aplicación llamados agentes (agents) residen en los elementos de red.

CMIP define una relación igual a igual entre el administrador y el agente incluyendo lo que se refiere al establecimiento y cierre de conexión, y a la dirección de la información de administración. Las operaciones CMIS (*Common Management Information Services*) se pueden originar tanto en administradores como en agentes, permitiendo relaciones simétricas o asimétricas entre los procesos de administración. Sin embargo, la mayor parte de los dispositivos contienen las aplicaciones que sólo le permiten hacer de agente.

Un sistema CMIP debe implementar una serie de protocolos de los cuales el CMISE (*Common Management Information Service Element*) es el que trabaja mano a mano con CMIP: todas las operaciones de administración de red que crea CMISE el CMIP las mapea en una operación en el CMIP remoto.

A.2.4.4 Protocolos de aplicación en CMIP

Para comunicarse entre sí dos entidades de aplicación pares del administrador y del agente se utilizan APDU's (*Application Protocol Data Units*). Como hemos visto, CMIP está compuesto de los protocolos OSI que siguen:

- ACSE (*Association Control Service Element*)
- ROSE (*Remote Operation Service Element*)
- CMISE (*Common Management Information Service Element*)

A.2.4.5 Administración PROXY

En nuestro contexto un *proxy* es un administrador intermediario habilitado para realizar acciones en nombre de otro administrador. Si el dispositivo administrado no soporta CMIP, todo lo relativo a administración que vaya a él se re dirige al *proxy* el cual le hará llegar la información adaptada al protocolo que soporte, y viceversa.

A.2.4.6 Ventajas del CMIP

El principal beneficio que aporta el protocolo CMIP es que no sólo se puede enviar información de administración de o hacia un terminal, sino que es posible desarrollar tareas que serían imposibles bajo SNMP. Por ejemplo, si un terminal no puede encontrar un servidor de ficheros en un tiempo predeterminado, CMIP notifica el evento al personal adecuado. En SNMP el usuario tendría que guardar el número de intentos de acceso al servidor mientras que en CMIP de esto se encarga el propio protocolo.

CMIP soluciona varios de los fallos de SNMP. Por ejemplo, tiene incluidos dispositivos de administración de la seguridad que soportan autorizaciones, control de acceso, contraseñas... Como resultado de la seguridad que de por sí proporciona CMIP no necesita de posteriores actualizaciones.

Otra ventaja de CMIP es que haya sido creado no solo por gobiernos sino que también por grandes empresas, en los que puede tener en el futuro un mercado fiel.

A.2.4.7 Desventajas del CMIP

Si todo lo dicho hace a CMIP tan bueno, cualquiera se puede hacer la pregunta del por qué no se usa. La respuesta es que CMIP significa también desventajas: CMIP requiere 10 veces más recursos de red que SNMP. En otras palabras, muy pocas redes de la actualidad son capaces de soportar una implementación completa de CMIP sin grandes modificaciones en la red (muchísima más memoria y nuevos protocolos de agente). Por eso mucha gente piensa que CMIP está destinado al fracaso.

La única solución es disminuir el tamaño de CMIP cambiando sus especificaciones. Así han aparecido varios protocolos que funcionan con la base de CMIP con menos recursos, pero todavía no ha llegado el momento de prescindir del tan extendido SNMP.

Otro problema de CMIP es su dificultad de programación: existe tal cantidad de variables que solo programadores muy habilidosos son capaces de sacarles todo su potencial.

A.2.5 RMON *Remote Network Monitoring*.

El estándar MIB RMON fue definido primeramente por el RFC 1271 en 1991 y actualizada recientemente en el RFC 1757. El propósito de RMON es extender MIB-II de manera que pueda proveer un mecanismo para la captura de información no atendida de datos más detallados que los provistos pro el los grupos MIB-II

El MIB RMON puede ser implementado directamente en las aplicaciones de administración y no se requiere SNMPv2.

