



# UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

---

---

## FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

RECOMENDACIONES PARA LA ADMINISTRACIÓN  
DE REDES UTILIZANDO LA TECNOLOGÍA SNMP,  
SEGÚN LA COMUNIDAD INTERNET.

### T E S I S   P R O F E S I O N A L

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

**PRESENTA:**

CUAUHTÉMOC CARLON CARLON

**DIRECTOR DE TESIS:**

ING. JOSÉ MANUEL QUINTERO CERVANTES

FES ARAGÓN, ABRIL DEL 2007



Universidad Nacional  
Autónoma de México

Dirección General de Bibliotecas de la UNAM

**Biblioteca Central**



**UNAM – Dirección General de Bibliotecas**  
**Tesis Digitales**  
**Restricciones de uso**

**DERECHOS RESERVADOS ©**  
**PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL**

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

# A G R A D E C I M I E N T O S

---

A mi madre

**María Cristina Susana Carlon Vargas**

*A quien dedico este trabajo, porque con sus consejos, guía y enseñanza me enseñó el camino y con su esfuerzo, amor y dedicación me dotó de las armas que necesité para alcanzar mi meta, que no solo es mía, si no también de ella.*

A mis maestros

*Quienes con su paciencia y dedicación me llenaron de su conocimiento y me hicieron lo que soy ahora.*

A mi asesor

*José Manuel Quintero Cervantes, quien no sólo me enseñó, sino que también me mostró un camino.*

A la Ing. Antonia Navarro Gonzáles

*Quien me enseñó con tanto cariño en cada una de sus clases, a ella quién se convirtió en mi conciencia y guía en la finalización de mi meta, a ella quien me dedico su tiempo para hacerme un mejor profesionista y persona.*

A la UNAM

*Les agradezco la oportunidad que me dio de realizar mis estudios y la formación académica y personal.*

Al CAE504

*Por haber sido el objeto de estudio de mi tesis.*

---

<b>Introducción</b>	<b>I</b>
---------------------	----------

**PRIMERA PARTE:  
FILISOFÍA DE LA ADMINISTRACIÓN DE REDES SEGÚN  
LA COMUNIDAD DE INTERNET.**

**Capítulo 1: Evolución De La Administración De Redes**

1.1 Introducción	1
1.2 Evolución de la administración de redes	3
1.2.1- Modelo Cliente – Servidor	5
1.2.2.- Modelo per – to – per	6
1.3 Común denominador entre la administración de empresas y la administración de redes	7
1.4 Objetivos de la administración de redes	7
1.4.1 Alta disponibilidad de la red	7
1.4.2 Reducción de costos operacionales de la red	7
1.4.3 Reducción de cuellos de botella en la red	8
1.4.4 Incrementar la flexibilidad de operación e integración	8
1.4.5 Alta eficiencia	8
1.4.6 Facilidad de uso	8
1.4.7 Seguridad	9
1.5 Intentos para administrar las redes	9

**Capítulo 2: Administración de Sistemas**

2.1 Introducción	11
2.2 Modelos administrativos de redes	12
2.3 Administración de sistemas según OSI	14
2.3.1 Modelo funcional	14
2.3.2 Modelo de organización	15
2.3.3 Modelo de comunicaciones	15
2.3.4 Características principales del protocolo CMIP	16
2.3.5 Modelo de información	
2.3.6 Management Information Base (MIB)	17

### **Capítulo 3: Administración Según “Comunidad Internet”**

3.1 Introducción	18
3.2 La Comunidad Internet	18
3.3 Analogía de la administración de redes	21
3.4 Arquitectura de la administración de redes	22
3.4.1 Elementos principales de un sistema de administración de red, según la “Comunidad Internet”	23
3.4.1.1 Entidad administradora de red	24
3.4.1.2 Dispositivos administrados	24
3.4.1.2.1 Agentes	24
3.4.1.2.2 La MIB	25
3.4.1.3 Protocolos de administración	25

### **Capítulo 4: Introducción a Las Buenas Prácticas**

4.1 Introducción	27
4.2 El uso de buenas prácticas	27
4.3 Evaluación de necesidades y costos	28
4.4 Selección de topologías y tecnologías afines a las necesidades y productos	29
4.4.1 Análisis de requerimientos de hardware y software	30
4.4.2 Inventario de hardware	31
4.4.3 Inventario de direcciones IP	31
4.4.4 Descubrimiento de red	31
4.4.5 Modelado del tráfico de la red	32
4.4.6 Determinación de los niveles de confianza	32
4.4.6.1 Nivel de confianza alto	33
4.4.6.2 Nivel de confianza medio	33
4.4.6.3 Nivel de confianza bajo	33
4.4.7 Consideraciones de capacidad	34
4.4.8 Consideraciones de implantación	35
4.4.9 Evaluación de costos	35
4.5 Rendimiento de los dispositivos de la red	36
4.6 Modelado de la carga de trabajo de la red	36
4.6.1 El modelo de negocios eTOM	36
4.6.2 Diseño del modelo del proceso de negocios	39
4.6.3 Requerimientos del proceso de negocios	39
4.6.4 Definición del flujo del proceso	39
4.6.5 Componentes de un diagrama de flujo en el proceso de negocios	39

eTOM.	40
4.7 Simulación del comportamiento de la red bajo la carga de trabajo esperada	43
4.8 Realización de pruebas de estrés	43
4.9 Rediseño de la red según las necesidades	43
4.10 Retroalimentación al modelado de carga de trabajo	44
4.11 Productos obtenidos después del uso de las “ <i>Buenas prácticas</i> ”	44

## **Capítulo 5: La Base De Datos MIB**

5.1 Introducción	45
5.2 Sintaxis ANS.1	46
5.3 SMI Estructura de información de administración	47
5.3.1 Búsqueda de un grupo de objetos en la SMI conociendo el OID	48
5.4 Localización de la MIB en el árbol de registro	49
5.5 Objetos administrados	50
5.5.1 Un objeto consta de lo siguiente	50
5.5.2 Algunos ejemplos de objetos administrados	50
5.5.3 Ejemplo de definición de un objeto	50
5.5.4 Estructura de información ISO-CCITT	52
5.5.5 Identificadores de objetos e Instancias	53
5.5.5.1 Los objetos escalares	53
5.5.5.2 Los objetos tabulares	53
5.6 La MIB – II	54
5.6.1 Las Diferentes Clases de Módulos MIB	56
5.7 Ampliación de la MIB	57

## **Capítulo 6: Introducción a SNMPv1**

6.1 Introducción	58
6.2 Evolución de SNMP	59
6.3 Simple Network Management Protocol	60
6.5 Operaciones de SNMPv1	64
6.6 PDU (Protocol Data Unit)	65
6.7 Secuencia de transmisión de un mensaje SNMPv1	68
6.8 Secuencia de recepción de un mensaje SNMPv1	69
6.9 Tipos de mensajes SNMPv1	70
6.10 Definición en lenguaje ANS.1 del mensaje SNMP	75
6.11 Interacción del protocolo SNMPv1	77

## **Capítulo 7: Introducción a SNMPv2**

7.1 Introducción	78
7.2 SNMPv2 (RFC del 1901, ..., 1908)	78
7.3 Operaciones de SNMPv2	79
7.4 Secuencia de mensajes	80
7.5 Formato de los mensajes SNMPv2	80

## **Capítulo 8: Introducción a SNMPv3**

8.1 Introducción	83
8.2 El protocolo SNMPv3	83
8.3 Arquitectura de SNMPv3	84
8.4 Entidad SNMP	85
8.5 Administrador tradicional SNMPv3	88
8.5.1 Categorías de aplicaciones (Applications)	88
8.5.2 Motor SNMP (SNMP engine)	89
8.6 Agente tradicional SNMPv3	90
8.7 Comunicación entre módulos	91
8.8 Despachador de primitivas	91
8.9 Primitivas del subsistema del procesamiento de mensajes	92
8.10 Primitivas del subsistema de seguridad	92

## **SEGUNDA PARTE:**

## **HERRAMIENTAS PARA LA ADMINISTRACIÓN DE REDES**

### **Capítulo 9: Introducción Al Cableado Estructurado**

9.1 Introducción	97
9.2 Cableado estructurado	97
9.3 Cableado horizontal o de planta	98
9.3.1 Armario de distribución de planta	98
9.4 Elementos básicos del cableado horizontal	98
9.4.1 Cable Horizontal y Hardware de Conexión	98
9.4.2. Rutas y Espacios horizontales	98
9.4.2.1 El cableado horizontal incluye:	99
9.4.2.2 El cableado horizontal típico:	99

9.4.2.3 Topología	99
9.4.2.4 Distancia del cable	99
9.5 Cableado vertical ó backbone	100
9.5.1 Funciones del backbone	100
9.5.2 Topología	100
9.5.3 Cables Reconocidos	101
9.5.4 Distancias	101
9.6 Aterrizaje del cableado estructurado	102
9.7 Subsistemas de la norma ANSI/TIA/EIA-568	103

## **Capítulo 10: Direccionamiento lógico**

10.1 Introducción	105
10.2 Direccionamiento IP	105
10.3 Clasificación de las direcciones IP	105
10.4 Estructura de las direcciones IP	106
10.5 Clases de direcciones IP	107
10.5.1 La máscara de subred	108
10.6 Direcciones IP Reservadas	109
10.7 Subredes	109
10.8 Redes Privadas	111

## **Capítulo 11: Introducción a MG -SOFT**

11.1 Introducción	113
11.2 Interfaz de MG – SOFT MIB Browser	114
11.3 Barra de menús	114
11.4 Barra de herramientas	115
11.5 La barra de estados	115
11.6 El área de trabajo	116
11.7 La pestaña Query	117
11.8 Contactar con un agente SNMP	118
11.9 Selección de nodos en el Árbol MIB	119
11.10 Organización del árbol MIB	120
11.11 Propiedades de un nodo	121
11.12 Especificación de los parámetros del protocolo SNMPv1	121
11.12.1 Configuración de SNMPv1	122
11.13 Configuración del un perfil de agente	123
11.14 Configuración del protocolo SNMPv1	125
11.15 Descubrimiento de agentes SNMP	126



11.16 Monitoreo, Gráficas y Estadísticas	127
--	-----

### **TERCERA PARTE:**

## **PROPUESTA DE TESIS: OPTIMIZACIÓN DE LA RED DEL CENTRO DE APOYO EXTRACURRICULAR CAE504**

### **Capítulo 12: Análisis De La Red Del CAE504**

12.1 Introducción	131
12.2 Objetivos del CAE504	132
12.3 Misión	132
12.4 Visión	132
12.5 Necesidades de redes en el CAE504	133
12.6 Distribución del CAE504	134
12.7 Topología de la red del CAE504	134
12.8 Mapa de la red del CAE504	135
12.9 Inventario de hardware	137
12.10 Inventario de direcciones IP	143

### **Capítulo 13: Propuestas Para la Implantación De Mecanismos De Administración Para la Red Del CAE504**

13.1 Introducción	149
13.2 Propuesta 1: Reconfiguración al mínimo costo y máximo beneficio	150
13.2.1 Análisis de la configuración de los equipos de interconexión	150
13.3 Propuesta 2: Implantación óptima para la red del CAE504, siguiendo los lineamientos del cableado estructurado.	162
13.3.1 Redistribución del CAE504	162
13.3.2 Adopción de los estándares del cableado estructurado	163
13.3.3 Direccionamiento IP recomendado	168
13.4 Comparación de la eficiencia de la configuración actual del CAE504 con la propuesta de tesis.	170
13.5 Implantación del agente SNMP y su monitoreo	172
13.6 Presupuesto requerido para implantar la propuesta 2	176

<b>Conclusiones</b>	<b>177</b>
<b>Glosario</b>	<b>179</b>
<b>Referencias Bibliográficas</b>	<b>185</b>
<b>Referencias de Internet</b>	<b>186</b>
<b>Referencias de estándares</b>	<b>187</b>

## Introducción

---

La necesidad de administrar la diversidad de dispositivos en una red ha sido el principal motor que ha impulsado la búsqueda y diseño de herramientas con la finalidad de lograr una optimización de los recursos dispuestos en una red.

Debido a la gran cantidad de recursos económicos y por supuesto de recursos humanos utilizados en la implantación de una red, y más cuando una determinada red ya implantada es concebiblemente grande, se requiere de estrategias eficientes para su control.

Es casi inconcebible la ausencia de un mecanismo de administración para un sistema de comunicación de datos medianamente pequeño y más aún cuando este sistema es demasiado grande como para ser visualizado en su conjunto en la mente de un solo individuo.

Aunque OSI hizo lo propio, diseñando un mecanismo de administración de redes, éste no es compatible con la torre de protocolos TCP/IP, como se verá en el contenido de este trabajo, no obstante, existen algunas recomendaciones útiles dispersas, que utilizan los expertos en redes de datos.

A diferencia del estándar OSI, la “Comunidad Internet”, deja en manos de los administradores de red, las etapas de: análisis, planeación, diseño e implantación de la red. Esto reduce al modelo propuesto por la “Comunidad Internet”, a una entidad administradora, un agente, una base de datos MIB y un protocolo de comunicación SNMP.

Las etapas de: análisis, planeación, diseño e implantación de la red, son llevadas a cabo mediante el uso del concepto de “*Buenas Prácticas*”. Las cuales son un conjunto de técnicas, utilizadas para diseñar, optimizar ó expandir una red.

De esta forma el modelo de la “Comunidad Internet”, se vuelve bastante sencillo en comparación con el modelo administrativo propuesto por OSI.

En el modelo de administración de la “Comunidad Internet”, se hace un énfasis en la base de datos MIB, pues esta contiene toda la información correspondiente al nodo administrado. Esta información es accedida, consultada y modificada por un agente SNMP, a través de mensajes SNMP, los cuales son enviados por la entidad administradora de red.

Esto es posible llevarlo a cabo, una vez implantada la red, según el concepto de “*Buenas Practicas*” en la etapa de análisis de dicho concepto.

Para llevar a cabo una buena implantación de una red, se requerirán algunas herramientas y estándares propios de las redes, como por ejemplo: el concepto de cableado estructurado, algún software que permita enviar mensajes SNMP, técnicas de direccionamiento IP, etc.

Una vez que se cuente con el conocimiento y manejo de herramientas y técnicas correspondientes a la administración de redes, se debe proceder al análisis de algún caso en particular. Un ejemplo de esto, es el caso de la optimización de la red del CAE504.

Lo primero que se tiene que hacer según la filosofía de las “*Buenas Practicas*”, es el análisis de las necesidades del CAE504, posteriormente se analizará la red, para ver si se están consiguiendo cubrir dichas necesidades, de no ser así, se procederá a hacer una propuesta en la cual se justificará cada recomendación que se pretenda llevar a cabo para dicho centro de apoyo extracurricular.

Las recomendaciones más importantes serán expuestas en este trabajo y más aún, estas recomendaciones serán enriquecidas con herramientas y estándares para lograr proponer una forma de administrar las redes de manera eficiente.

A continuación se hará una breve descripción del contenido de los capítulos:

El capítulo 1 lleva por nombre *Evolución de la Administración de Redes*, donde su propósito es dar un panorama general de los primeros intentos por satisfacer la necesidad de administrar una red.

El capítulo 2 se titula *Administración de redes según la estructura OSI*, éste describe de manera general los módulos de los cuales consta la *administración de sistemas*, nombre dado a la administración de redes por parte de OSI.

El capítulo 3 trata la *Administración de redes según la comunidad Internet*, como el título lo menciona, la comunidad de Internet ha propuesto un mecanismo de administración basado en un protocolo denominado SNMP y un agente residido en un nodo administrado, así como una base de datos denominada MIB.

El capítulo 4 se llama *Introducción a las Buenas Prácticas*. El uso de las buenas prácticas hace referencia a las recomendaciones de expertos en el ramo de la administración de redes.

El capítulo 5 se titula *La MIB. Base de Información de Administración*. En este capítulo se aborda la forma en que se encuentra ordenada la información de un determinado dispositivo.

El capítulo 6 se llama *Introducción a SNMPv1*. En este capítulo se intenta dar una referencia a cerca de como funciona el protocolo de administración SNMP y sus operaciones de administración.

El capítulo 7 es titulado *Introducción a SNMPv2*, en este capítulo se habla de las innovaciones de SNMPv1 para el surgimiento de SNMPv3.

El capítulo 8 se titula *Introducción a SNMPv3*, en este capítulo se introduce a la última versión de SNMP, donde se observan las mejoras en el módulo de seguridad.

El capítulo 9 lleva por título *Introducción al cableado estructurado*. Este capítulo aborda las partes constitutivas del estándar del cableado estructurado con la finalidad de implantar un cableado eficiente para una red de datos.

El capítulo 10 es titulado *direccionamiento IP*. Esta herramienta es muy útil a la hora de llevar a cabo el direccionamiento lógico de una red, es por ello que se debe ser cuidadoso en el momento de seleccionar las clases de direcciones IP, las cuales son tratadas en este capítulo.

El capítulo 11 se titula *Introducción a MG – SOFT*, en este capítulo se da, de manera general una visión a cerca de la herramienta de software, que se utilizará en este trabajo, para llevar a cabo el monitoreo de la red. No obstante, la tarea de monitoreo se puede llevar a cabo con cualquier otro software semejante.

El capítulo 12 lleva por nombre: *Análisis de la red del CAE504*, en este capítulo se analiza la configuración de los equipos de interconexión, así como, la eficiencia de la red en cuestión.

Se registran los inventarios tanto de hardware como de direcciones IP y se lleva a cabo una revisión de las necesidades del CAE504, para ver si el diseño de la red actual, cubre dichas necesidades.

El capítulo 13 es titulado *Propuestas Para la Implantación De Mecanismos De Administración Para la Red Del CAE504*, en este capítulo se llevan a cabo una serie de recomendaciones divididas en dos propuestas, para la optimización del CAE504 basadas en lo revisado en este trabajo.

Por último, al final de la obra se incluye: un glosario con los términos utilizados en cada capítulo y las conclusiones. También se hace mención de las referencias consultadas, tanto de referencias bibliográficas como en línea (Internet).

## Capítulo 1

### Evolución De La Administración De Redes

---

#### 1.1 Introducción:

La administración de redes se ha convertido en un foco de atención crítico, debido a la gran diversidad de dispositivos que pueden incorporarse a una red, estos dispositivos suelen ser de distintos fabricantes e incluso utilizar distintos protocolos de comunicación para llevar a cabo sus funciones.

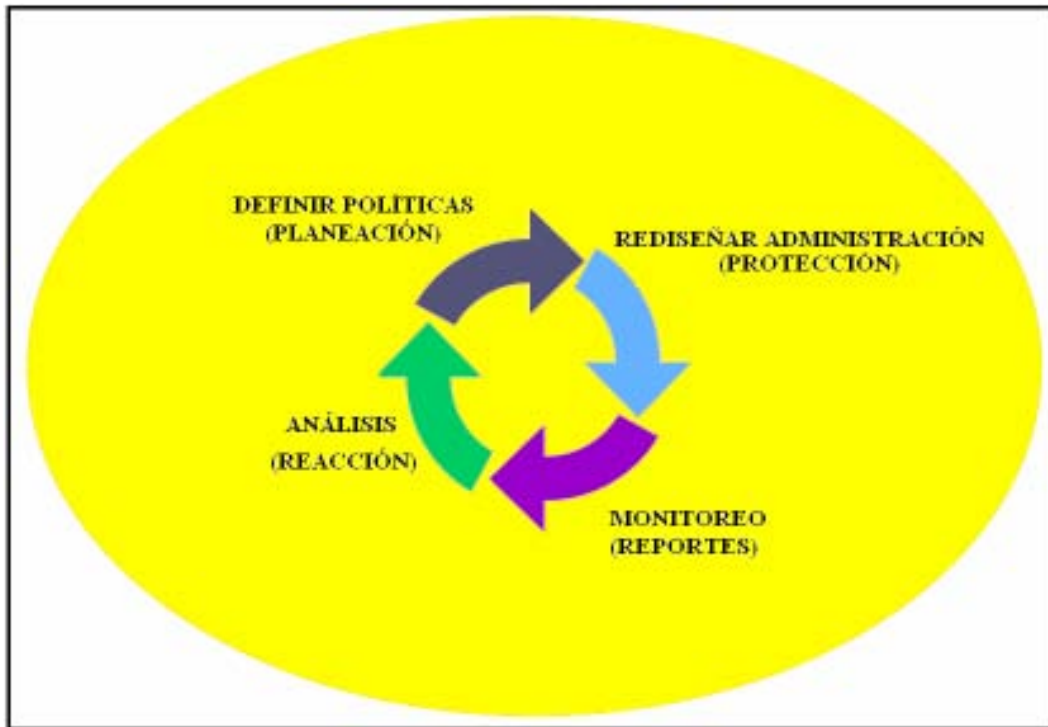
Es por ello que se requiere de una entidad administradora de dichos dispositivos. El modelo Cliente – Servidor con una gran cantidad de estaciones de trabajo necesita de la administración de redes para manejar y controlar las redes, clientes y las distintas tecnologías de interconexión que puedan existir entre éstos.

La administración de redes es un conjunto de técnicas con el propósito de mantener una red operativa, eficiente, segura, constantemente monitoreada y con una planeación adecuada y propiamente documentada.

La administración de las redes, se vuelve más importante y difícil, sí se considera que las redes actuales comprendan lo siguiente:

- Mezclas de diversas señales, como voz, datos, imagen y gráficas.
- Interconexión de varios tipos de redes, como *WAN*, *LAN* y *MAN*.
- El uso de múltiples medios de comunicación, como par trenzado, cable coaxial, fibra óptica, señales de satélite, infrarrojo, microondas, etc.
- Diversos protocolos de comunicación, incluyendo *TCP/IP*, *NetBeui*, etc.
- El empleo de muchos sistemas operativos, como *Netware*, *Windows*, *UNIX*, etc.
- Diversas arquitecturas de red, incluyendo *Ethernet 10 base T*, *Fast Ethernet*, *Token Ring*, etc.

Debido a estos puntos, la administración de redes hoy en día es muy diferente a como se llevaba a cabo en la época de las computadoras multiacceso. La administración de redes moderna cuenta con un ciclo administrativo como lo muestra la figura 1.1.



**Figura 1.1 Ciclo de la administración**

El ciclo de la administración mostrado en la figura 1.1 se compone de cuatro etapas cuando la red ha sido implantada.

La etapa de análisis se refiere a la toma de decisiones con base a las estadísticas obtenidas previamente en el monitoreo.

En la etapa de definición de políticas se lleva a cabo la planeación y la implantación de las mejoras a la red analizada.

La etapa de rediseño de administración, es la etapa donde después de haber hecho las mejoras se implanta un mejor mecanismo de administración. Este nuevo mecanismo debe de cubrir las expansiones ó modificaciones hechas a la red.

La última etapa es la de monitoreo, debido a que esta etapa es la que nos provee de las estadísticas necesarias que serán utilizadas para su análisis posterior.



## 1.2 Evolución de la administración de redes:

Las redes de telecomunicaciones dentro del ámbito informático han evolucionado a partir de la necesidad de compartir información y procesos con usuarios remotos.

En una primera fase se desarrollaron las grandes computadoras multiacceso, desde luego éstas eran difíciles de utilizar y tenían un costo muy elevado.

Estas primeras computadoras multiacceso tenían un uso local y eran operadas por una única persona o interfase como se muestra en la figura 1.2

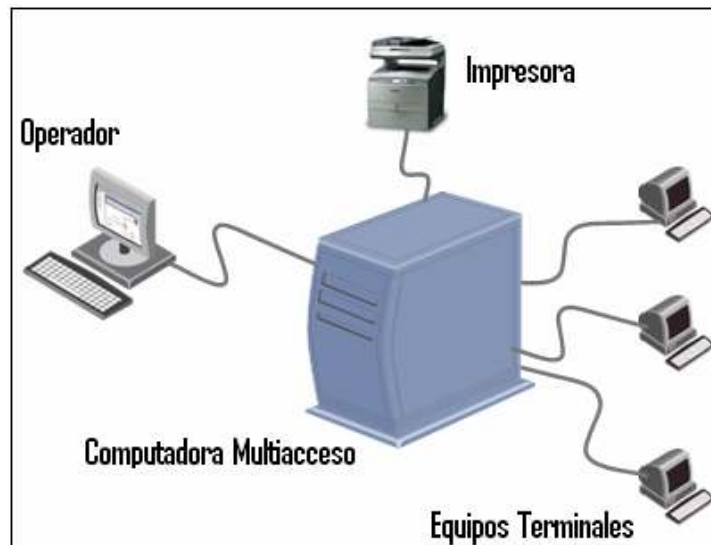


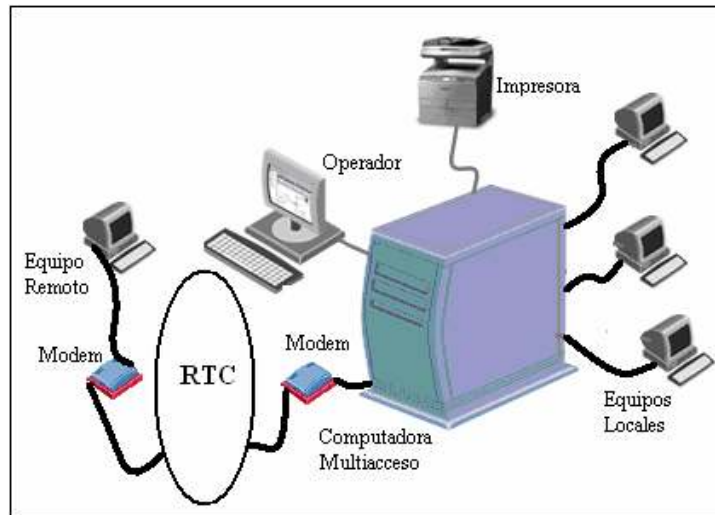
Figura 1.2 Sistema constituido por un único ordenador multiacceso

En la figura 1.2, se observa la conexión de equipos terminales los cuales se conectan a una gran computadora central multiacceso, esta gran computadora se encarga de proveer cualquier servicio que alguna de sus computadoras subordinadas soliciten.

Cabe destacar que esta computadora multiacceso, así como sus nodos terminales eran homogéneas, de tal forma que la tecnología para la construcción de la del sistema multiusuario era desarrollada por una marca en particular, haciendo imposible poder incorporar elementos de otros fabricantes a dicho sistema, por ello las técnicas de administración eran de tipo propietario, es decir, las recomendaciones a seguir para la administración eran proporcionadas por el fabricante de los equipos.

Más adelante el uso de las redes de telecomunicaciones permitió el acceso remoto de equipos terminales a las grandes computadoras multiacceso. Las redes de tecnología conmutada y el uso de módems eran más baratos que el hecho de adquirir varias computadoras multiacceso.

Esto derivó en el acceso remoto, es decir, por primera vez se podía acceder a una computadora multiacceso de manera remota, utilizando módems y redes de telecomunicaciones (RTC) como se muestra en la figura 1.3.



**Figura 1.3 Sistema constituido por una única computadora multiacceso conectada a través de modem a un equipo remoto.**

La administración del sistema multiusuario seguía siendo de tipo centralizado y basada en métodos del fabricante de la computadora multiacceso, aunque esta administración ya no cubría a la red de telecomunicaciones, al equipo remoto y su módem, pues estos elementos de la red ya eran de tipo externo.

A medida que el progreso tecnológico abarataba los costos de la introducción de computadoras multiacceso en las empresas, los sistemas multiusuarios pasaron de tener configuraciones centralizadas a configuraciones de tipo distribuido con diversas computadoras multiacceso, y por consecuencia la administración de estos sistemas comenzó a pasar de modelos centralizados a modelos distribuidos ó jerárquicamente distribuidos en función del rango de las computadoras multiacceso del sistema distribuido.

Más adelante con el empleo masivo las computadoras personales del tipo PC en las grandes corporaciones se desarrollaron redes locales en conexiones con redes

de área extendida para poder cubrir las distancias correspondientes a campus o ciudades.

Esto dio origen a la proliferación de fabricantes, los cuales desarrollaron terminales y dispositivos de interconexión derivando de esto, las redes heterogéneas.

Las nuevas redes heterogéneas exigían una administración demasiado complicada. Es por ello que a partir de ese momento, resulta evidente la necesidad de diseñar mecanismos de estandarización para poder administrar la creciente complejidad de los sistemas de redes.

De esta forma surgieron las redes de área local LANs (Local Area Network), las cuales generalmente son de tipo heterogéneo y debido a esto se concibieron dos modelos de aplicaciones para tratar su administración:

### **1.2.1- Modelo Cliente – Servidor:**

Este modelo consiste en la manera de describir la forma de trabajo de los procesos que ejecutan las computadoras <sup>1</sup>.

**El cliente:** Es un programa que reside en una computadora, el cual ejecuta los procesos que piden información, recursos y servicios a un programa llamado servidor, al cual está unido. Esta conducta convierte al cliente en un consumidor de servicios.

El programa cliente:

- Contacta con el programa servidor.
- Da formato a la petición de información.

**El Servidor:** Es un programa que reside en una computadora que ofrece algún tipo de servicio solicitado mediante un mensaje de un programa llamado cliente. Esto convierte al programa servidor en un proveedor de servicios.

---

<sup>1</sup> Comer, Douglas E. *Interworkings whit TCP/IP – Volume I: Principles, Protocols, and Architecture*. Tercera edición, Prentice-Hall, 1995.

El programa servidor:

- Recibe la petición y la procesa.
- Responde enviando la petición al cliente.

Los programas servidores pueden estar instalados en sistemas operativos diferentes como *Windows NT*, *Windows XP*, *Unix*, etc.

La mayor parte de las operaciones que se realizan en Internet tienen como base el modelo Cliente – Servidor.

Así el programa cliente y el programa servidor interactúan por medio de mensajes que no son otra cosa que solicitudes de servicios y respuestas a los mismos.

La figura 1.4 muestra el modelo Cliente – Servidor



**Figura 1.4 Modelo Cliente – Servidor**

**1.2.2.- Modelo per – to – per:**

Este modelo propone que no existan roles fijos entre un cliente y un servidor, es decir, cualquier computadora puede ser cliente o servidor en un determinado momento. Un ejemplo clásico de este modelo se da en las redes de Microsoft utilizando el protocolo *NetBeui* con la estructura de “*Grupo de trabajo*”, donde no está definido un administrador propiamente.

Debido a que en este trabajo nos avocaremos al modelo Cliente – Servidor, no profundizaremos más en el modelo per to per.

La evolución de las redes de computadora homogéneas, en donde había una gran computadora central hacia el tipo de redes LAN heterogéneas fue gradual. La transformación al ambiente de redes LAN se vuelve complicado debido a la gran diversidad de aplicaciones y protocolos de diferentes estándares y fabricantes. Sin embargo las limitaciones de la tecnología, protocolos y topologías imponen restricciones a cerca del número de computadoras que se pueden conectar a una

LAN. Por este motivo la forma de conexión a una red, los distintos dispositivos que forman parte de una red y sobre todo su administración se vuelven de vital importancia para el buen funcionamiento y aprovechamiento de los distintos recursos de una red.

### **1.3 Común denominador entre la administración de empresas y la administración de redes.**

Existen diversos puntos de vista sobre la definición de administración de redes (Network Management). Aplicando la definición de administración de negocios en el área de las redes de comunicación de datos, podemos ver que la administración de redes involucra los siguiente: Planeación, Organización, Monitoreo, contabilidad y control de actividades y recursos. Sin embargo, las estructuras de administración del modelo de referencia OSI (Open Systems Interconnection) y el modelo de la “Comunidad Internet”, se enfocan primordialmente en el monitoreo y el control de actividades y recursos. Los otros dos aspectos: Planeación y organización, no están contemplados en las dos estructuras mencionadas.

La planeación y la organización en las redes de comunicaciones de datos son los puntos medulares de la administración de redes, ya que pueden llegar a consumir en buena medida muchos de los recursos humanos y económicos de una empresa. Es por esto que si las redes no siguen una metodología de planeación y organización no sirve de nada la información obtenida en el monitoreo, la contabilidad y el control de actividades.

### **1.4 Objetivos de la administración de redes**

#### **1.4.1 Alta disponibilidad de la red:**

Se refiere a la capacidad de proveer eficiencia operacional, reduciendo los tiempos de espera de la red y proveyendo de tiempos de respuesta aceptables. Los problemas que pueda presentar una red deben ser rápidamente detectados y corregidos para evitar cualquier tipo de costo adicional.

#### **1.4.2 Reducción de costos operacionales de la red:**

Este es un objetivo primario cuando se habla de administración de redes. Como las tecnologías cambian rápidamente es deseable la administración de sistemas heterogéneos y de múltiples protocolos.

### **1.4.3 Reducción de cuellos de botella en la red:**

El análisis de los datos supervisados puede revelar problemas como una excesiva demanda de determinados recursos que ocasiona cuellos de botella.

#### **Las causas pueden ser:**

- Los recursos no son suficientes y se requieren componentes adicionales o actualizados.
- Los recursos no están compartiendo las cargas de trabajo uniformemente y tienen que equilibrarse.
- Un recurso está funcionando mal y debe sustituirse.
- Un programa está acaparando un recurso en particular; esto puede hacer necesario sustituirlo por otro programa, agregar o actualizar recursos, o ejecutar el programa en períodos de baja demanda.

### **1.4.4 Incrementar la flexibilidad de operación e integración:**

Debido a que la velocidad de cambio de las tecnologías es mayor a la de los requerimientos y necesidades, debe ser posible absorber nuevas tecnologías a un costo mínimo y adicionar nuevo equipo sin mucha dificultad. Además debe permitir lograr una fácil migración de un software de administración de redes a otra versión.

### **1.4.5 Alta eficiencia:**

A veces se debe incrementar la eficiencia de una red en detrimento de algún otro objetivo de la administración de redes. Estas decisiones se toman de acuerdo a criterios tales como la utilización, costo operacional, costo de migración y flexibilidad de los distintos componentes de la red en cuestión.

### **1.4.6 Facilidad de uso:**

Cuando se habla de facilidad de uso, se hace referencia a las interfases de usuario, donde éstas juegan un papel muy importante en el éxito del producto. El uso de aplicaciones de administración de redes no deben ser complicadas ni requerir demasiada especialización por parte del administrador.

### **1.4.7 Seguridad:**

Este rubro es de suma importancia para el administrador ya que él es el encargado de proporcionar los mecanismos de seguridad, pues la información es un activo muy importante para cualquier empresa como por ejemplo información financiera.

### **1.5 Intentos para administrar las redes.**

Con la mira de proveer soluciones a los objetivos de la administración de redes, surgieron distintos organismos de estandarización que trataron de solucionar el problema de la administración de redes heterogéneas como el equipo de ingenieros de Internet IEFT (Internet Engineering task force) que definió el protocolo simple de administración de redes SNMP (Simple Network Management Protocol) sobre el cual versa este trabajo.

Pero este protocolo no sirve de mucho sin otros elementos como un agente que reside en un nodo administrado, la base de datos denominada MIB, la cual tiene toda la información propia del dispositivo administrado, así como, una entidad administradora de red, que se encarga de monitorear y ajustar los mecanismos necesarios para administrar los distintos dispositivos que se pueden encontrar en una red.

La entidad administradora funciona de la siguiente manera: manda un mensaje SNMP, el cual es interpretado por el agente en cuestión, dependiendo del tipo de mensaje, se lleva a cabo un ajuste en el nodo administrado.

Dentro de este sistema también puede suceder algún evento inesperado, para el cual el agente está obligado a reportar a la entidad administradora de red.

El esquema que propuso OSI, es mucho más robusto debido a que no sólo cuenta con un protocolo de comunicación denominado CMIP, sino que a diferencia de la propuesta de la “Comunidad Internet”, propuso de igual forma mecanismos para la organización, comunicación y control de información de la red. Todo esto fue dividido en los modelos funcionales siguientes:

- Modelo de organización.
- Modelo de comunicación
- Modelo de información.

Como se puede observar la “Comunidad Internet”, sólo hace hincapié en la comunicación de la entidad administradora de red y el nodo administrado; mientras que la estructura propuesta por OSI, cubre más aspectos de la administración, haciendo este modelo mucho más robusto, pero a su vez muy difícil de implantar.

Debido a esta complejidad, la tendencia es utilizar la filosofía de administración propuesta por la “Comunidad Internet”, por su sencillez de implantación, desde luego, la parte de organización e implantación es responsabilidad del administrador de la red.

En este trabajo nos avocaremos al modelo propuesto por la “Comunidad Internet” debido a que es el más utilizado junto con el protocolo de administración SNMP.



## Capítulo 2

### Administración De Sistemas

---

#### 2.1 Introducción

Como se comentó en el capítulo 1, a medida que las redes de computadora fueron haciéndose más grandes y complejas, fue necesario de igual forma diseñar mecanismos para la administración de las mismas.

Uno de los organismos que puso manos a la obra en esta empresa fue OSI, quién diseñó lo que ellos denominaron la “*Administración de sistemas*”. Es importante hacerle notar al lector que en este capítulo sólo se dará una reseña de la estructura de administración según OSI debido a que en la práctica se usa el modelo de la “Comunidad Internet”.

Cuando se requiere enseñar los procesos de comunicación entre dos dispositivos en una red, se recomienda utilizar el modelo de referencia OSI con sus siete capas, para tener una mejor comprensión al estudiar el conjunto de protocolos TCP/IP junto con sus procesos de comunicación en la red, los cuales son en realidad utilizados en estos momentos en Internet. De igual forma, el modelo de administración de redes según OSI, se recomienda revisar debido a que guarda ciertas similitudes con el modelo propuesto por la “Comunidad Internet”, el cual es el más utilizado en estos momentos.

#### **Las similitudes más importantes son:**

- Ambos modelos tienen un protocolo de comunicación.
- Ambos modelos utilizan agentes en los nodos administrados.
- Ambos modelos tienen una base de datos denominada MIB.

No obstante, sí el lector está interesado en leer más acerca del modelo de administración según OSI se le sugiere la serie de recomendaciones X.700.

## 2.2 Modelos administrativos de redes

A medida que las redes de computadoras se fueron haciendo más grandes y complejas, las necesidades de administración fueron cobrando una gran importancia, esto orilló a que surgieran diferentes propuestas con la finalidad de llevar a cabo la administración de redes.

En la década de los ochentas, la organización de estandarización OSI, propuso un esquema para la administración de redes llamado “*Administración de sistemas*”, el cual consta de cinco modelos, una base de datos para estructurar la información, denominada MIB y una guía para la definición de los objetos administrados.