Las especificaciones de RMON definen funciones de supervisión estándares e interfaces para comunicarse entre dispositivos basados en SNMP. RMON proporciona a las redes la capacidad de proveer una forma efectiva y eficiente de supervisar subredes mientras se reduce la carga en agentes y estaciones de administración.

El MIB RMON usa un agente conectado a una red *broadcast* para registrar las estadísticas de tráfico. Típicamente, un agente es solo un responsable de la administración de la información y contiene tablas de control y de datos. Las tablas de control contienen parámetros de control que especifican las estadísticas que quieres accesar. Las tablas de datos contienen estadísticas que el agente obtiene.

Así, el estándar RMON es un desprendimiento de SNMP, que consiste en definir un conjunto de variables (u objetos, en el lenguaje de SNMP) que recopilan información estadística del tráfico que fluye a través de los conmutadores. Estas variables, forman parte de los llamados “grupos” en RMON versión 1 y en RMON versión2

La diferencia entre las versiones consiste en que RMON 1 recopila estadísticas de tramas físicas, es decir en las capas 1 y 2 del modelo OSI. Mientras que RMON 2 lo hace respecto a los datagramas de protocolos de nivel 3 del modelo OSI; y permite el supervisión de las capas 3 a 7.

Así, cualquier software de administración o analizador de tráfico que tenga la capacidad de generar solicitudes de SNMP hacia el dispositivo, puede pedir que el mismo le proporcione el contenido de estas variables y representar estas estadísticas en forma de gráficos o tablas, en la pantalla de la PC. Los grupos de RMON son los siguientes:Los grupos de RMON son los siguientes:

Tabla A1.3 Grupos RMON (Capas física y de datos)

Grupo	Descripción
Statistics	Muestra estadísticas para el segmento de LAN completo, no relacionado con hosts individuales Ej.: Paquetes totales, errores, broadcasts, distribución de paquetes, etc
History	Muestra estadísticas basándose en el tiempo para un segmento completo de LAN. Ej.:(tráfico, errores, etc)
Alarm	Supervisa las estadísticas del MIB, disparar acciones si se supera el umbral establecido y no se toman mas acciones hasta que el valor cae por debajo del valor de recupero
Event	Tabla de todos los eventos generados por el agente RMON, que pueden ser desencadenados por otros grupos RMON, tales como *Alarm* y *Packet Filter*. Cuando un evento se dispara, un numero de acciones tiene lugar (Ej.: envío de un *trap*, disparar una sesión de captura, etc.)
Host	Brinda estadísticas basadas en direcciones MAC, NO direcciones de red (¿Quién está conversando?). Ej.: Número de paquetes, bytes, broadcasts, errores por cada estación.
HostTopN	Rankea los host más activos, basado en tráfico o errores
Matrix	Brinda estadísticas basadas en pares de comunicación entre direcciones MAC Ej.: Número de paquetes enviados entre la estación A y el server B.
Filter	Permite establecer las condiciones contra parámetros existentes en los paquetes, ya sea para capturarlos como para supervisarlos
Packet Capture	Captura paquetes en un buffer interno acorde a los parámetros definidos en el grupo Filter. Es particularmente útil en condiciones de error.

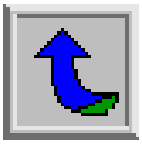
Tabla A1.4 Grupos RMON2 (Capa de red y aplicaciones)

Grupo	Descripción
Protocol Directory	Define que protocolos son capaces de ser reconocidos y contabilizados por RMON2
Protocol Distribution	Contabiliza el numero de paquetes y bytes que han sido enviados por los protocolos definidos en el grupo anterior
Address Translation Map	Provee un mapa entre las direcciones de capa 3 (red) y las direcciones físicas MAC de capa 2 (enlace)
Network Layer Host	Lista las direcciones de red y asocia los paquetes y bytes de entrada y salida de cada uno.
Network Layer Matrix	Mantiene control del número de bytes y paquetes para cada conversación detectada por los agentes
Application Layer Host	Mantiene estadísticas respecto a las aplicaciones derivadas de la tabla de capa de red.
Application Layer Matrix	Mantiene contadores de paquetes y bytes para cada conversación de capa de red basada por protocolo.
User Defined History	Periódicamente muestrea objetos MIB definidos por el usuario
Probe Configuration	Objetos de configuración de dispositivos (varios)
RMON Conformity	Requerimientos de cumplimiento con la MIB de RMON2