Por otra parte en la década de los noventas surgió otra organización llamada “Comunidad Internet”. Esta organización propuso otro esquema administrativo el cual esta basado en el protocolo SNMP, dejando la parte de planeación, organización, análisis e implantación a un concepto denominado “*Buenas Prácticas*”, él cual no es propiamente un estándar, sí no, recomendaciones sugeridas por expertos en la materia.

La figura 2.1 muestra un esquema, en donde su raíz: la evolución de la administración de redes, deriva en dos formas de llevar a cabo la labor de administrar redes de computadora:

- La estructura OSI con sus características.
- La estructura de la “Comunidad Internet” con su propia filosofía.

Como ya se mencionó, en este capítulo se hablara de la administración de sistemas según OSI. En la figura 2.1 se muestra dicha estructura a través de un cuadro sinóptico que ilustra las partes esenciales de está distribución de administración.

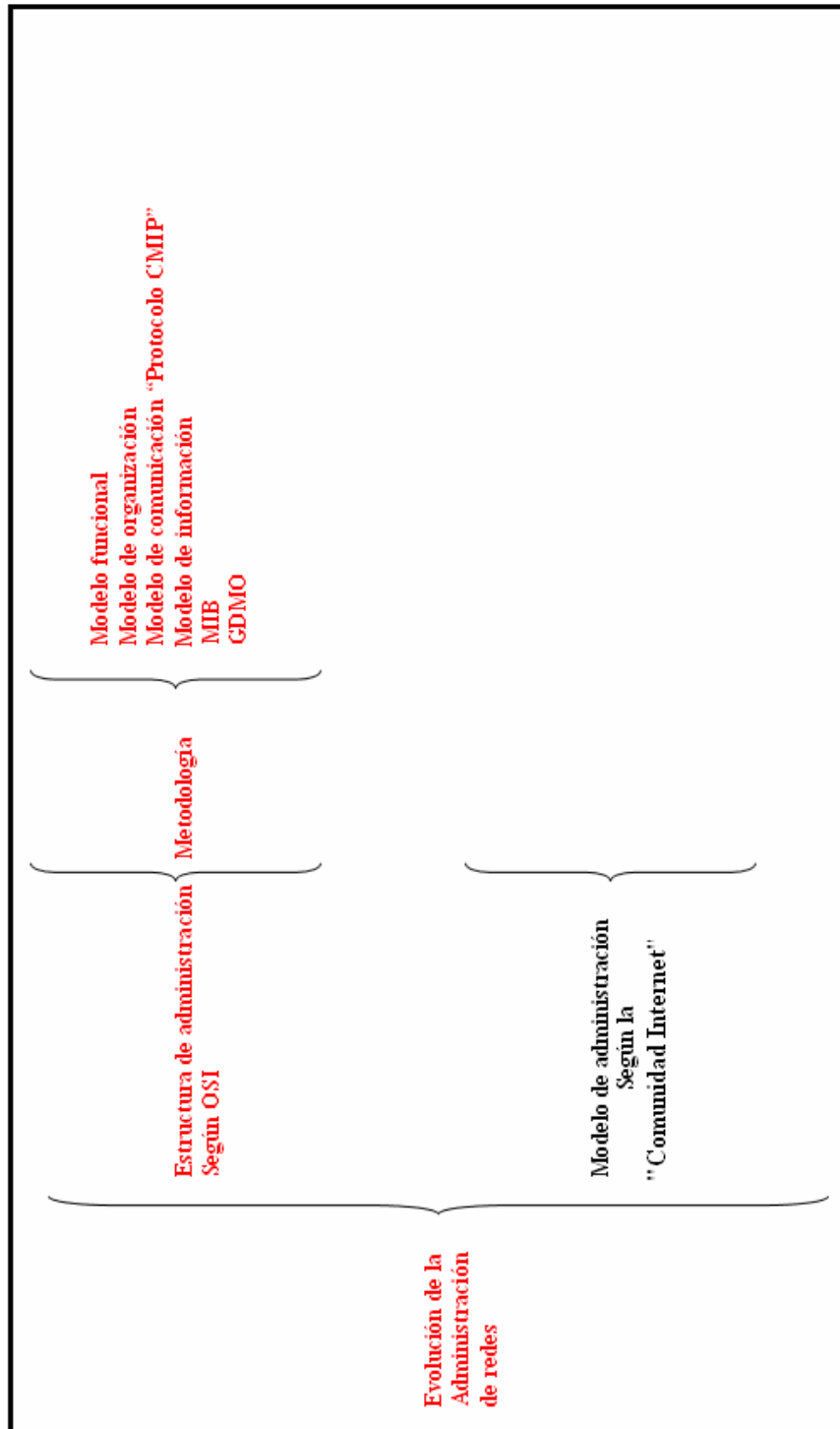


Figura 2.1. Formas de administración de redes

A continuación se dará una breve reseña de la administración según la estructura OSI, dejando en claro que este trabajo se basará en la filosofía de la “Comunidad Internet”.

## **2.3 Administración de sistemas según OSI**

El fundamento del sistema de administración OSI, es la base de datos MIB (*Management Information Base*), que contiene información relativa a los recursos y elementos que deben ser administrados. La estructura de administración de información SMI (*Structure Management Information*) identifica los nodos, y dentro de estos nodos se encuentra el nodo MIB. En esta base de datos se representan y nombran los grupos de objetos que componen el nodo administrado.

Cada recurso que se monitorea por el sistema de administración OSI se representa por un objeto administrado como por ejemplo: conmutadores, PCs, programas, etc.

En este caso de administración, la complejidad de la administración se traslada al agente (éste reside en un dispositivo administrado). Los protocolos de administración permiten realizar funciones más complejas dado que el modelo de administración también es complejo.

Este sistema de administración permite hablar de diversos modelos de administración de sistemas, los cuales se describen a continuación:

### **2.3.1 Modelo funcional**

El modelo funcional describe las cinco áreas en las que tradicionalmente se ha dividido la administración de red: administración de fallos, administración de configuración, administración de presentación, administración de contabilidad y administración de seguridad.

El sistema de administración basado en OSI define una serie de niveles con interfaces de administración que interactúan con la base de datos MIB. El nivel de aplicación interactúa, a su vez, con otros procesos de administración mediante el protocolo de información de administración común CMIP (*Common Management Information Protocol*) como lo muestra la figura 2.2.

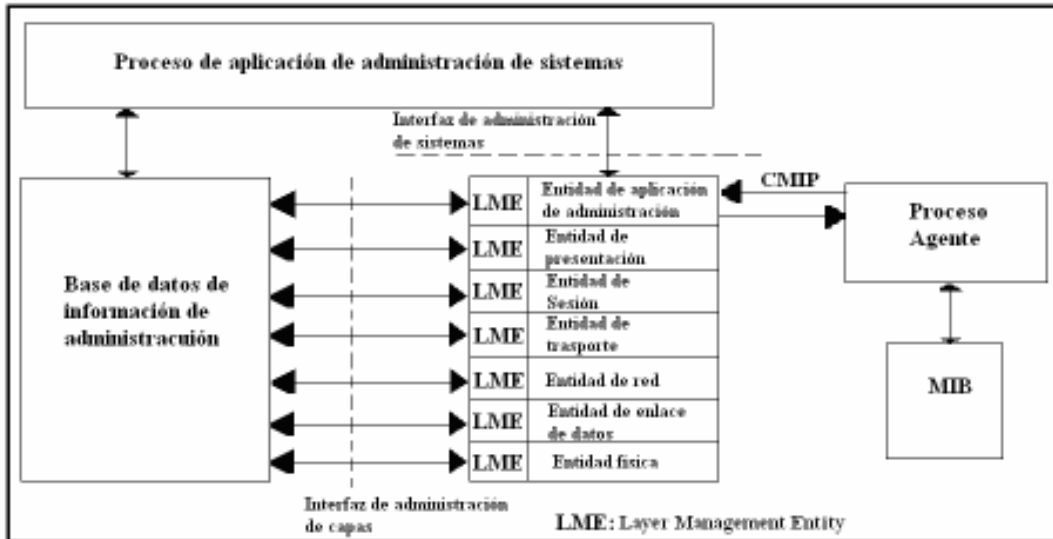


Figura 2.2 Marco de administración según OSI

Las áreas funcionales de administración específicas están constituidas a su vez por diversas funciones específicas SMF (Funciones de administración del sistema) que realizan procesos de administración interactuando con los diversos servicios.

### 2.3.2 Modelo de organización

El modelo de organización parte de una estructura de red dividida en dominios de administración. La división de dominios se realiza a partir de dos aspectos principales:

- Políticas funcionales.
- Dominio geográfico tecnológico.

La red se estructura en dominios administrativos, con la necesidad de establecer y mantener cada una de las responsabilidades de cada dominio. Por otra parte el sistema permite que dentro de un dominio, se pueda reasignar el papel de administrador y agente.

### 2.3.3 Modelo de comunicaciones

El Protocolo CMIP se define en el estándar 9596 de OSI. Este protocolo ofrece un mecanismo de transporte en la forma de servicio de pregunta y respuesta para las

capas del modelo OSI. La especificación del protocolo describe de manera precisa, el como se ejecutan los servicios individuales.

Una parte de la especificación del protocolo CMIP es la definición de la *Abstract Syntax Notation* (ANS.1) para codificar y decodificar unidades de datos del protocolo CMIP.

### **2.3.4 Características principales del protocolo CMIP.**

- CMIP Requiere de una gran cantidad de memoria y capacidad de procesamiento.
- Se generan largas cabeceras en los mensajes del protocolo.
- Las especificaciones son difíciles de realizar y tediosas de implantar en una aplicación.
- La comunicación con los agentes esta orientada a conexión.
- La estructura de funcionamiento es distribuida.
- Permite una jerarquía de sistemas de operación.
- El protocolo asegura que los mensajes lleguen a su destino.

El hecho de que se trate de una administración conducida por eventos se traduce en:

- El agente notifica al administrador acerca de sucesos concernientes al recurso administrado.
- El agente es responsable de monitorizar los recursos.
- Presenta la ventaja de que hay menos administración de tráfico.
- Presenta la ventaja de tener agentes más complejos.

Sí se requiere saber más se recomienda dar lectura al estándar 9596 de ISO donde se describe de manera amplia el funcionamiento del protocolo CMIP.

### **2.3.5 Modelo de información**

El modelo de información proporciona una representación de los recursos administrados. En el esquema de la figura 2.3 se muestra el proceso de obtención de la información de administración del entorno de red.

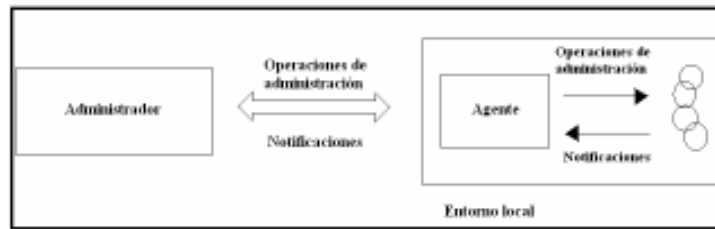


Figura 2.3 Esquema del proceso de administración en un entorno local.

El objetivo consiste en modelar los aspectos de administración de los recursos reales, así como definir una estructura para la información de administración que se trasmite entre sistemas.

Este modelado se estructura en función de unos objetos administrados (MO: *Managed Object*) que se pueden definir como abstracciones de un recurso que representa sus propiedades para el propósito de administrar, por ejemplo un equipo de interconexión activo. Para el caso que nos ocupa, sólo es necesario definir los aspectos del recurso útiles para su administración. De la misma forma no se define la relación entre el recurso y su abstracción como objeto administrado, que suele ser definido por el fabricante.

### 2.3.6 Management Information Base (MIB)

Una MIB es un conjunto de definiciones de uno ó varios recursos formados por clases de objetos administrados, acciones, notificaciones, atributos y sintaxis, etc. Actualmente hay una gran variedad de MIBs definidas y normalizadas.

Una MIB no tiene por que ser auto contenida, ya que permite referenciar a otras MIBs. La sintaxis de MIBs se basa en la notación de guía para definición de objetos administrados GDMO (*Guidelines for Definition of Managed Object*). Existe una serie de criterios para implantar una MIB, como el uso de herencias de definiciones ya existentes y el establecer ligaduras de nombrado siempre que sea posible.

Una MIB puede interpretarse como la extracción de árbol de herencia y extracción de los posibles árboles de agregación.

Una vez mostrada la complejidad de la administración de redes según OSI, se hace necesario buscar algún otro modelo de administración más sencillo para llevar a cabo esta tarea, es por ello que en el siguiente capítulo se explicará como llevar a cabo la administración de redes según la "Comunidad de Internet".

## Capítulo 3

### Administración Según “Comunidad Internet”

---

#### 3.1 Introducción

Como ya se mencionó en el capítulo anterior, los modelos de administración más importantes son la estructura de administración de OSI y la filosofía de administración de la “Comunidad Internet”, en este capítulo nos dedicaremos a revisar la ideología de la administración propuesta por la “Comunidad Internet”, así como los componentes que la integran, tales como: la entidad administradora de red, el agente residido en el nodo administrado, la base de datos denominada MIB, y el medio de comunicación entre la entidad administradora de red y el agente, es decir, el protocolo de comunicación SNMP.

Este modelo de administración propuesto por la “Comunidad Internet” es el más utilizado y popular en estos momentos debido a su sencillez, mientras que el modelo de administración propuesto por OSI, es demasiado robusto, complejo y difícil de implantar en una red determinada, esto aunado a que la estructura de administración de OSI está basada en el modelo de referencia OSI con las siete capas que lo conforman, el cual no se usa en la práctica, esto da como consecuencia que los administradores de red no lo utilicen para administrar sus redes.

No obstante, el modelo propuesto por la “Comunidad Internet”, el cual es bastante simple como se verá en el contenido de este capítulo, se ha hecho bastante popular en cuanto a la administración de redes se refiere.

#### 3.2 La Comunidad Internet

La “Comunidad Internet” (*Internet Society, ISOC*) es una asociación no gubernamental y sin fines de lucro.

ISOC es la única organización dedicada exclusivamente al desarrollo mundial de Internet, con la tarea específica de concentrar sus esfuerzos y acciones en asuntos particulares sobre Internet; fundada en 1991 por una gran parte de los arquitectos pioneros encargados de su diseño. La ISOC tiene como objetivo principal ser un centro de cooperación y coordinación global para el desarrollo de protocolos y estándares compatibles para Internet.



La “Comunidad Internet”, propuso un modelo de administración de redes muy sencillo, sin complicaciones basado en la torre de protocolos de TCP/IP, el cual brinda una excelente herramienta para el funcionamiento del protocolo SNMP, siendo éste el más popular para la administración de dispositivos de redes, no obstante, el modelo de administración propuesto por la “Comunidad Internet” requiere de otros elementos para poder llevar a cabo su cometido, la figura 3.1 muestra la ubicación de los elementos administrativos dentro de la filosofía de administración según la “Comunidad Internet”, los cuales se listan a continuación:

- Entidad administradora de red.
- Nodos administrados
  - MIB y Agente.
- Protocolo de comunicación SNMP.

La figura 3.1 muestra como a partir de la evolución de la administración de redes se hizo necesario el diseño de algún modelo para llevar a cabo la administración de redes. El modelo propuesto por la “Comunidad Internet”, tiene como base el uso de las “*Buenas Prácticas*”, de las cuales se hablará en el capítulo 4 y dentro de lo que son las “Buenas Prácticas”, justo en la etapa del análisis, es donde entra el modelo propuesto por la “Comunidad Internet”, con sus elementos como son: La entidad administradora de red, el nodo administrado, la MIB, el agente SNMP y el protocolo SNMP.

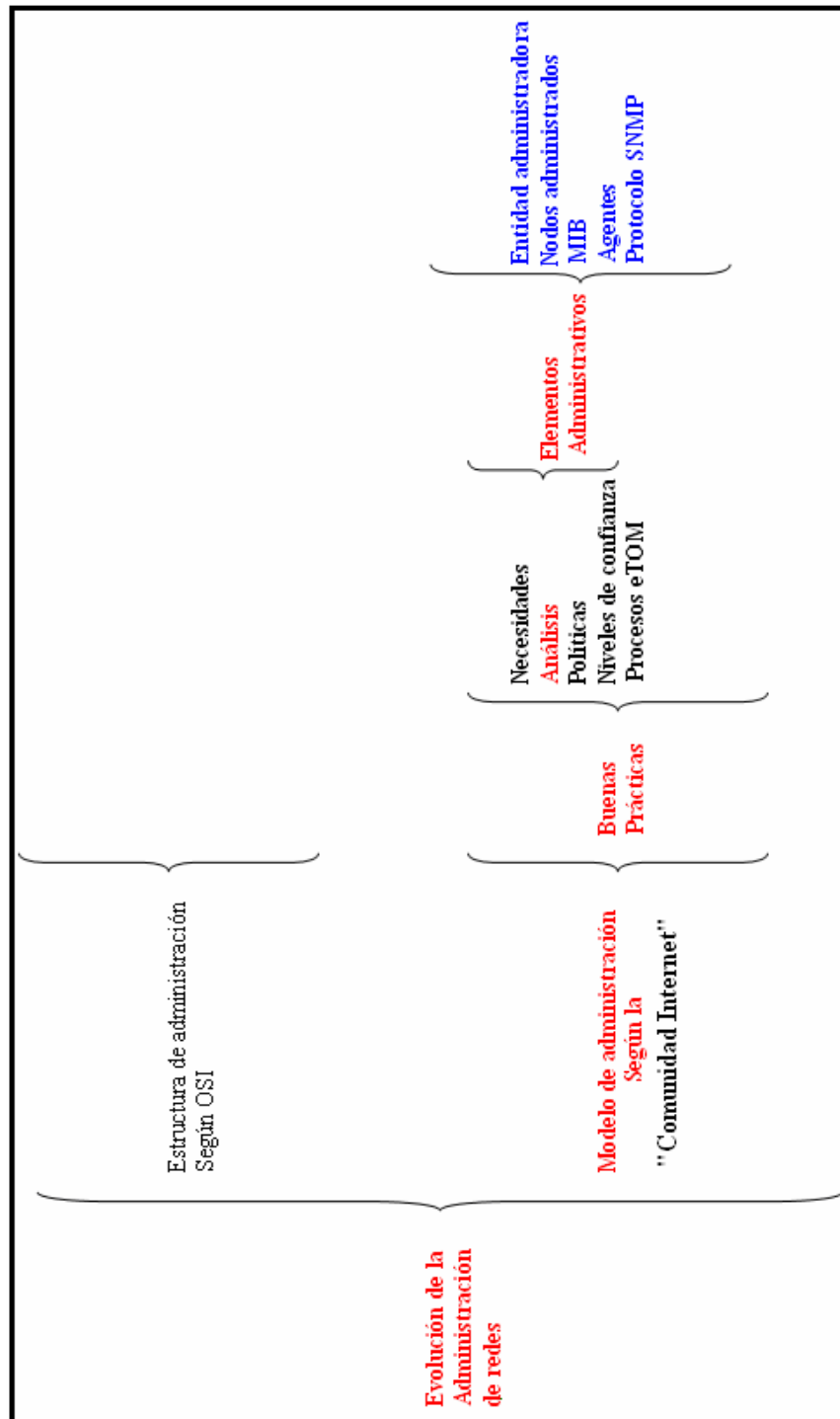


Figura 3.1. Filosofía para la administración de redes según la comunidad de Internet.

### 3.3 Analogía de la administración de redes

En este apartado se introducirá al lector en las bases de la administración de redes.

Para entender cómo funciona un sistema de administración de redes, iniciaremos con una analogía. Supongamos que una compañía tiene una oficina central y tres sucursales, el director de la compañía está en la oficina central y en cada sucursal hay un jefe de sucursal. El director general solicita a cada jefe de sucursal un informe del estado de la sucursal a su cargo, y en caso de necesitar algún ajuste, el director se lo comunica al jefe de sucursal para que lo lleve a cabo. Es decir, el director general se comunica con el jefe de sucursal para conocer el estado y los ajustes que se deben aplicar en cada sucursal según sea necesario. De manera excepcional, el jefe de sucursal necesita enviarle una notificación al director general de que algo anormal ocurre en su sucursal.

La comunicación entre director general y los jefes de sucursal, está en un formato normalizado y de acuerdo a un protocolo establecido. Asimismo, cada jefe de sucursal tiene su propia base de datos, donde el formato de la base de datos es el mismo en cada caso.

En administración de redes el director general se llama **entidad administradora de red**, el jefe de sucursal se llama **agente**, la base de datos de cada agente se llama **MIB** y el protocolo para la comunicación de informes se llama **protocolo de administración**, para este caso SNMP.

La figura 3.2 ilustra de manera análoga la administración de redes con la administración de una determinada compañía.

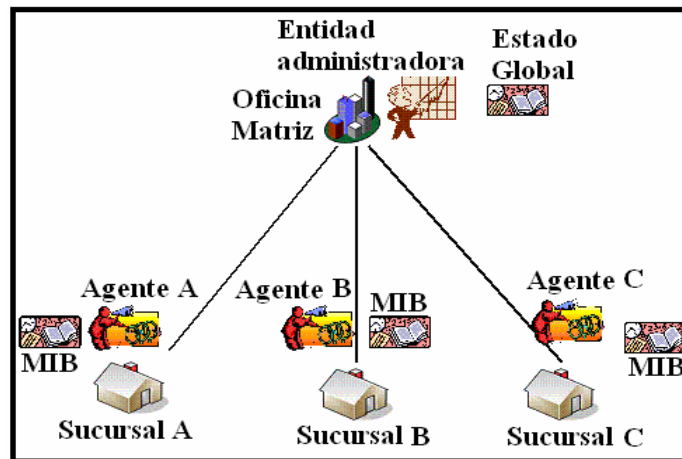


Figura 3.2 Administración de una compañía

Como se puede observar en la figura 3.2, la analogía de la administración de una determinada compañía está constituida de un administrador ó director, el cual se encarga de revisar frecuentemente el estado de cada sucursal para que sus operaciones sean realizadas de una manera correcta, no obstante, la comunicación del jefe de sucursal no está condicionada exclusivamente a peticiones del administrador, si no que si llega a suceder algún evento inesperado, el jefe de sucursal es capaz de hacérselo saber al administrador de manera inmediata, de esta forma no es necesario que el jefe de sucursal espere la petición de un informe por parte del administrador.

Es de suma importancia mencionar que la forma de comunicarse tanto del administrador como del jefe de sucursal es bien conocida por ambas partes.

### 3.4 Arquitectura de la administración de redes

La figura 3.3 muestra una red, la cual contiene los siguientes elementos administrados por la entidad administradora de red: un grupo de PCs, *Switch*, *Router* y un *Access Point*.

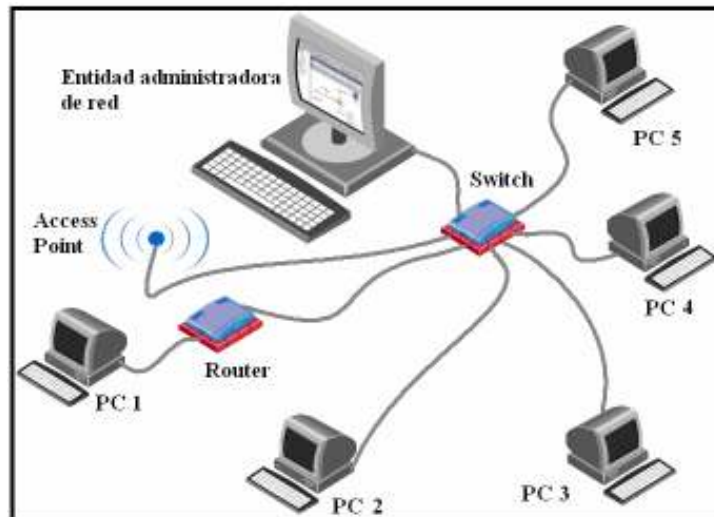
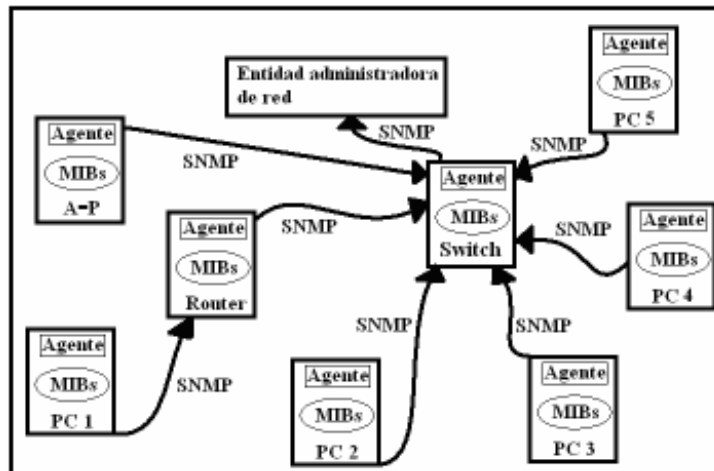


Figura 3.3 Esquema de dispositivos administrables.

La figura 3.3 se puede llevar a un diagrama más abstracto, pues se debe tener en cuenta que la entidad administradora de red, es una aplicación y no el hardware asociado a ésta. En la figura 3.3, del mismo modo tanto las PCs y los dispositivos de interconexión mostrados en la figura en cuestión tienen instalados agentes, que como ya se mencionó en el capítulo 1, es software que reside en cada dispositivo,

de ahí podemos hacer una representación de bloques de los elementos que constituyen la estructura de administración de red como lo muestra la figura 3.4.



**Figura 3.4** Diagrama de agentes interactuando a través del protocolo SNMP con la entidad de administración de red.

**Nota:** La nomenclatura “A – P” hace referencia al *Access Point* representado en la figura 3.3 y la figura 3.4.

La figura 3.4 deja a un lado el hardware para mostrar el software de administración contenido dentro de cada dispositivo que compone la red de la figura 3.3, donde se muestran los componentes principales de un sistema de administración de red.

### 3.4.1 Elementos principales de un sistema de administración de red, según la “Comunidad Internet”.

- Entidad administradora de red.
- Dispositivos administrados
  - Donde reside el agente.
  - Donde reside la MIB.
- Protocolo de administración

En la siguiente sección se describe de manera general cada componente que forma parte del sistema sugerido por la “Comunidad Internet”.

### 3.4.1.1 Entidad administradora de red

Es una aplicación con control humano que se ejecuta en una estación centralizada denominada centro de operaciones de la red NOC<sup>1</sup> (*Network Operation Center*).

Sus principales características son:

- Se encarga de controlar la recolección, procesamiento, análisis y visualización de la información de administración.
- Es donde se inician las acciones que controlan el comportamiento de la red, y donde el administrador de la red interactúa con los dispositivos de la red

### 3.4.1.2 Dispositivos administrados:

Un dispositivo administrado es un nodo de red que contiene un agente SNMP y reside en una red administrada.

Los dispositivos administrados pueden ser *routers*, servidores de acceso, PCs, *switches*, concentradores, impresoras, etc.

Dentro de cada dispositivo administrado existe un agente el cual se encarga de recoger y almacenar información de administración, la cual es puesta a disposición de la entidad administradora de red usando el protocolo SNMP.

#### 3.4.1.2.1 Agentes

Un agente es un módulo de software de administración de red que reside en un dispositivo administrado.

Un agente posee un conocimiento local de información de administración, la cual es traducida a un formato compatible con el protocolo SNMP. Este agente también se encarga de comunicarse con la entidad administradora de red y actualizar la MIB.

---

<sup>1</sup> Miller, Mark A. *Managing Internetworks With SNMP*. Segunda edición, M&T Books, 1993.

### **3.4.1.2.2 La MIB**

Es una base de datos de información de administración, ésta es una colección de información que está organizada jerárquicamente.

Las MIB's son accedidas usando un protocolo de administración de red, como por ejemplo, SNMP. En el capítulo cinco se hablará de ellas de manera más extensa.

### **3.4.1.3 Protocolos de administración:**

Permite llevar a cabo el ejercicio de la comunicación de la entidad administradora y los agentes que residen en los dispositivos administrados.

- Permite al administrador comunicarse con el agente para conocer el estado de los dispositivos (Permite consultar la MIB).
- Los agentes pueden informar al administrador de situaciones inesperadas en los dispositivos administrados.
- El protocolo no controla por si mismo a los dispositivos administrados, si no que proporciona una herramienta con la que el administrador de red puede administrar la red.

Los dispositivos administrados son supervisados y controlados usando cuatro comandos SNMP básicos: Lectura, escritura, notificación y operaciones transversales.

El comando de lectura es usado por una entidad administradora de red para supervisar elementos de red.

La entidad administradora de red examina diferentes variables que son mantenidas por los dispositivos administrados.

El comando de escritura es usado por una entidad administradora de red para controlar elementos de red. La entidad administradora de red cambia los valores de las variables almacenadas dentro de los dispositivos administrados.

El comando de notificación es usado por los dispositivos administrados para reportar eventos en forma asincrónica a una entidad administradora de red. Cuando cierto tipo de evento ocurre, un dispositivo administrado envía una notificación a la entidad administradora de red.

Las operaciones transversales son usadas por una entidad administradora de red, para determinar qué variables soporta un dispositivo administrado y para recoger secuencialmente información en tablas de variables, como por ejemplo, una tabla de rutas.

Administrar la red hace referencia a:

- Supervisar la red.
- Comprobar la red.
- Sondear la red.
- Configurar la red.
- Analizar la red.
- Evaluar la red.
- Controlar la red
- Entre otras.

Existen varios protocolos de administración que se pueden utilizar para este fin como:

- CMIT/SMOSE.
- SNMP.
- CMOT
- Etc.

Entre todos ellos destaca el protocolo SNMP, por varios motivos tales como: es de fácil implantación, no requiere muchos recursos, es un protocolo abierto y es fácilmente extensible.

Por los motivos ya mencionados y considerando su sencillez de uso y comprensión, es el protocolo de administración más popular hasta el momento y más utilizado por la “Comunidad Internet” para llevar a cabo la administración de redes.

Como el objetivo que se persigue en este trabajo es la implantación del protocolo SNMP dentro de la administración de redes según la “Comunidad Internet”, los componentes de esta filosofía de administración de redes serán ventilados en los siguientes capítulos.



## Capítulo 4 Introducción a Las Buenas Prácticas

---

### 4.1 Introducción

En este capítulo se abordará el uso de las “*Buenas prácticas*” para llevar a cabo en el caso de diseñar la red: un análisis, diseño e implantación de la misma. Para el caso donde ya se cuente con una red, y sólo se requiere, ya sea optimizarla o expandirla, sólo parte de las “*Buenas practicas*” serán implantadas.

Se dará una reseña de los métodos más utilizados en el ámbito de la administración de redes, ya sea en el área de rendimiento, diseño ó procesos, donde se tocarán aspectos como el mapa de red, la topología, los equipos de interconexión, tiempo de procesado, etc.

El impacto de expansión de la red, debe ser reducido al mínimo, es por ello que los niveles de confianza se vuelven estratégicos.

En la obtención de resultados, así como el análisis de los mismos, suele cobrar importancia en el rediseño de la red con la finalidad de lograr la optimización de la red en favor de las necesidades requeridas por la empresa o institución para la cual está siendo implantada ó rediseñada dicha red.

Se debe tomar en cuenta varios parámetros para el rediseño de la red, ya sea por resultados no esperados o para soportar en la medida de lo posible su crecimiento.

### 4.2 El uso de buenas prácticas

Debido a la robustez del modelo de administración de OSI, el modelo de la “Comunidad Internet” ha sido el más aceptado en cuanto a administración de redes se refiere, no obstante, como la parte fundamental de la administración de redes se basa en la comunicación del agente con la entidad administradora de red, a través de un protocolo de comunicación, la “Comunidad Internet” ha dejado a los diseñadores de red, las partes de análisis, diseño e implantación de la red, estos puntos se llevan a cabo con el empleo de lo que se conoce como el uso de “*Buenas Prácticas*”, éstas no son estándares, si no una serie de técnicas recomendadas para la administración, sin llegar a ser una metodología de regla.

La figura 4.1 ilustra las diferentes etapas por las cuales se recomienda pase el proceso de administración de redes según el concepto de “*Buenas prácticas*”, sin embargo, se debe tener especial cuidado en la primer etapa, la de “*Evaluación de necesidades y costos*”, ya que si se cometen errores en ésta, las siguientes etapas arrojarán resultados erróneos, por tanto, esta etapa requiere una atención especial por parte de los administradores de red, pues todas las demás etapas se apoyan en los resultados obtenidos en esta etapa.

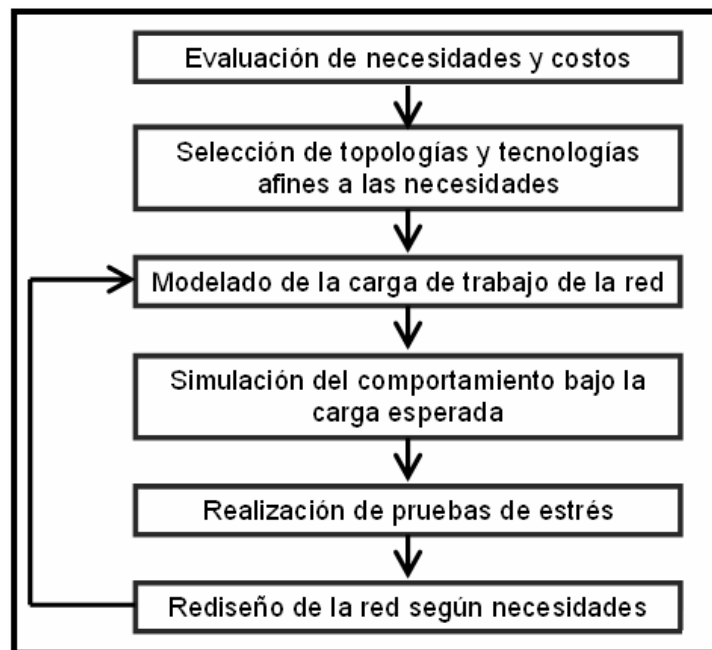


Figura 4.1 Las etapas del uso de buenas prácticas

### 4.3 Evaluación de necesidades y costos

En esta etapa es importante considerar todo lo relacionado con la funcionalidad de la red que va a ser diseñada ó modificada, desde sus necesidades, infraestructura, personal, software, crecimiento, etc.

Se requiere de esta etapa, ya sea para adquirir el equipo necesario o en caso de que la red vaya a ser rediseñada, evaluar la infraestructura existente, para ver cual equipo, según las necesidades de la red será reemplazado o en caso de necesitar alguna otra tecnología, se justifique su adquisición. De igual manera la evaluación del conocimiento del personal, púes es importante contar con los recursos

humanos capacitados para la configuración y resolución de fallos inesperados, y así poder garantizar el correcto funcionamiento de la red.

En seguida se listan los aspectos a considerar y productos requeridos para llevar a cabo una buena evaluación de necesidades y costos:

- **Aspectos a considerar:**
  - Infraestructura actual de hardware.
  - Nivel de conocimiento de los usuarios.
  - Tipo de información que circulará en la red.
  - Aplicaciones propietarias y no propietarias a usar.
  - Crecimiento esperado a corto y mediano plazo.
  
- **Productos requeridos:**
  - Inventario de hardware y software.
  - Perfil del usuario medio de la red.
  - Definiciones de niveles de servicio.
  - Reporte de adquisiciones requeridas.

Una vez que han sido evaluados y satisfechos los aspectos a considerar y analizados los productos requeridos por el administrador de la red, se puede pasar a la siguiente etapa.

#### **4.4 Selección de topologías y tecnologías afines a las necesidades y productos.**

La selección de la topología junto con las tecnologías de interconexión juegan un papel muy importante a la hora de diseñar una red, es por ello que si se selecciona una topología inadecuada según las necesidades de la red y a ésta se le asignan dispositivos de interconexión sin el análisis necesario, se podrán generar dominios de colisión muy grandes en la red y por ello, la red tendrá un rendimiento de operaciones muy bajo, de tal forma que no arrojará los resultados esperados. Si a esto se le suma el descuido de no analizar los medios para transmitir la información en la red, resulta obvio que el tráfico por la carga de trabajo en la red, no será el calculado y por ende no se alcanzarán las velocidades esperadas.

En seguida se listan las características a considerar en el diseño de redes físicas y lógicas:

Cuando se habla de redes físicas se hace referencia a la capa física y de enlace de datos, y cómo será configurada de acuerdo a las topologías existentes, junto con los medios físicos que la constituirán.

- **Características a considerar para una red física.**
  - Tráfico y carga de trabajo esperados sobre el medio de transmisión.
  - Equipos de interconexión.
  - Medios de transmisión disponibles.
  - Velocidades esperadas.
  - Costos de los equipos de interconexión y medios de transmisión.

Al hablar de redes lógicas se hace referencia a:

- **Características a considerar para una red lógica:**
  - Nivel de procesamiento del tráfico esperado sobre software de análisis.
  - Tecnologías afines disponibles de monitoreo y estándares.
  - Costo de tecnologías propietarias.
  - Direccionamiento IP adecuado a las necesidades.

Una vez de haber analizado las características de la red tanto de manera física como lógica, es necesario llevar a cabo un análisis de hardware.

#### **4.4.1 Análisis de requerimientos de hardware y software.**

En esta parte se lleva a cabo todo lo que tiene que ver con la parte tangible e intangible de la red, es por ello que los siguientes puntos son imprescindibles:

- Inventario de Hardware
- Inventario de IP's
- Descubrimiento de red
- Análisis del modelo actual del tráfico de red.
- Determinación de niveles de confianza.
- Consideraciones de capacidad.
- Consideraciones de implementación.
- Costos de adquisición y mejora

#### 4.4.2 Inventario de hardware

En este punto se debe considerar:

- Marca y modelo:
  - Usados para buscar información sobre el dispositivo.
- Cantidad de memoria RAM:
  - Impacta en la capacidad y el rendimiento de los dispositivos.
- Carga de trabajo:
  - Determinar condiciones de uso excesivo o de poco uso de los dispositivos.
- Interfaces de red:
  - Redes y subredes conectadas al dispositivo de interconexión.
  - Tipo de enlace de cada una de las conexiones.
  - Unidad máxima de transferencia MTU (*Maximum Transfer Unit*) de cada interfaz

Esta información proporciona una idea de cómo se conecta el dispositivo a la red, ayudando a tener un panorama general de ésta.

#### 4.4.3 Inventario de direcciones IP

Si la red ya existe se debe hacer un inventario de direcciones IP, con la finalidad de conocer cuales son las direcciones IP en uso y ver si es posible llevar a cabo un mejor direccionamiento IP de los equipos que componen la red.

#### 4.4.4 Descubrimiento de red

El inventario de hardware por sí solo refleja la infraestructura de una forma atómica. Es por ello que se necesita realizar un descubrimiento de toda la red para tener un panorama global de la infraestructura física, y de esta manera poder analizar los cambios a realizar, en dispositivos particulares.