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

Ciertos fabricantes están cooperando para el desarrollo de extensiones particulares para ciertas clases de productos y la administración remota de dispositivos, basadas en RMON (*Remote MONitoring*), normas RFC 1757 (antes 1271) para Ethernet y RFC 1513 para *Token Ring* del IETF (*Internet Engineering Task Force*), que incluyen sobre unos 200 objetos clasificados en 9 grupos: Alarmas, Estadísticas, Historial, Filtros, Ordenadores, N Principales, Matriz de Tráfico, Captura de Paquetes y Sucesos. Con RMONv2 se decodifican paquetes a nivel 3 de OSI, lo que implica que

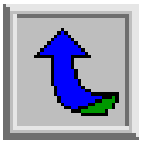
el tráfico puede supervisarse a nivel de direcciones de red (puertos de los dispositivos) y aplicaciones específicas.



ANEXOS

ANEXO 1. CAPTURA DE PANTALLA DE LA CONFIGURACION DE LA SONDA WANPROBE

```
***** Cisco SwitchProbe  V4.7.0 (Build 125) *****


Interface number : 1

[1]  Change IP Address                  10.1.200.198
[2]  Change Net Mask                    255.255.255.0
[3]  Change Default Gateway Address     10.1.200.190
[4]  Change Read Community              public
[5]  Change Write Community             private
[8]  Select Interface                   ETHERNET
[9]  Change Server Address              10.1.200.201
[10] Upgrade Software
[11] Enter Command-line mode
[12] Reset Agent

[31] Go to Next Page

          Enter your response or Enter "exit" to logout


Selection#:
Selection#: 8

Select Interface :

[1]  ETHERNET                MODE = MANAGE + MONITOR
[2]  SERIAL                  MODE = MANAGE
[3]  WAN                     MODE = MONITOR
[4]  WAN                     MODE = MONITOR
[5]  WAN                     MODE = MONITOR
[6]  WAN                     MODE = MONITOR

New Interface [1] : 4


           ***** Cisco SwitchProbe  V4.7.0 (Build 125) *****


Interface number : 4

[6]  Change Interface Speed             125
[7]  Change Encapsulation Protocol      FRAME_RELAY
[8]  Select Interface                   WAN
[11] Enter Command-line mode
[12] Reset Agent

[31] Go to Next Page
```



```
          Enter your response or Enter "exit" to logout

Selection#: 31

           ***** Cisco SwitchProbe  V4.7.0 (Build 125) *****

Interface number : 4

[13] Configure Agent Options
[14] Configure Interface Options
[15] Change RMON parameters
[16] Change RMON2 parameters
[18] Software Options
[19] Security Options
[20] Console Logout

[32] Go to Previous Page

          Enter your response or Enter "exit" to logout

Selection#: 13

           ***** Cisco SwitchProbe  V4.7.0 (Build 125) *****

Agent Options Menu:

[1]   Toggle router_discovery     on
[2]   Toggle router_enable        on
[3]   Toggle modem_log            off
[4]   Toggle slip_ip              off
[12]  Toggle ncp_request          on

[13] Go Back to Main Menu

           ***** Cisco SwitchProbe  V4.7.0 (Build 125) *****

Interface number : 4

[13] Configure Agent Options
[14] Configure Interface Options
[15] Change RMON parameters
[16] Change RMON2 parameters
[18] Software Options
[19] Security Options
[20] Console Logout
```

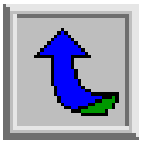
```
[32] Go to Previous Page

          Enter your response or Enter "exit" to logout


Selection#: 14


           ***** Cisco SwitchProbe  V4.7.0 (Build 125) *****


Interface Options Menu:

Interface number : 4

[1]   Toggle dlci_mode            on
[3]   Toggle nrzi_dte             off
[4]   Toggle nrzi_dce             off
[5]   Toggle crc_16               off
[6]   Toggle crc_disable          off
[8]   Toggle rawhdr_capture       off
[9]   Toggle pvc_discovery        on
[10]  Toggle mod128_lapb          off
[17]  Toggle Manage mode          off
[18]  Toggle Monitor mode         on

[19] Go Back to Main Menu


           ***** Cisco SwitchProbe  V4.7.0 (Build 125) *****


Interface number : 4

[13] Configure Agent Options
[14] Configure Interface Options
[15] Change RMON parameters
[16] Change RMON2 parameters
[18] Software Options
[19] Security Options
[20] Console Logout

[32] Go to Previous Page

          Enter your response or Enter "exit" to logout


Selection#: 18


           ***** Cisco SwitchProbe  V4.7.0 (Build 125) *****


Software Options Menu:
```

```
Interface number : 4

[1] Resource Monitor      on
[4] ART MIB Support       on

[32] return to previous menu

Selection#:

           ***** Cisco SwitchProbe  V4.7.0 (Build 125) *****


Interface number : 4

[13] Configure Agent Options
[14] Configure Interface Options
[15] Change RMON parameters
[16] Change RMON2 parameters
[18] Software Options
[19] Security Options
[20] Console Logout

[32] Go to Previous Page

          Enter your response or Enter "exit" to logout


Selection#: 15


           ***** Cisco SwitchProbe  V4.7.0 (Build 125) *****


RMON Parameters Menu:

Interface number : 4

[1]  Change max_host                      256
[2]  Change max_matrix                    1024
[3]  Change SHist_buckets                 50
[4]  Change LHist_buckets                 50
[5]  Change SHist_interval                30
[6]  Change LHist_interval                1800
[7]  Change dlci_sh_buckets               10
[8]  Change dlci_lh_buckets               10
[9]  Change dlci_sh_interval              180
[10] Change dlci_lh_interval              1800
[11] Toggle start_stats                   Yes
[12] Toggle start_history                 Yes

[13] Go Back to Main Menu

Selection#:
```

```
          ***** Cisco SwitchProbe  V4.7.0 (Build 125) *****

Interface number : 4

[13] Configure Agent Options
[14] Configure Interface Options
[15] Change RMON parameters
[16] Change RMON2 parameters
[18] Software Options
[19] Security Options
[20] Console Logout

[32] Go to Previous Page

          Enter your response or Enter "exit" to logout


Selection#: 16


          ***** Cisco SwitchProbe  V4.7.0 (Build 125) *****

RMON2 Parameters Menu:

Interface number : 4

[1]  Change nl_hosts                      4000
[2]  Change al_hosts                      8000
[3]  Change nl_matrix                     6000
[4]  Change al_matrix                     12000
[5]  Change dlci_nl_hosts                 4000
[6]  Change dlci_al_hosts                 8000
[7]  Change dlci_nl_matrix                6000
[8]  Change dlci_al_matrix                12000
[9]  Change min_aging                     300
[10] Toggle start_protocol_dist           Yes
[11] Toggle start_nl_host                 Yes
[12] Toggle start_nl_matrix               Yes
[13] Toggle enable_other_domains          Yes
[14] Toggle enable_all_host               Yes
[15] Toggle enable_all_matrix             Yes
[16] Change age_check_interval            300
[17] Change noise_threshold               0

[18] Go Back to Main Menu

Selection#:

          ***** Cisco SwitchProbe  V4.7.0 (Build 125) *****


Interface number : 1
```

```
[13] Configure Agent Options
[14] Configure Interface Options
[15] Change RMON parameters
[16] Change RMON2 parameters
[18] Software Options
[19] Security Options
[20] Console Logout
[21] Change ARTMIB parameters

[32] Go to Previous Page

          Enter your response or Enter "exit" to logout


Selection#: 13


           ***** Cisco SwitchProbe  V4.7.0 (Build 125) *****


Agent Options Menu:

[1]   Toggle router_discovery     on
[2]   Toggle router_enable        on
[3]   Toggle modem_log            off
[4]   Toggle slip_ip              off
[12]  Toggle ncp_request          on

[13] Go Back to Main Menu

           ***** Cisco SwitchProbe  V4.7.0 (Build 125) *****


Interface number : 1

[13] Configure Agent Options
[14] Configure Interface Options
[15] Change RMON parameters
[16] Change RMON2 parameters
[18] Software Options
[19] Security Options
[20] Console Logout
[21] Change ARTMIB parameters

[32] Go to Previous Page

          Enter your response or Enter "exit" to logout


Selection#: 14


           ***** Cisco SwitchProbe  V4.7.0 (Build 125) *****
```

```
Interface Options Menu:

Interface number : 1

[17]  Toggle Manage mode          on
[18]  Toggle Monitor mode         on

[19] Go Back to Main Menu

Selection
```