Ello implica hacer un mapa de la red, sí la red ya existe tenemos dos formas de hacerlo:

- **Descubrimiento automático (Software):**

- Ahorra tiempo y trabajo.
- Depende de la disponibilidad de la red.
- Requiere de configuración particular.
- Puede servir para la administración futura.

- **Descubrimiento manual:**

- Requiere de tiempo y trabajo.
- Necesita un sistema de consulta eficiente.
- Es personalizado.

Si la red no existe, el mapa se obtiene al momento de estar diseñando la red en cuestión.

#### **4.4.5 Modelado del tráfico de la red.**

Teniendo ya todo el modelo o mapa físico de la red, es importante observar qué tipo de tecnologías son usadas para controlar el tráfico de la red y los dispositivos que implantan dichas tecnologías.

Se debe detectar la existencia de dispositivos que estén dedicados a un cierto tipo de tráfico, y en que segmento de red se encuentran.

Se debe evaluar la necesidad de utilizar diferentes segmentos de red para cada tipo de tráfico, así como cuales son los dispositivos adecuados para cada segmento con su tipo de tráfico.

#### **4.4.6 Determinación de los niveles de confianza**

Se llama nivel de confianza al estado que guarda cierto dispositivo o conjunto de dispositivos (en un segmento) con relación al estado ideal de dicho dispositivo o segmento de red, considerando aspectos como:

- Funcionalidad.
- Disponibilidad.
- Seguridad

#### **4.4.6.1 Nivel de confianza alto**

Este nivel de confianza es dado a aquellos equipos ó segmentos de red que cuentan con las últimas versiones de software disponibles, así como las últimas actualizaciones de las mismas y es por ello que debe cumplir con los siguientes puntos:

- El dispositivo funciona de acuerdo a lo que se requiere de él.
- Se espera que conserve su funcionamiento ideal aún en situaciones extraordinarias.
- Rebasa el grado de disponibilidad adecuado para su funcionalidad.
- Se considera que no puede comprometer la seguridad de la red.
- No requiere de configuración o mejoras en caso de un cambio moderado en la red.

Es de destacarse que el hardware asociado a este dispositivo debe ser basto para el soporte del software que trabajará sobre éste.

#### **4.4.6.2 Nivel de confianza medio**

Los distintos dispositivos que se encuentran en este nivel deben tener como característica que cumplan con los requerimientos mínimos para desempeñar la función para la cual fueron adquiridos tomando en cuenta los siguientes puntos:

- El dispositivo es capaz de obtener el nivel de confianza alto, por mejoras y/o configuración.
- Cuenta ya con una disponibilidad cercana o igual a la mínima para su funcionalidad.
- No se encuentra comprometiendo la seguridad de la red.
- Se debe generar un informe de cómo llevar al dispositivo a un nivel de confianza alto.
- En caso de necesitar una mejora, el costo no debe ser excesivo.

#### **4.4.6.3 Nivel de confianza bajo**

Este nivel de confianza es para aquellos dispositivos que por razones de compatibilidad con nuevas tecnologías no pueden ser actualizados. Por ejemplo existe cierto software que requieren de sistemas operativos nuevos los cuales no

pueden ser cargados en el dispositivo, pues el nuevo hardware requerido para ello, no es compatible con la arquitectura de este dispositivo.

Los siguientes puntos son muy usuales en un dispositivo de nivel de confianza bajo:

- Las especificaciones del dispositivo no le permiten adquirir un nivel alto de confianza.
- Se considera muy costoso o muy difícil llevar al dispositivo a otro nivel de confianza.
- Se encuentra comprometiendo la seguridad de la red en su totalidad.
- Ha alcanzado su tiempo de vida con una carga media o alta de trabajo.
- Existen situaciones externas que impiden el funcionamiento o mejora del dispositivo

Es importante dedicar suficiente tiempo para definir las tecnologías y requerimientos que un dispositivo debe tener para poder tener un nivel alto de confianza.

Al principio se considera que todo dispositivo tiene un nivel nulo ó bajo de confianza, ya con el perfil alto definido, se otorga por comparación un nivel a cada dispositivo.

Los dispositivos que por cualquier motivo conserven un nivel nulo ó bajo tras la comparación, deben ser descartados de la infraestructura.

### **4.4.7 Consideraciones de capacidad**

Una vez establecido el nivel alto de confianza, y con el modelo objetivo de tráfico de la red, debe considerarse si los dispositivos, cual sea su nivel de confianza, tienen las capacidades para soportar las tecnologías y carga de trabajo que requiere el modelo de tráfico de la red, así como el impacto que puede tener en el dispositivo.

#### **Tecnologías con un alto uso de recursos:**

- Algoritmos tipo HASH.
- IPv6, entre otros.



### **Servicios que requieren gran ancho de banda: Pasar a la siguiente hoja**

- Monitoreo de red.
- Voz sobre IP

Una vez reconocidas aquellas tecnologías relacionadas con la capacidad de los dispositivos, se debe analizar el impacto que tendrán en los dispositivos.

Como resultado del análisis, el nivel de confianza de ciertos dispositivos puede bajar. Aunque se considere a un dispositivo muy capaz, su nivel de confianza no debe subir si no cumple con las necesidades de nivel de confianza del nivel superior a éste, según las necesidades establecidas para cada nivel de confianza.

### **4.4.8 Consideraciones de implantación**

En este punto se debe tomar en cuenta todo lo que tiene que ver con los siguientes puntos:

- Dispositivos con uso excesivo.
- Dispositivos incompatibles.
- Dispositivos mal configurados.
- Direccionamiento lógico incorrecto

### **4.4.9 Evaluación de costos**

- Mejora de equipo existente:
  - Se consideran los dispositivos con un nivel de confianza medio, y se estima el costo total para llevarlos a un nivel de confianza alto.
- Adquisición de nuevo equipo:
  - Se cotizan dispositivos que cumplan con el perfil de confianza alto, para remplazar aquellos con nivel bajo de confianza y/o para cubrir necesidades faltantes.
- El estimado total considerando mejoras y adquisiciones, sirve como base para establecer las necesidades de hardware.

**Se debe tomar en cuenta que resulta mejor: Pasar a la siguiente hoja**

- Sí adquirir un equipo con un perfil alto de confianza.
- Sí invertir en mejorar equipos con niveles medios o incluso bajos de confianza.

Al final de cuentas, se debe tener un balance costo-beneficio en el estimado total.

#### **4.5 Rendimiento de los dispositivos de la red.**

Una vez seleccionadas las tecnologías según las necesidades ó requerimientos de la red, se prosigue a la evaluación del rendimiento. Generalmente los diseñadores y administradores de redes llevan a cabo una simulación del comportamiento de la red con herramientas de software, capaces de modelar el comportamiento de todo tipo de redes, incluyendo los elementos como: *routers*, *switches*, concentradores, protocolos, etc.

#### **4.6 Modelado de la carga de trabajo de la red.**

Llegado a este punto, donde ya se tiene la red lógica y la red física, y por consiguiente ya se cuenta con el mapa de la red en donde se ha definido la topología, el número de PCs u equipos afines, impresoras, equipos de interconexión, etc. Es el momento de someter a la red al procesado de las actividades de una empresa o institución para la cual fue diseñada según las necesidades de la misma.

Para ello utilizaremos técnicas de modelado como las del estándar: mapa de operaciones de telecomunicaciones eTOM (*enhanced Telecom Operations Map*).

##### **4.6.1 El modelo de negocios eTOM**

El eTOM, es un modelo de procesos de negocio, una estructura generalizada que describe todos los procesos requeridos por una proveedora de servicios SP (*Service Provider*), analizándolos en diferentes niveles de detalle. Para cualquier empresa, sirve como un punto de partida para el control de procesos y provee de un marco de referencia para la reingeniería de procesos, de acuerdo a las necesidades, relaciones internas, alianzas y acuerdos de trabajo. eTOM resalta las funciones requeridas, entradas y salidas.

El propósito de eTOM es proporcionar una visión que permita competir exitosamente a través de la implementación de la administración de procesos de negocios. eTOM se convierte en una herramienta útil para planificadores, administradores y estrategas; haciendo énfasis en una estructura, componentes de procesos, interacciones de los mismos, roles y responsabilidades; proporcionando un conjunto de requerimientos para la solución de sistemas, arquitecturas, tecnologías e implementación.

**eTOM describe los procesos de las empresas de la siguiente manera:**

- Se comienza con la descripción general de la empresa.
- Se definen los procesos de negocios en una serie de agrupaciones, empleando una jerarquización.
- Se lleva a cabo una descomposición de los procesos para estructurarlos y así obtener los procesos de negocios más detallados.

**La descomposición de procesos, incluye:**

- La administración de las relaciones con los clientes.
- Las relaciones existentes desde el marketing hasta la facturación
- El servicio de soporte después de las ventas.
- Entre otros.

El modelo eTOM a nivel conceptual se muestra en la figura 4.2.

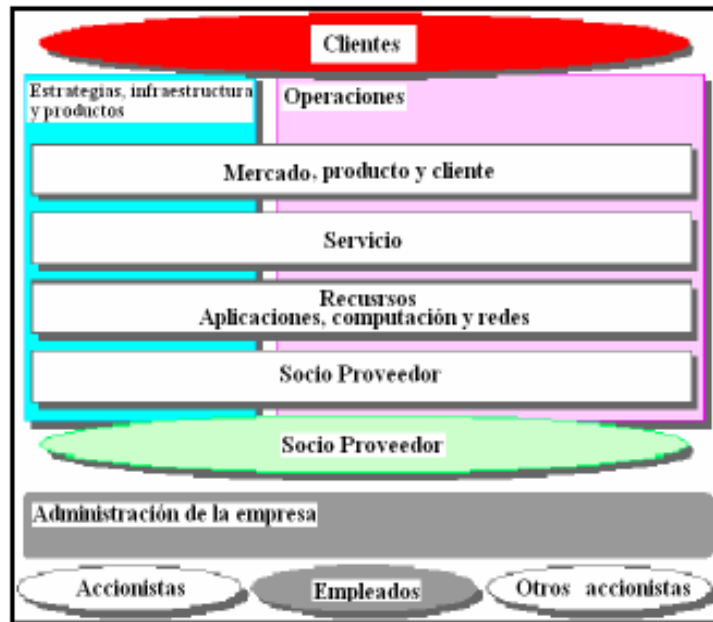


Figura 4.2 Modelo eTOM, nivel conceptual

Los niveles conceptuales de eTOM, son vistos en tres áreas de procesos, las cuales se describen a continuación.

**A) Operaciones:**

El área de procesos de operaciones, es el corazón de eTOM, incluye todos los procesos de operaciones que soportan las aplicaciones de los clientes y su administración. Por ejemplo: aquellas operaciones que se establecen directamente con el cliente. La vista de operaciones en el modelo eTOM, incluye la administración de ventas y el manejo de relaciones socio-proveedores.

**B) Estrategia, Infraestructura y Productos:**

Esta área incluye procesos que desarrollan estrategias, construcción de infraestructura, desarrollo y administración de productos, así como la administración de la cadena de proveedores.

**C) Administración de la empresa:**

Es un área que incluye procesos básicos de negocios, requeridos para el correcto funcionamiento de una empresa. Dichos procesos están enfocados sobre el nivel empresarial, objetivos y propósitos, teniendo relación con la mayoría de los otros procesos dentro de la empresa, como el área de operaciones, estrategia, infraestructura y productos. Ejemplos de estos procesos son: la administración financiera, la administración de recursos humanos, etc.

En la actualidad, la administración de redes se incluye en el modelo eTOM, donde los procesos de soporte de operación, activación de servicios, aprovisionamiento y facturación, permiten tener un control total de la infraestructura de la red, desde la relación con el cliente o usuario final, hasta su facturación o direccionamiento de costos a diferentes departamentos (procesos agrupados en forma vertical) y desde el control de dispositivos hasta el manejo de negocios (procesos agrupados en su forma horizontal).

#### **4.6.2 Diseño del modelo del proceso de negocios**

En seguida se lista una metodología que nos permite modelar un proceso.

- a) Requerimientos del proceso.
- b) Definición del flujo del proceso.
- c) Creación del modelo del proceso.
- d) Definición de los actores.
- e) Asignación de las tareas.
- f) Simulación del flujo del modelo del proceso.

#### **4.6.3 Requerimientos del proceso de negocios**

En esta fase se estudia el objetivo del proceso, de tal forma que una vez entendido el proceso en su totalidad, pueda ser dividido en actividades y subprocesos, para tratar cada uno de éstos de manera individual, con la finalidad de darles un análisis y una solución propia a cada actividad y subproceso.

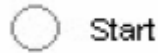
#### **4.6.4 Definición del flujo del proceso**

El objetivo de esta etapa es definir la secuencia del flujo de las diferentes actividades y subprocesos del proceso del negocio, relacionando cada paso con su actividad y subproceso.

Una vez comprendida cada actividad y subproceso, así como su jerarquización, se procede a la construcción del diagrama de flujo que representa al proceso en su totalidad.

#### 4.6.5 Componentes de un diagrama de flujo en el proceso de negocios eTOM. Pasar a la siguiente hoja

1. El Símbolo de la figura 4.3 sirve para iniciar el diagrama de flujo.



**Figura 4.3 Inicio del proceso**

2. El Símbolo de la figura 4.4 nos indica la representación de una actividad, en él se incluye tanto el personal involucrado, así como las diferentes tecnologías para llevar a cabo dicha actividad.



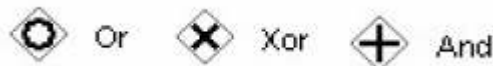
**Figura 4.4 Procesado de una actividad**

3. El símbolo de la figura 4.5, nos sirve para unir diferentes alternativas, como por ejemplo actividades y subprocesos, en este símbolo no solo se agrega el nombre de la decisión a tomar, si no que también se le asigna un porcentaje que indica la probabilidad de que se lleve a cabo dicha actividad conectada a esta decisión.



**Figura 4.5 Elección de alternativas**

4. Los símbolos de la figura 4.6 indican que se llevará a cabo una operación lógica con las entradas correspondientes y proporcionará una salida de la operación seleccionada.



**Figura 4.6 Operaciones lógicas**

5. El símbolo de la figura 4.7, representa el final de todo el proceso del modelado de negocios.



**Figura 4.7 Fin del proceso.**

Cada uno de los elementos se unen entre sí a través de ramas.

En los elementos de decisión, las ramas llevan el nombre de la decisión tomada.

Es importante destacar que a cada actividad y subproceso se le debe de asignar un tiempo de procesado, para saber si las tecnologías ó el personal son las adecuadas, dependiendo del tiempo requerido, se lleva a cabo la toma de decisiones.

Una vez diseñado el diagrama de flujo, tomando en cuenta cada actividad y subproceso junto con todos los elementos que cada uno de éstos implica, se lleva a cabo la simulación del modelo.

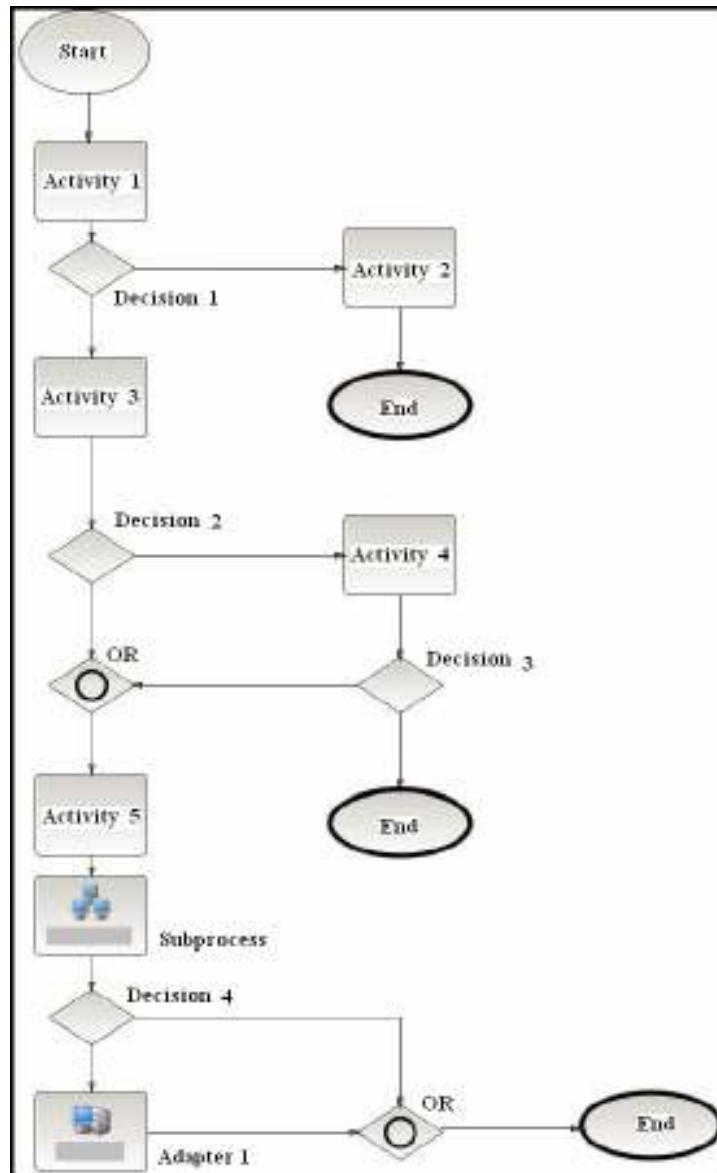


Figura 4.8 Modelado de un proceso

En la figura 4.8 se muestra un diagrama de flujo que ilustra un proceso cualquiera.

Para llevar a cabo la simulación existen diferentes herramientas de software..

Como se ha podido observar, en este trabajo se utilizan algunas técnicas del modelado eTOM sin profundizar en toda su estructura. Si el lector está interesado



en conocer más a detalle el modelado eTOM se le recomienda ir a <http://www.itsm.org/>, pues en este trabajo no se ahondará más en dicho modelado.

#### **4.7 Simulación del comportamiento de la red bajo la carga de trabajo esperada.**

Una vez hecho el diagrama de flujo con los elementos de eTOM sobre el software de simulación y simulado el proceso en el software, se obtendrán resultados, los cuales pueden ser los esperados o no esperados, aunque también estos resultados nos pueden dejar ver algunos detalles que no fueron considerados a la hora de diseñar la red, no obstante, este es el objetivo de la simulación.

La interpretación de la información obtenida en la simulación puede darnos las bases para llevar a cabo la toma de decisiones necesarias y correspondientes para la optimización de la red en diseño o en expansión.

#### **4.8 Realización de pruebas de estrés.**

Generalmente este tipo de prueba se lleva a cabo cuando la red en cuestión existe. Para la realización de las pruebas de estrés, se utiliza otro software, el cual sirve para medir la carga de trabajo. Cuando ésta se sale de los límites esperados, se utilizan los datos obtenidos para un rediseño futuro ó inmediato de la red.

#### **4.9 Rediseño de la red según las necesidades**

Después de haber sometido a las diversas simulaciones y haber realizado las pruebas de estrés, a la red que se esta diseñando, generalmente siempre se requiere hacer algún tipo de ajuste a dicho diseño. De ser así se debe regresar a la etapa de modelado de la carga de trabajo de la red.

En el caso de que la red ya exista y en ella se practique la prueba de estrés, es posible que la red se encuentre trabajando con un tráfico que supera al previsto originalmente. Esta situación llevará al análisis de los datos obtenidos y con ello se hará necesario regresar a la etapa de modelado de carga de trabajo, para un rediseño óptimo de la red en cuestión.

#### **4.10 Retroalimentación al modelado de carga de trabajo.**

Pasar a la siguiente hoja

Una vez analizados todos los resultados obtenidos en las etapas anteriores, se recomienda regresar a la etapa de “*Modelado de carga de trabajo*” con la finalidad de hacer los ajustes necesarios para optimizar la red que se está diseñando, en algunos casos cuando no se ha tenido el suficiente cuidado en la etapa de “*Evaluación de necesidades y costo*” se tendrá que regresar más atrás es decir a la etapa de “*Selección de topologías y tecnologías afines a las necesidades*”.

#### **4.11 Productos obtenidos después del uso de las “*Buenas prácticas*”.**

La siguiente lista muestra lo que se debe obtener al emplear las “*Buenas prácticas*” dentro de la administración de redes:

- Esquema físico de la red.
- Modelo de tráfico esperado de la red
- Perfiles de niveles altos de confianza.
- Inventario de hardware utilizable.
- Inventario de direcciones IP.
- Presupuesto de adquisiciones y mejoras de tecnologías.

Como se puede inferir, el uso de las “*Buenas Prácticas*” corresponde al diseñador de la red en cuestión y la parte de la comunicación de una entidad administradora con el nodo administrado le corresponde al modelo propuesto por la “Comunidad Internet”. No obstante, es necesario que el nodo administrado cuente con una base de datos que contenga la información referente a dicho nodo para poder llevar a cabo la administración del dispositivo. Esta base de datos se denomina MIB, la cual se describe en el siguiente capítulo.

## **5.1 Introducción**

En este capítulo se hablará a cerca del estándar ANS.1 como lenguaje formal para la implantación de las instrucciones de la MIB.

De igual forma en este capítulo se dará una breve reseña de la estructura de información de administración SMI, así como, una breve explicación de cómo navegar a través del árbol de registros, que es la representación de dicha estructura.

En el árbol de registro existen diferentes nodos los cuales pertenecen a diferentes organizaciones de estandarización, uno de ellos es el nodo “mib - 2” el cual tiene como prefijo 1.3.6.1.2.1.

El estándar MIB es un estándar mundial, no obstante, se puede ampliar por fabricantes de dispositivos, y por ello se darán definiciones de las diferentes MIBs.

Se mencionarán las diferencias entre objeto e instancia ó variable de objeto, así como, la estructura de los grupos de dichos objetos dentro de la MIB – II.

## 5.2 Sintaxis ANS.1

Antes de entrar en la definición, descripción y utilización de la MIB es necesario dar una reseña acerca del lenguaje formal que sirve para definir las estructuras de datos de la MIB.

La Notación de Sintaxis Abstracta ANS.1 (*Abstract Syntax Notation One*), es un lenguaje formal desarrollado y estandarizado por el comité internacional de consulta de telégrafos CCIT X.208 (*International Telegraph Consultative Comite X.208*) e ISO 8824. Este lenguaje puede ser usado para definir sintaxis abstractas de aplicaciones de datos, sin embargo, no es usado con esos propósitos. En la práctica ANS.1 es usado para definir la estructura de las aplicaciones y presentación del protocolo de unidad de dato (PDU), del mismo modo puede ser usada para definir la información de administración del protocolo SNMP.

ANS.1 es un lenguaje formal que puede ser usado para definir estructuras de datos.

La sintaxis abstracta se utiliza para describir tanto las estructuras de datos que intercambian las entidades del protocolo SNMP como la información de administración que contienen estas estructuras de datos.

Junto con el concepto de sintaxis abstracta, existe el concepto de sintaxis de transferencia. Esta última permite, a partir de la definición de las estructuras de datos, utilizar una forma determinada de transmisión de datos a través de la red. La sintaxis de transferencia que se utiliza junto con la ANS.1 son las reglas de codificación básicas BER (*Basic Encoding Rules*).

Sí bien se usa ANS.1 para la sintaxis abstracta, dado que esta notación es muy extensa, se restringe su uso para mantener la simplicidad de los agentes.

El análisis y la implantación del lenguaje ANS.1, así como la explicación de las reglas de codificación básica BER quedan, fuera de los objetivos de este trabajo, es por ello que sí el lector requiere saber más acerca del lenguaje formal ANS.1 y las reglas BER, se le recomienda consultar la obra “*SNMP, SNMPv2, SNMPv3 and RMON 1 and 2*” de William Stalling Third Edition de la editorial Addison Wesley.

### 5.3 SMI Estructura de información de administración

El objetivo de especificar una estructura de la información de administración consiste en poder referenciar a un recurso en un sistema remoto. Pero para ello se requiere una serie de elementos, como un protocolo IP que nos permite llegar al sistema remoto, y un protocolo como SNMP que nos permite llegar al proceso de administración de red del sistema remoto. Sin embargo, existe un problema: ¿Cómo llegar a los recursos del sistema remoto?, para ello se va a utilizar un método común para nombrar los objetos. Este método usa el concepto de identificadores de objetos (*Object Identifier, OID*).

La figura 5.1 ilustra lo expuesto en diagrama a bloques, donde se muestran las diferentes etapas de la estructura de información.

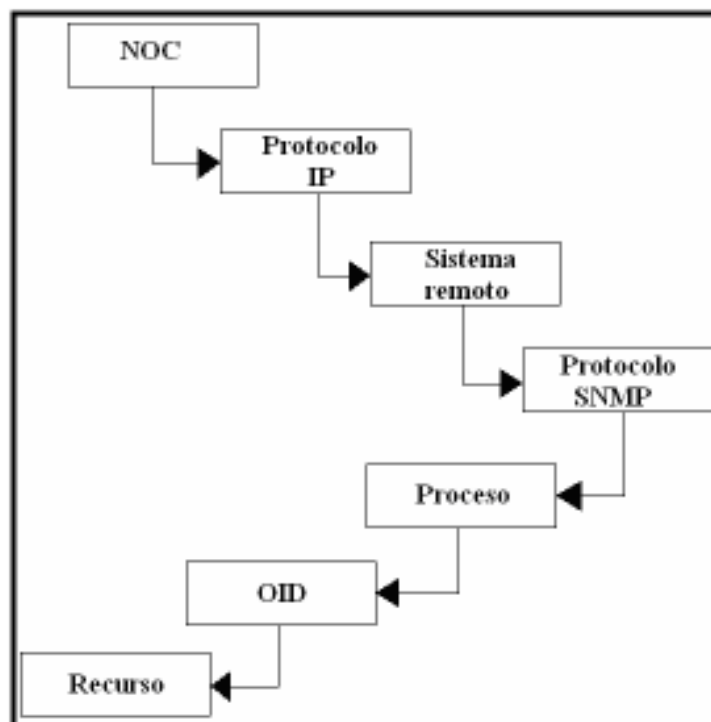


Figura 5.1 Diagrama a bloques para alcanzar un recurso remoto en la red.

Los OID son una secuencia de enteros no negativos separados por un punto que forman un árbol. Este árbol denominado de registro, está estandarizado a nivel mundial.

El árbol de registro está formado por ramas y nodos. En cada nodo existe una etiqueta que consistente en un número entero y quizás un texto breve. Cada nodo puede tener nodos hijos (subordinados o sub - *identifiers*), conectados a éste mediante líneas (ramas).

El árbol comienza con un nodo inicial denominado *root* que se puede extender hasta cualquier nivel de profundidad.

Los OIDs son los que permiten nombrar y alcanzar objetos mediante el protocolo SNMP, pero ¿cómo devolver los valores de los objetos? o dicho de otra forma ¿cómo responder a una operación “*Get*”? (ésta y otras operaciones se ventilarán el capítulo 6). Para que ello sea posible es necesario conocer la estructura de los valores OIDs que nos pueden llegar desde los objetos, es decir la Macro OBJECT -TYPE.

Es de suma importancia destacar que en este trabajo se explica la estructura de información de administración con la finalidad de ubicar a la MIB, objetivo de este capítulo, si el lector desea saber más acerca de esta estructura se le recomienda consultar el RFC 1155.

Se hace notar que los identificadores de los objetos ubicados en la parte superior del árbol, por encima del nodo “*Internet*” pertenecen a diferentes organizaciones de estándares, mientras los identificadores de los objetos ubicados en la parte inferior del nodo “*Internet*” del árbol son colocados por las organizaciones asociadas, como se puede observar en la figura 5.2.

### **5.3.1 Búsqueda de un grupo de objetos en la SMI conociendo el OID**

A manera de ilustrar cómo se navega a través del árbol de registro se propone buscar el grupo de objetos “*directory*”, el cual tiene un OID = 1.3.6.1.1, no obstante, se debe tener en cuenta que “*directory*” es un grupo de objetos (nodo), no un objeto.

Para tener un mayor entendimiento de cómo navegar en el árbol, nos auxiliaremos de la figura 5.2. Lo primero que se tiene que hacer es dirigirse al nodo raíz “*root*”, una vez allí, se toma el primer dígito del OID, en este caso en particular es el ‘1’, el cual nos dirige al nodo etiquetado como “*iso (1)*”, posteriormente tomamos el siguiente dígito, el cual es el ‘3’, éste nos lleva al nodo etiquetado “*ISO identified organization (3)*”, después se toma nuevamente el siguiente dígito el cual es el ‘6’,

éste nos lleva al nodo “US DoD (6)”, aplicando el mismo proceso para el siguiente dígito, el cual es el ‘1’, llegamos al nodo “Internet (1)”, por último para este caso en particular tomamos el dígito siguiente, el cual es el ‘1’ para llegar al grupo de objetos buscado “directory”.

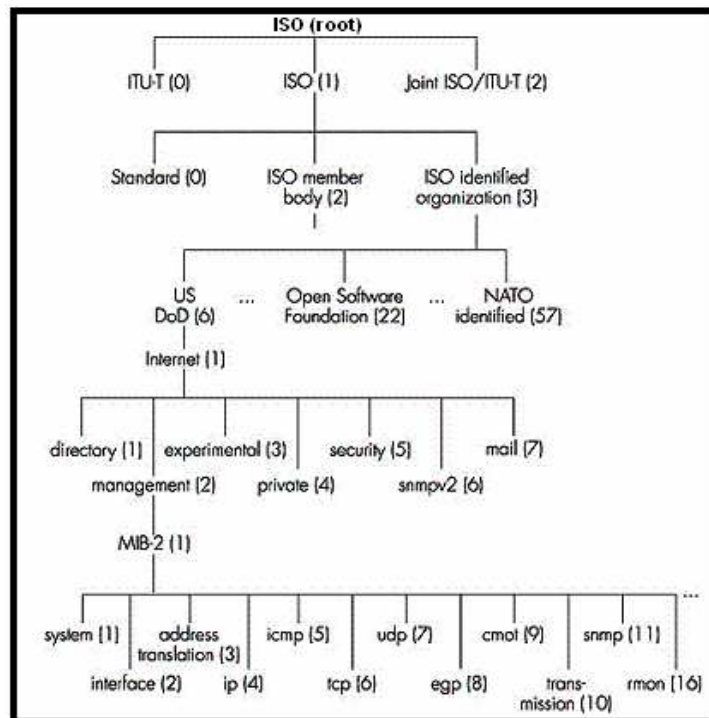


Figura 5.2 Árbol de registro SMI

#### 5.4 Localización de la MIB en el árbol de registro

La jerarquía MIB es un nodo del árbol de registros, la cual cuenta con once subnodos. Para encontrar cualquier objeto dentro de la MIB siempre se comenzará con el prefijo 1.3.6.1.2.1 como lo muestra la figura 5.2.

A manera de ilustrar lo anterior, digamos que queremos encontrar el grupo de objetos “system”.

La ruta que tendremos que seguir es la siguiente:

- 1.3.6.1.2.1.1

El lector debe notar que encontramos el grupo de objetos “system”, no un objeto en particular.

## 5.5 Objetos administrados

Este apartado presenta la definición formal de los objetos que componen la MIB – II.

En la terminología de la administración de redes se habla de objetos y de instancias de objeto ó variables.

- Una instancia de objeto o variable es un elemento particular de un objeto.

### 5.5.1 Un objeto consta de lo siguiente:

- Un nombre el cual se conoce como OID.
- Atributos:
  - Un tipo de datos.
  - Una descripción detallada del objeto.
  - Información de estatus: si es definición actual u obsoleta.
- Operaciones validas sobre el objeto: Lectura y/ó escritura.

### 5.5.2 Algunos ejemplos de objetos administrados son:

- Descripción de un sistema.
- Tiempo de respuesta en operación.
- La dirección IP de las interfases de un router.

### 5.5.3 Ejemplo de definición de un objeto:

Definición formal del objeto *sysDescr* (*system description*) como se especifica en el RFC 1213 (*Request for Comment 1213*), es la siguiente:

```
sysDescr OBJECT – TYPE
    SYNTAX DisplayString (SIZE (0...255))
    ACCES read-only
    STATUS mandatory
    DESCRIPTION
```



“Una descripción textual de la entidad, este valor debe incluir el nombre completo y la identificación de versión del tipo de hardware del sistema, el sistema operativo software y el software de red, es obligatorio que sólo contenga caracteres ASCII imprimibles.”

`::= {system 1}`

La MIB define los objetos de la red operados por el protocolo de administración de red, y las operaciones que pueden aplicarse a cada objeto.

En seguida se dará una breve explicación de cada uno de los elementos que definen un objeto:

- *sysDescr*: Se refiere a la descripción del sistema.
- *Sintaxis*: Especifica el tipo de datos de la variable, entero, cadena dirección IP, etc.
- *DisplayString*: Especifica una cadena de objetos, utilizada para modelar información textual tomada del juego de caracteres ASCII. Por convención, los objetos con esta sintaxis se dice que tienen un tamaño de (0..255).
- *OBJECT – TYPE*: Es una macro, la cual tiene la siguiente expansión:

### Macro para la definición de objetos

---

<pre>IMPORTS ObjectName FROM RFC1155-SMI        DisplayString FROM RFC1158-MIB; OBJECT-TYPE MACRO ::= BEGIN   TYPE NOTATION ::=     "SYNTAX" type(ObjectSyntax)     "ACCESS" Access     "STATUS" Status     DescrPart     ReferPart     IndexPart     DefValPart   VALUE NOTATION ::= value (VALUE     ObjectName)</pre>	<pre>Access ::= "read-only"   "read-write"             "write-only"   "not-accessible" Status ::= "mandatory"   "optional"   "obsolete"             "deprecated" DescrPart ::= "DESCRIPTION" value              (description DisplayString)   empty ReferPart ::= "REFERENCE" value (reference              DisplayString)   empty</pre>
--	--

Sí el lector requiere conocer más a cerca de esta macro se recomienda consultar el RFC 1212.

- *PhyAddress*: Es una cadena de octetos, este tipo de datos se usa para modelar direcciones de medios, para muchos tipos de medios será una representación binaria, por ejemplo una dirección Ethernet, representada con una cadena de 6 octetos.
- *Acces*: Especifica el nivel de permiso como: Leer, leer y escribir, escribir, no accesible.
- *Status*: Define si la variable es obligatoria u opcional.
- *Descripción*: Describe textualmente a la variable.
- *System 1*: El '1' indica que es el primer objeto de del grupo "System".

La figura 5.3 muestra otro ejemplo de la declaración de un objeto en la jerarquía MIB – II, en este caso se trata del objeto "tcpMaxConn", el cual tiene un OID: 1.3.6.1.2.1.6.4, su nodo padre es "tcp".

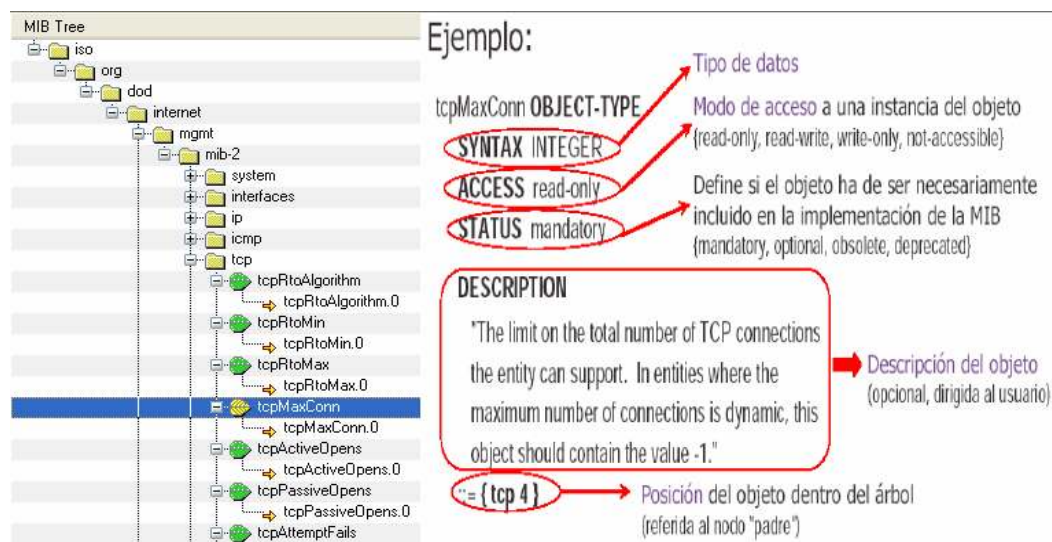


Figura 5.3 Declaración del objeto "tcpMaxConn"

### 5.5.4 Estructura de información ISO-CCITT

La ISO y el CCITT promovieron la idea de estructurar la información en un árbol global de nombres y asignar un identificador a cualquier objeto que necesitase un nombre, este árbol se muestra en la figura 5.2.

El subárbol “Internet” bajo el nodo “DoD” (*Department of Defense de los EUA*), es propiedad de la tabla de actividades de Internet IAB (*Internet Activities Board*) y es administrado por la asociación de de asignadores de números de Internet IANA (*Internet Assigned Numbers Assosiation*). Las estructuras administrativas de información y de nombres están integradas en ese esquema global.

### **5.5.5 Identificadores de objetos e Instancias**

Un objeto administrado, algunas veces llamado objeto MIB ó simplemente objeto, es una de las características específicas de un dispositivo administrado.

Los objetos administrados están compuestos de una o más instancias que son esencialmente variables.

Existen dos tipos de objetos administrados: Escalares y tabulares.

#### **5.5.5.1 Los objetos escalares:**

Éstos definen una simple instancia de objeto.

#### **5.5.5.2 Los objetos tabulares:**

Éstos definen múltiples instancias de objeto relacionadas, que están agrupadas conjuntamente en tablas MIB.

Los objetos que se requieren administrar son subnodos del árbol ISO – CCITT. A cada uno se le asigna una etiqueta que consiste en un entero y una breve descripción textual. El identificador de objeto es una serie de enteros que marcan la trayectoria que va desde la raíz del árbol hacia el objeto. Por ejemplo, el identificador del objeto “*sysDescr*” es: 1.3.6.1.2.1.1.1 o en forma textual `iso_org_dod_internet_mgmt_mib-2_system_sysDescr`.

Un OID indica la clase de objeto que se requiere conocer.