ANEXO 2. CONFIGURACIÓN DE LOS ENRUTADORES QUE FORMARON PARTE DE LA EMULACIÓN DE LA RED WAN

```
crlab-3810b#sh run
Building configuration...

Current configuration:
!
versión 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname crlab-3810b
!
enable secret 5 $1$SQaD$kWnTczbRe3ij64ck3MzW71
enable password cisco
!
!
!
!
!
network-clock base-rate 56k
ip subnet-zero
!
frame-relay switching
isdn voice-call-failure 0
!
!
controller E1 0
!
controller E1 1
!
!
interface Ethernet0
 ip address 10.1.200.190 255.255.255.0
 no ip directed-broadcast
!
interface Serial0
 no ip address
 no ip directed-broadcast
 encapsulation frame-relay
 no ip mroute-cache
 no fair-queue
 clockrate 125000
 frame-relay intf-type dce
 hold-queue 1024 out
!
interface Serial0.1 point-to-point
 ip address 10.2.60.1 255.255.255.252
```

```
 no ip directed-broadcast
 frame-relay interface-dlci 101
!
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
 serial restart-delay 0
!
router eigrp 1
 network 10.1.200.0 0.0.0.255
 network 10.2.60.0 0.0.0.255
 no auto-summary
!
no ip http server
ip classless
!
!
map-list atm1
!
map-class frame-relay frmc
 frame-relay adaptive-shaping becn
 frame-relay cir 125000
 frame-relay bc 1600
 frame-relay be 800
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
snmp-server engineID local 000000090200000107B4832FC
snmp-server community public RO
snmp-server community private RW
snmp-server enable traps snmp
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps hsrp
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps bgp
snmp-server enable traps rsvp
snmp-server enable traps frame-relay
snmp-server enable traps rtr
snmp-server host 10.1.200.201 public
rtr responder
!
line con 0
 transport input none
line aux 0
line 2 3
line vty 0 4
 password cisco
 login
!
end
```

```
crlab-2503#sh run
Building configuration...

Current configuration:
!
versión 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
enable secret 5 $1$n7EH$bJuw7VO1dqoPl2bLX/uTs/
enable password ciscojams
!
!
!
!
!
ip subnet-zero
!
isdn switch-type basic-5ess
isdn voice-call-failure 0
!
!
!
interface Ethernet0
 ip address 10.1.200.170 255.255.255.0
 no ip directed-broadcast
!
interface Serial0
 ip address 10.2.70.1 255.255.255.0
 no ip directed-broadcast
 clockrate 125000
!
interface Serial1
 no ip address
 no ip directed-broadcast
 encapsulation frame-relay
!
interface Serial1.1 point-to-point
 ip address 10.2.60.2 255.255.255.252
 no ip directed-broadcast
 frame-relay interface-dlci 101
!
interface BRI0
 no ip address
 no ip directed-broadcast
 shutdown
 isdn switch-type basic-5ess
!
router eigrp 1
 network 10.2.60.0 0.0.0.255
 network 10.2.70.0 0.0.0.255
```

```
 no auto-summary
!
ip classless
no ip http server
!
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
snmp-server engineID local 00000009020000D058AD6BC6
snmp-server community public RO
snmp-server community private RW
snmp-server enable traps snmp
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps hsrp
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps bgp