Un identificador de instancia ó nombre de variable se utiliza para obtener el valor preciso que se necesita. Por ejemplo, en el caso del objeto “*sysDescr*” donde la instancia sería “*sysDescr.0*”, debido a que no tiene más que sólo un elemento (la descripción del sistema) el identificador de instancia es el identificador del objeto más un ‘0’, agregado al final de la serie de enteros: 1.3.6.1.2.1.1.1.0. En caso de

que el objeto tuviera varios elementos por ejemplo el estatus de las interfaces de un router. Los valores de las variables de cada interfaz serian recuperados agregando números consecutivos a cada interfaz.

La figura 5.4 ilustra el grupo de objetos “system”, el objeto “sysDescr” y la instancia “sysDescr.0”, en el árbol presentado por la aplicación MG - SOFT.



Figura 5.4 Árbol de la MIB, grupo system.

## 5.6 La MIB - II

Toda la información del agente se guarda en la base de datos denominada MIB, ésta base de datos forma una estructura de árbol, donde la raíz es el nodo mib - 2.

La estructura donde se guarda la información de un dispositivo en particular se denomina por la base de datos de información de administración MIB (Management Information Base), la cual es consultada por un agente a petición de la entidad de administración de la red.

La MIB – II describe una MIB estándar para administrar entidades de Internet basadas en TCP/IP.

Desde su creación la MIB – II se ha convertido en la MIB básica para manejar todos los dispositivos basados en TCP/IP de Internet.

La MIB – II define 10 grupos de objetos de administración, cada grupo incluye objetos para administrar distintas entidades de protocolos TCP/IP. Por ejemplo el grupo TCP incluye contadores y tablas relacionadas con el funcionamiento del

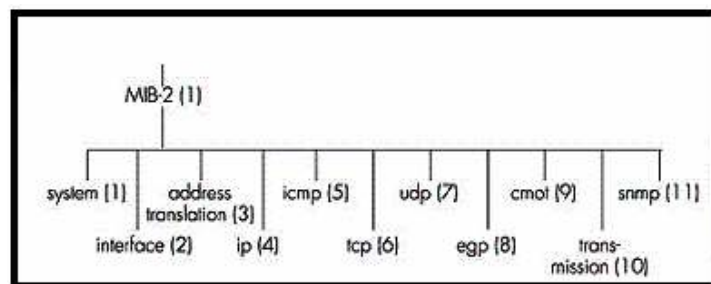
modulo TCP dentro de un dispositivo de Internet y el grupo IP incluye contadores y tablas relacionadas con el funcionamiento del modulo IP.

Aunque la MIB – II se presenta como un solo conjunto de definiciones, no se requieren dispositivos administrados para implantar cada objeto MIB. Más bien, se permite una funcionalidad opcional en el nivel del grupo de objetos.

Sí un dispositivo administrado implanta cualquier objeto de un grupo, deberá implantar todos los objetos del grupo; no obstante, no se requiere que el dispositivo implante grupos que no tienen sentido para el objeto concreto.

Por ejemplo las computadoras estándar de Internet no implantan EGP (Exterior Gateway Protocol) y por tanto no requieren implantar el grupo EGP.

La figura 5.5 muestra los once grupos de objetos que pertenecen a la MIB – II.



**Figura 5.5 Grupos de objetos MIB**

Como ilustra la figura 5.5 existen once grupos de objetos definidos de manera universal; no obstante, los vendedores pueden definir ramas privadas que incluyen los objetos administrados para sus propios productos.

Las MIBs que no han sido estandarizadas típicamente están localizadas en la rama experimental, como lo muestra la figura 5.3.

El corazón de la jerarquización del árbol MIB se encuentra compuesto de varios grupos de objetos, los cuales en su conjunto son llamados “mib-2”, como se puede observar en la tabla 5.1.

**Los grupos son los siguientes:**

Grupos	Identificador de objetos
System	OBJECT IDENTIFIER ::= {mib - 2 1}
Interfaces	OBJECT IDENTIFIER ::= {mib - 2 2}
AT	OBJECT IDENTIFIER ::= {mib - 2 3}
IP	OBJECT IDENTIFIER ::= {mib - 2 4}
ICMP	OBJECT IDENTIFIER ::= {mib - 2 5}
TCP	OBJECT IDENTIFIER ::= {mib - 2 6}
UDP	OBJECT IDENTIFIER ::= {mib - 2 7}
EGP	OBJECT IDENTIFIER ::= {mib - 2 8}
CMOT	OBJECT IDENTIFIER ::= {mib - 2 9}
Transmission	OBJECT IDENTIFIER ::= {mib - 2 10}
SNMP	OBJECT IDENTIFIER ::= {mib - 2 11}
.....	

**Tabla 5.1 Grupos de objetos en el nodo mib - 2**

**NOTA:**

La nomenclatura AT representa al grupo de objetos: *Address Traslation*.

### **5.6.1 Las Diferentes Clases de Módulos MIB.**

Existen tres tipos de módulos MIB:

- **Estándar:** Diseñados por un grupo de trabajo del **IETF** y estandarizado por el grupo de ingenieros de Internet **IESG** (*Internet Engineering Steering Group*). Los prefijos de los identificadores de objetos se encuentran bajo el subárbol mgmt.
- **Experimental:** Mientras un grupo de trabajo desarrolla una MIB, los identificadores de objetos temporales se colocan bajo el subárbol experimental. Si el MIB adquiere la condición de estándar, se colocan los identificadores bajo el subárbol mgmt.
- **Privadas:** La mayor parte de las empresas desarrollan módulos MIB propios que soporten ciertas características particulares, las cuales no son generalmente contempladas en los módulos MIB estándar.

## 5.7 Ampliación de la MIB

Ampliar la MIB se refiere a la capacidad de la MIB de almacenar nuevos elementos. Si un fabricante quiere añadir un nuevo comando a un dispositivo, como puede ser un router, tan sólo tiene que añadir las variables correspondientes a su base de datos (MIB).

Casi todos los fabricantes implementan versiones de agente del protocolo SNMP en sus dispositivos como: routers, concentradores, sistemas operativos, etc.

En este capítulo se dio una introducción a la base de datos MIB, la cual es imprescindible a la hora de llevar a cabo la administración de un dispositivo remoto. No obstante el lector se a de pregunta ¿cómo se lleva a cabo la interacción de un dispositivo remoto con la entidad administradora de red? y más aún ¿cómo se mueven los valores de esta base de datos MIB? Entre otras cuestiones. Pues bien, esto se lleva a cabo mediante el protocolo SNMP del cual se hablara en los siguientes tres capítulos.

## 6.1 Introducción

En este capítulo se aborda el funcionamiento del protocolo SNMP, actualmente el protocolo de administración más utilizado en las redes que cuentan con la estructura de protocolos *TCP/IP*, la cual es la principal tecnología para interconexión de redes heterogéneas.

Un sistema de administración de red basado en el protocolo SNMP está compuesto por los siguientes elementos:

- Varios agentes, o nodos administrados
- Al menos una estación de administración (*NOC*),
- Un cierto volumen de información relativa a los dispositivos administración (MIB)
- Un protocolo para la transmisión de dicha información entre los agentes y las estaciones de administración (SNMPvX).

Los mecanismos utilizados para definir la información relativa a los dispositivos administrados apenas han sufrido modificaciones desde su aparición a finales de los años 80. Uno de los objetivos principales de su diseño fue la flexibilidad, de modo que la información definida pudiese seguir siendo utilizada posteriormente por protocolos diferentes, o incluso por distintas versiones del mismo protocolo.

Uno de los requerimientos fundamentales del diseño del protocolo SNMP fue la sencillez, lo que si bien facilitó su expansión en perjuicio de protocolos más complejos, como por ejemplo CMIP, ha hecho necesarias varias revisiones para adaptar el protocolo SNMPv1 a las necesidades actuales, entre las que cabe destacar las exigencias en cuanto a la seguridad del sistema de allí la aparición del protocolo SNMPv2 y SNMPv3.



## 6.2 Evolución de SNMP

Las primeras aproximaciones a la administración de Internet aparecieron en marzo de 1987 con una serie de protocolos como el protocolo simple de monitoreo SGMP (*Simple Gateway Monitoring Protocol*), el alto sistema de administración de entidad HEMS (*High – Level Entity Management System*) y el protocolo de información de administración común sobre TCP CMOT (*Common Management Information Protocol over TCP/IP*). Sobre TCP/IP Estos protocolos de administración se ocupaban básicamente del buen funcionamiento de los nodos de encaminamiento, como los *routers* centrales del conjunto de redes en Internet.

Posteriormente en febrero de 1988, se produjeron una serie de revisiones para actualizar el protocolo SGMP, que dieron origen a SNMPv1, pero no fue hasta agosto del mismo año cuando aparecieron realmente las primeras recomendaciones del protocolo SNMPv1, así como de la SMI y la MIB, desde el principio SNMPv1 tuvo mucho éxito, si bien no dejaba de ser un protocolo de monitorización principalmente. Hubo en marzo de 1991 nuevas revisiones del entorno, que dieron lugar a una nueva especificación de la base de datos MIB-I las cuales arrojaron como resultado a la MIB-II. Fue a partir de ahí que diversos fabricantes se dieron a la obtención de MIBs particulares que permitían la compatibilidad entre plataformas de administración en entornos de red heterogéneos, dado que SNMPv1 era esencialmente un protocolo abierto.

Posteriormente en mayo de 1993 el grupo IETF sacó una nueva versión más completa del protocolo denominada SNMPv2 con diversas versiones y un éxito relativo. Finalmente en el verano de 1998 se anunciaban los primeros documentos con una nueva versión SNMPv3 más avanzada.

El concepto de SNMPv1 será expuesto en este capítulo, pero la introducción a SNMPv2 y SNMPv3, serán descritos en los capítulos 7 y 8 respectivamente, mientras que el concepto de monitoreo remoto RMON no será expuesto en este trabajo, lo único a mencionar que es un estándar para monitoreo de redes, si el lector requiere saber más acerca de RMON se le recomienda ir a la obra de Stalling Williams. *SNMP, SNMPv2, and RMON: Practical Network Management*, segunda edición, 1996.

La figura 6.1 muestra diagrama de la evolución histórica del protocolo SNMP,

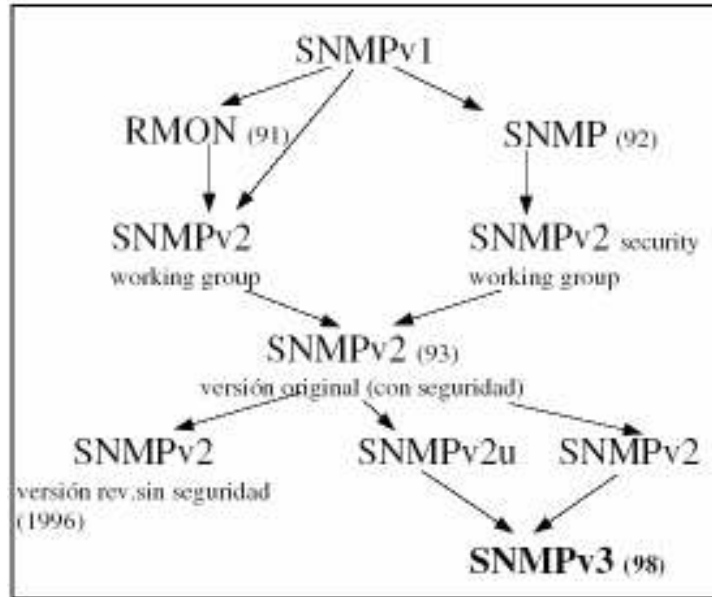


Figura 6.1. Evolución histórica de protocolo SNMP

### 6.3 Simple Network Management Protocol

En términos generales el protocolo SNMPv1 es el mecanismo mediante el cual se comunica la entidad administradora NMS (*Network Management System*) con los agentes (*Agents*) de los nodos administrados de una red heterogénea.

SNMPv1 es un protocolo que opera en el nivel de aplicación, utilizando el protocolo de transporte UDP/IP, por lo que ignora los aspectos específicos del hardware sobre el que funciona. La administración se lleva a cabo a nivel de capa de aplicación, no obstante se utilizando el protocolo IP para llevar a cabo el *ruteo*, por lo que se pueden controlar dispositivos que estén conectados en cualquier red accesible desde Internet, y no únicamente aquellos localizados en una red local específica.

SNMPv1, si bien es un protocolo abierto, también puede utilizarse con un agente *Proxy* para administrar sistemas propietarios. Cabe destacar también que en SNMP la comunicación con los agentes no está orientada a conexión y que al ser un protocolo basado en UDP/IP no garantiza la llegada de los mensajes y “*TRAPS*” (Serán explicados más adelante) a su destino, con lo que se tiene que integrar un conjunto de mecanismos especiales en capas superiores para evitar estas deficiencias, dichos mecanismos salen de los objetivos de este trabajo, es por ello que no se hablará más acerca de ellos.

El protocolo SNMPv1 se sitúa en el tope de la capa de transporte del modelo de referencia OSI como lo muestra la figura 6.2, o por encima de la capa UDP de la pila de protocolos TCP/IP, como lo ilustra la figura 6.3.

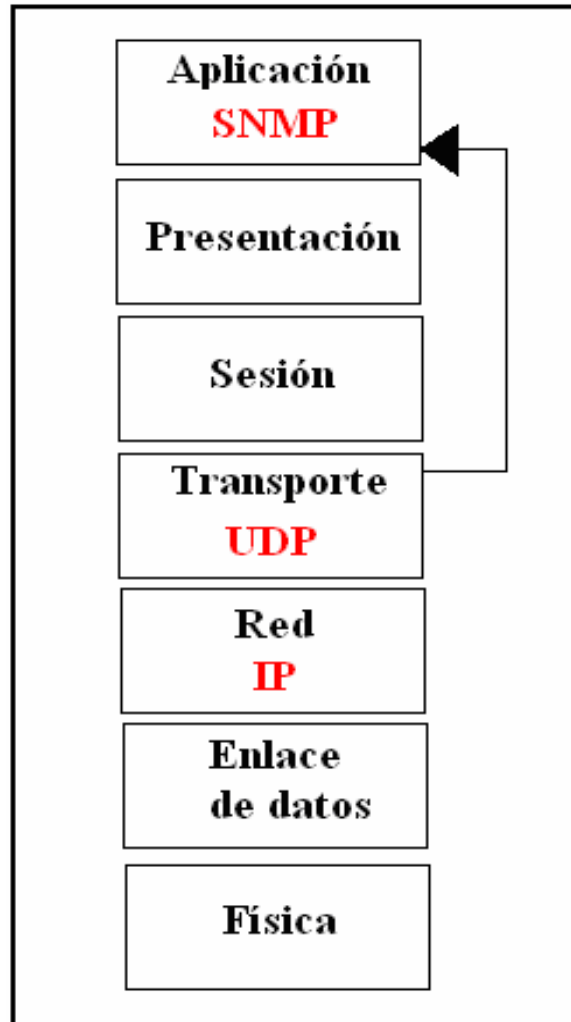


Figura 6.2 Modelo de referencia OSI

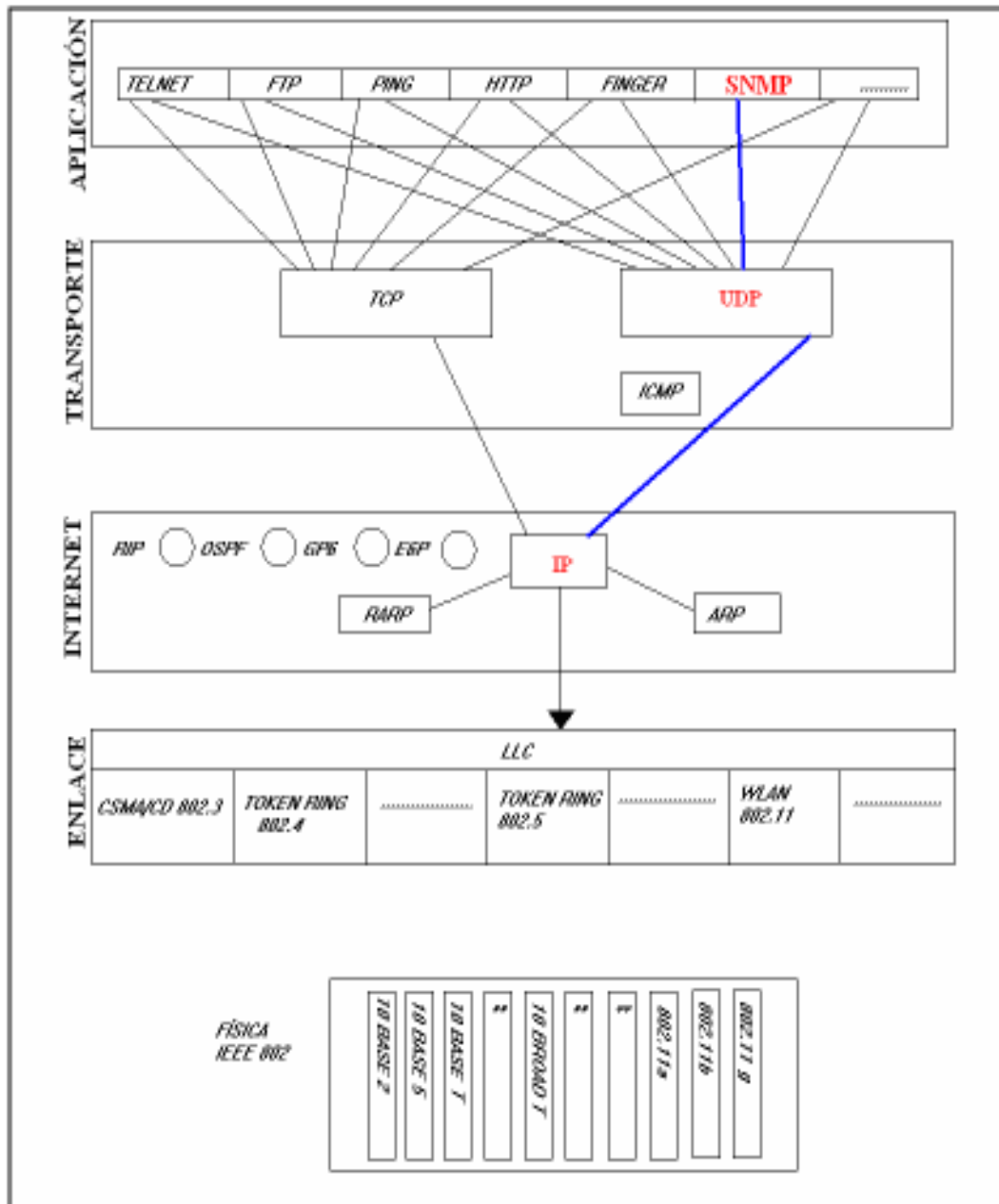


Figura 6.3 Pila de protocolos TCP/IP

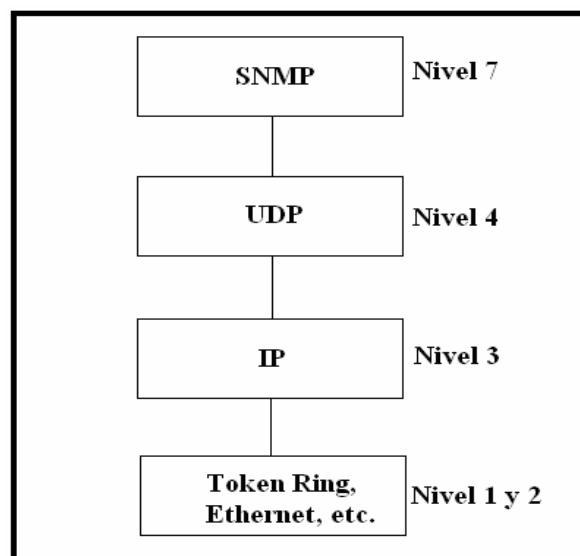
SNMPv1 necesita debajo de él, el soporte de la capa de transporte UDP, pues ésta le provee de lo siguiente:

- Multiplexación.
- Demultiplexación de servicios.
- Checksum para confiabilidad.