snmp-server enable traps rsvp
snmp-server enable traps frame-relay
snmp-server enable traps rtr
snmp-server enable traps dlsw
snmp-server host 10.1.200.201 public
rtr responder
!
line con 0
 transport input none
line aux 0
line vty 0 4
 password cisco
 login
!
end



crlab-3810c#sh run
Building configuration...

Current configuration:
!
versión 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname crlab-3810c
!
enable secret 5 $1$ZYQJ$auAA.q11/Wk/RDOotAVfh0
enable password cisco
!
!
!
!
```

```
!
network-clock base-rate 56k
ip subnet-zero
!
isdn voice-call-failure 0
cns event-service server
!
!
controller E1 0
 mode cas
 voice-group 1 timeslots 1-2 type fxo-loop-start
 voice-group 3 timeslots 3-4 type fxs-loop-start
 voice-group 5 timeslots 5-6 type e&m-wink-start
!
!
!
interface Ethernet0
 ip address 171.68.92.213 255.255.255.128
 no ip directed-broadcast
 no mop enabled
!
interface Serial0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 shutdown
 no fair-queue
!
interface Serial1
 ip address 10.2.70.2 255.255.255.0
 no ip directed-broadcast
!
interface Switch0
 no ip address
 no ip directed-broadcast
 encapsulation frame-relay
 shutdown
 no fair-queue
!
interface FR-ATM20
 no ip address
 no ip directed-broadcast
 shutdown
!
router eigrp 1
 network 10.2.70.0 0.0.0.255
 network 171.68.92.128 0.0.0.127
 no auto-summary
!
ip classless
no ip http server
!
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
```

```
!
snmp-server engineID local 00000090200000107B0EF5C8
snmp-server community public RO
snmp-server community private RW
snmp-server enable traps snmp
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps hsrp
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps bgp
snmp-server enable traps rsvp
snmp-server enable traps frame-relay
snmp-server enable traps syslog
snmp-server enable traps rtr
snmp-server enable traps dlsw
snmp-server enable traps dial
snmp-server enable traps voice poor-qov
rtr responder
!
line con 0
 transport input none
line aux 0
line 2 3
line vty 0 4
 password cisco
 login
!
!
voice-port 0/1
 timeouts call-disconnect 0
 timing hookflash-out 0
 connection plar opx 777
!
voice-port 0/2
 timeouts call-disconnect 0
 timing hookflash-out 0
 connection plar opx 999
!
voice-port 0/3
 no disconnect-ack
 timeouts call-disconnect 0
!
voice-port 0/4
 no disconnect-ack
 timeouts call-disconnect 0
!
voice-port 0/5
 timeouts call-disconnect 0
!
voice-port 0/6
 timeouts call-disconnect 0
!
voice-port 1/1
```

```
 timeouts call-disconnect 0
 connection plar opx 666
!
voice-port 1/2
 timeouts call-disconnect 0
 connection plar opx 888
!
voice-port 1/3
 timeouts call-disconnect 0
!
voice-port 1/4
 timeouts call-disconnect 0
!
voice-port 1/5
 timeouts call-disconnect 0
!
voice-port 1/6
 timeouts call-disconnect 0
!
!
dial-peer voice 777 pots
 destination-pattern 777
 port 1/1
!
dial-peer voice 666 pots
 destination-pattern 666
 port 0/1
!
dial-peer voice 999 pots
 destination-pattern 999
 port 1/2
!
dial-peer voice 888 pots
 destination-pattern 888
 port 0/2
!
!
end
```