SNMPv1 necesita de la capa de Internet IP lo siguiente:

- Ruteo entre redes.
- Fragmentación y reensamblado de paquetes.

La figura 6.4 muestra la pila de comunicaciones SNMPv1, la cual se apoya en la estructura de protocolos TCP/IP de Internet.



**Figura 6.4 Torre de protocolos en Internet**

El protocolo SNMPv1 comunica a dos elementos:

- El agente (*agent*)
- Estación de administración de red (NMS).

El protocolo SNMPv1 es una arquitectura cliente-servidor, en la cual el agente desempeña el papel de servidor y el administrador hace el papel de cliente.

El agente es un programa que se ejecuta en cada nodo de la red que se desea administrar o monitorizar, éste se encarga de comunicar con la estación de administración de red y actualizar la base de datos denominada MIB, la cual se explicó en el capítulo 5.

Los agentes residen en **NODOS ADMINISTRADOS**, que son dispositivos tales como computadoras, *routers*, adaptadores de redes LAN, módems, concentradores, multiplexores, impresoras, etc.

Tienen las siguientes funciones:

- Recuperar información de administración de los objetos que controlan.
- Alterar los valores de los objetos.
- Recibir mensajes de peticiones, mandar respuestas y “*Traps*” de los objetos, y enviarlos, a su vez, a las NMS.

Los agentes ofrecen un interfaz de todos los elementos que se pueden configurar. Estos elementos se almacenan en la MIB, que representa la parte del servidor, en la medida que tiene la información que se desea administrar y esperan comandos por parte del cliente que es la estación administradora de red.

La estación administradora de red: es el software que se ejecuta en la estación encargada de monitorizar la red, y su tarea consiste en consultar los diferentes agentes que se encuentran en los nodos de la red, con el fin de consultar los datos que éstos han ido obteniendo.

En esencia, el SNMPv1 es un protocolo muy sencillo puesto que todas las operaciones se realizan bajo el paradigma de carga-y-almacenamiento (*load-and-store*), lo que permite un juego de operaciones reducido.

### 6.5 Operaciones de SNMPv1

El protocolo SNMPv1 es eminentemente un protocolo simple y de monitorización. A continuación se definen los tipos de operaciones permisibles con sus objetos:

- GetRequest: Petición de valores específicos de la MIB.
- GetNextRequest: Proporciona un medio para moverse por la MIB, es la petición de un objeto siguiente a uno dado de la MIB.

- GetResponse: Devuelve los valores solicitados por las operaciones anteriores.
- SetRequest: Permite asignar un valor a una variable.

Hay un comando especial en SNMPv1, llamado “TRAP”, que permite a un agente enviar datos que no han sido solicitados de forma explícita a la estación de administración de red, para informar de eventos tales como: errores, fallos en la alimentación eléctrica, reinicio de algún dispositivo, exceso de tráfico, etc.

Un administrador puede realizar sólo dos tipos diferentes de operaciones sobre un agente: leer o escribir un valor de una variable en la MIB del agente. Estas dos operaciones se conocen como petición-de-lectura (*get-request*) y petición-de-escritura (*set-request*). Hay un comando para responder a una petición-de-lectura llamado respuesta-de-lectura (*get-response*), que es utilizado únicamente por el agente.

La figura 6.5 ilustra la relación que existe entre los diversos tipos de operaciones de SNMPv1 y los nodos administrables, es decir, el papel de administrador (lado izquierdo) y el papel de agente (lado derecho).

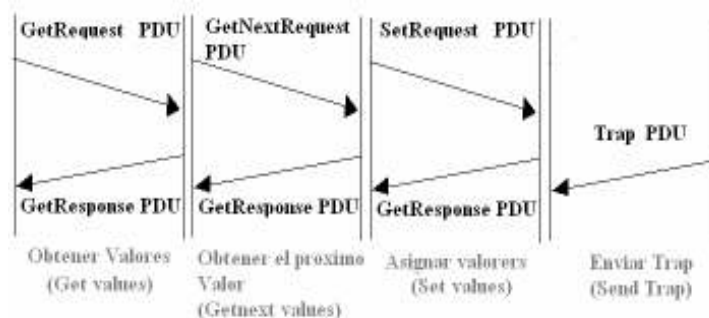


Figura 6.5 Relación Entre el NMS y el Agente.

## 6.6 Unidad de Dato de Protocolo PDU (Protocol Data Unit)

Se define como la unidad de datos de protocolo que es como se denomina a todo el conjunto de bits que llevan la información necesaria para que un mensaje SNMP pueda ser transportado por la red.

Se utiliza para el intercambio entre unidades pares, dentro de una capa del modelo OSI. Existen dos clases de PDUs:

- PDU de datos, que contiene los datos del usuario final (en el caso de la capa de aplicación).
- PDU de control, que sirven para gobernar el comportamiento completo del protocolo en sus funciones de establecimiento y ruptura de la conexión, control de flujo, control de errores, etc.

El uso de las MIBs privadas junto con mensajes de tipo “*TRAP*”, permiten la respuesta del sistema a alarmas específicas de los equipos de cada fabricante. Además, se posibilita la integración de agentes en multitud de dispositivos para su administración.

La definición de las variables MIB soportadas por un agente en particular se almacenan en archivos descritos en la notación especial denominada ANS.1 con la finalidad de que puedan ser utilizadas por programas clientes de administración de red de otros fabricantes como se explicó en el capítulo 3.

Es importante destacar algunos conceptos para el mejor entendimiento de la transmisión y recepción de mensajes SNMPv1:

**Entidad SNMP:** Es una "entidad lógica" a través de la cual un agente o una aplicación de administración están procesando un mensaje.

**Autenticación:** Se refiere a cómo las entidades SNMP identifican sus mensajes.

Cuando una entidad comienza una comunicación, es configurada para suministrar credenciales de autenticación como una parte de la comunicación. Dependiendo de los mecanismos de autenticación, serán válidas tres clases de servicios:

- A) **Identificación origen:** A través de esta clase un mensaje puede ser asociado con una entidad origen.
- B) **Integridad del mensaje:** Por ésta un mensaje alterado puede ser detectado con seguridad.
- C) **Protección limitada de retransmisión:** Por ésta, un mensaje que ha sido duplicado o retrasado en la red u otra entidad puede ser detectado fuera del tiempo de vida esperado del mensaje.

**Privacidad:** Se refiere a cómo las entidades SNMPv1 protegen sus mensajes.

Para lograr privacidad con seguridad, deberíamos usar un algoritmo de encriptación y la clave asociada.



**Autorización:** Se refiere a cómo una entidad agente SNMPv1 determina los objetos que son accesibles a una entidad de aplicación de administración dada, y las operaciones que se pueden realizar en estos objetos.

Cuando un agente ejecuta una operación, primero deberá identificar la colección de recursos de objetos de administración a monitorizar. Si los recursos son accesibles mediante algún mecanismo local, se dice que la operación se desarrolla desde el punto de vista de la MIB, el cual es normalmente un conjunto adecuado de todos los objetos administrados y controlados por una entidad. En cambio, si los recursos son accesibles mediante el envío de mensajes SNMPv1 a una entidad remota, entonces se dice que los objetos son válidos a través de una relación *Proxy*.

Una vez que los recursos son identificados, sólo resta determinar las operaciones SNMPv1 empleadas en ellos. A esto se denomina *Política de Acceso*, y es usada para el control del flujo de información entre la entidad agente SNMPv1 y una entidad de aplicación de administración de red dada.

**Comunidad:** Se define como una relación entre un agente y un administrador en un entorno SNMPv1. Una comunidad SNMPv1 se escribe como una cadena de octetos sin interpretación. Esta cadena se llama *nombre de comunidad*. Cada octeto toma un valor entre 0 y 255.

Cuando se intercambian mensajes SNMPv1, contienen tres partes:

- **Versión:** Este campo hace referencia al tipo de versión de SNMPv1 que se está empleando al construir la PDU del mensaje SNMPv1.
- **Una cadena de comunidad:** Esta cadena es mandada en texto sencillo.
- **SNMP PDU:** Estos datos contienen a la operación SNMPv1 y los operandos asociados.

A continuación se describe la secuencia de eventos que se produce en la emisión y recepción de un mensaje SNMPv1 por parte de la entidad de administración de red.

## 6.7 Secuencia de transmisión de un mensaje SNMPv1

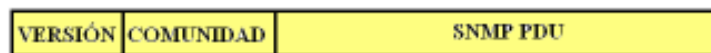
### 1. Construcción de la PDU.

Usando conocimiento local, la entidad origen comienza seleccionando la comunidad apropiada, la cual tiene la autorización adecuada para usar las operaciones y el acceso a los objetos MIB deseados. Posteriormente una estructura de mensaje es construida desde esta información. La figura 6.6 muestra la representación del bloque de la PDU del mensaje SNMPv1.



**Figura 6.6 Bloque de la PDU del mensaje SNMPv1**

2. La PDU se procesa por el servicio de autenticación junto a las direcciones correspondientes.
3. La entidad de protocolo construye el mensaje, que consiste en una versión, el nombre de la comunidad y el resultado del paso 2, como lo muestra la figura 6.7.



**Figura 6.7 Formato a bloques del mensaje SNMPv1**

4. El paso 3 da origen a un nuevo objeto ANS.1, éste es entonces codificado, usando las reglas de codificación básicas BER y pasando al servicio de transporte. La figura 6.8 muestra el bloque del objeto ANS.1.



**Figura 6.8 Diagrama de bloque del objeto ANS.1**

## 6.8 Secuencia de recepción de un mensaje SNMPv1.

Cuando un paquete es recibido del servicio de transporte se llevan a cabo los siguientes pasos:

1. Revisión básica de la sintaxis del mensaje, descartándolo si es erróneo.
2. Verificar el número de versión:
  - 2.1 Si no es una versión implantada por la entidad receptora, el paquete es descartado.
  - 2.2 Sí la versión del mensaje refiere a una versión implantada por la entidad receptora, entonces se revisa la comunidad del mensaje para ver si se refiere a una conocida a la entidad receptora.
    - 2.2.1 Si la comunidad no es conocida, el paquete es descartado.
    - 2.2.2 Sí la comunidad es conocida, ésta es revisada para ver si tiene autorización para utilizar la operación contenida en los datos del mensaje.
      - 2.2.2.1 Si no tuviera autorización, el paquete se descarta.
      - 2.2.2.2 Sí tiene autorización, entonces la entidad receptora revisa que clase de recursos de objetos están asociados con la comunidad.

Si la comunidad se refiere a recursos de objetos locales, entonces la operación se desarrolla de acuerdo con las MIBs apropiadas asociadas con la comunidad.

En cambio si la comunidad se refiere a recursos de objetos remotos, entonces:

- Si la operación es una respuesta, entonces guarda relación con la anterior petición, y una respuesta es enviada a la entidad que hizo la petición.
  - Si la operación es una Trap o un informe, entonces el agente *Proxy*, usando conocimiento local, determina la entidad SNMPv1 que debería enviar el mensaje.
  - De otra forma, la petición se propaga por la relación *Proxy* definida por la comunidad.
3. La entidad de protocolo pasa al usuario la porción PDU del mensaje y las direcciones de transporte del emisor y receptor al servicio de autenticación.
    - 3.1 Si la autenticación falla, el servicio de autenticación señala a la entidad de protocolos SNMPv1, para que genere un TRAP y descarte el mensaje.

- 3.2 Si la autenticación tiene éxito, el servicio de autenticación devuelve la PDU en la forma de objeto ANS.1
4. La entidad de protocolo hace una revisión básica de la sintaxis del mensaje, descartándolo si es erróneo.

En cualquier caso, la comunidad nombrada con la adecuada política de acceso SNMPv1 seleccionada finalmente procesará la PDU.

## 6.9 Tipos de mensajes SNMPv1

La secuencia de emisión y recepción de los mensajes SNMP derivan en lo que se conoce como “*Formato de mensajes SNMPv1*”, los cuales se muestra en las figuras 6.9.1, 6.9.2 y 6.9.3



Figura 6.9.1 Formato del mensaje SNMPv1

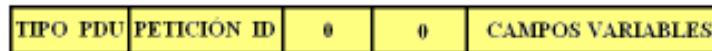


Figura 6.9.2 PDUs de operaciones GetRequest, GetNextRequest y SetRequest.

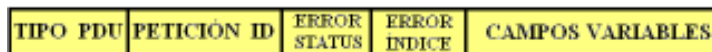


Figura 6.9.3 PDU de la operación GetResponse.

Es importante señalar que la localidad “*CAMPOS VARIABLES*” tiene su propio formato como lo muestra la figura 6.10.



Figura 6.10 Formato de la localidad Campos Variables.

Enseguida se dará una breve explicación de cada campo de los mensajes del protocolo SNMPv1.

**Tipo de PDU:** Puede ser de datos ó de control.

**Petición ID:** Valor entero usado por la aplicación para distinguir entre peticiones pendientes, provee a cada solicitud “*Get*” ó “*Set*” una única *ID*, lo que permite a la aplicación mandar rápidamente varios mensajes SNMPv1, reconocer mensajes duplicados en la red. Los agentes no pueden modificar este campo.

**Error – Status:** Sí no es cero, representa un error al procesar la petición y que debería ignorarse el “*Campo Variable*”. Por lo tanto es usado para indicar que una excepción ocurrió mientras se procesaba una petición como:

noError	(0)
toobig	(1)
noSuchName	(2)
badValue	(3)
readOnly	(4)
getError	(5)

**Error – Índice:** Si no es cero, proporciona información para indicar qué variable en una lista causó la excepción.

**Campos Variables:** Lista de variables, con su nombre y valor.

**Nombre:** Hace referencia a un nombre de variable.

**Valor:** El nombre de variable es acompañado de este valor.

La figura 6.11 muestra las diferentes secciones que componen un mensaje del protocolo SNMPv1 de transmisión ó petición, es importante hacer notar que las líneas que unen un formato con otro, indican la expansión de una sección del mensaje SNMPv1.

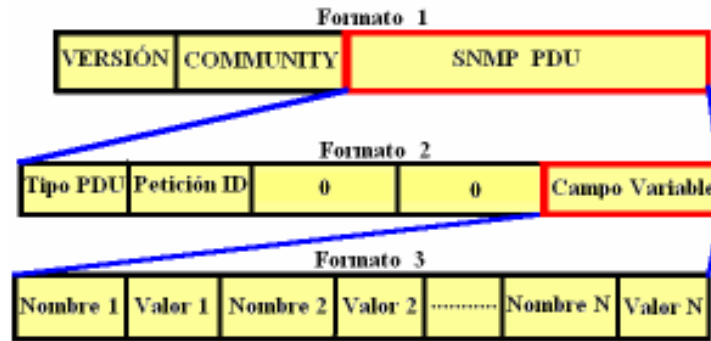


Figura 6.11 Formato del mensaje SNMPv1 de petición

La figura 6.11 muestra un mensaje de transmisión de la entidad administradora de red, la cual está pidiendo la ejecución de alguna de las siguientes operaciones:

- *GetRequest.*
- *GetNextRequest.*
- *SetRequest.*

La entidad administradora de red es la única que puede enviar este tipo de mensajes con las operaciones mencionadas, cabe destacar que cada mensaje enviado por esta entidad, es para una sola operación.

En seguida se describirá brevemente la expansión del mensaje de transmisión del protocolo SNMPv1.

Como ya se explicó en la sección 4.7 de este capítulo, lo primero que se hace al transmitir un mensaje SNMPv1 es construir la PDU, posteriormente se le asigna la versión y la comunidad a dicha PDU, no obstante, la PDU que es creada, tiene sus propios campos como son:

- Tipo de PDU.
- Petición ID.
- Error Status => 0
- Error Índice => 0
- Campo Variable.

Nota: Los campos “*Error Status*” y “*Error Índice*” son puestos a cero cuando se envía un mensaje de petición “*Get*” ó “*Set*”.

Como se puede observar en la figura 6.11 del mismo modo el formato 2 contiene un campo expansible que es el “*Campo Variable*”, el cual hace referencia a un conjunto de variables y cada una de éstas posee un valor propio de dicha variable.

En la sección 6.8 de este capítulo se describió el proceso a través del cual se lleva a cabo la recepción de un mensaje SNMPv1 por un agente residido en un determinado nodo administrado.

La figura 6.12 ilustra la estructura del mensaje del protocolo SNMPv1 de respuesta, es decir, cuando el agente responde al mensaje enviado por la entidad administradora de red.

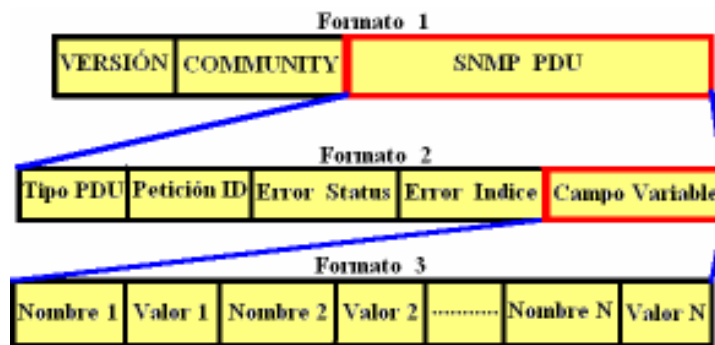


Figura 6.12 Formato del mensaje SNMPv1 de respuesta

La figura 6.12 muestra un mensaje de respuesta de un agente administrado a una entidad administradora de red, el cual está mandando un informe acerca del estado del dispositivo administrado, para ello utiliza la operación:

- SetResponse.

En seguida se describirá brevemente la expansión de respuesta de un agente a la petición de la entidad administradora de red.

Como ya se explicó en la sección 6.8 de este capítulo, lo primero que se hace un agente al recibir un mensaje SNMPv1 es verificar la sintaxis del objeto ANS.1, posteriormente verificar la versión y la comunidad en la PDU, así como autenticar los permisos de comunidad, si todo el proceso de recepción tuvo éxito, se procede a atender la petición y enviar la respuesta de la misma.

Se debe señalar que los campos del formato 2 de la figura 6.12 son los mismos que su homólogo en la figura 6.11, y por ello los campos siguen siendo los mismos:

- Tipo de PDU.
- Request ID.
- Error Status.
- Error Índice.
- Campo Variable.

Nota: Aquí los campos “Error Status” y “Error Índice” pueden tener valores distintos a cero cuando se envía un mensaje de respuesta “Trap”.

Como se puede observar en la figura 6.12 del mismo modo el formato 2 contiene un campo expansible que es el “*Campo Variable*”, el cual hace referencia a un conjunto de variables y cada una de éstas posee un valor propio de cada variable.

Se debe tener en cuenta que no todas las respuestas de un agente pueden ser informes, pues cabe la posibilidad de algún evento inesperado, en un determinado nodo administrado. Este evento inesperado puede obedecer condiciones como la falla de energía eléctrica, que el dispositivo haya sido reiniciado, que el dispositivo este fallando, excedente de tráfico, etc.

La figura 6.13 ilustrará el cambio de los campos en el formato 2 de la mencionada figura.

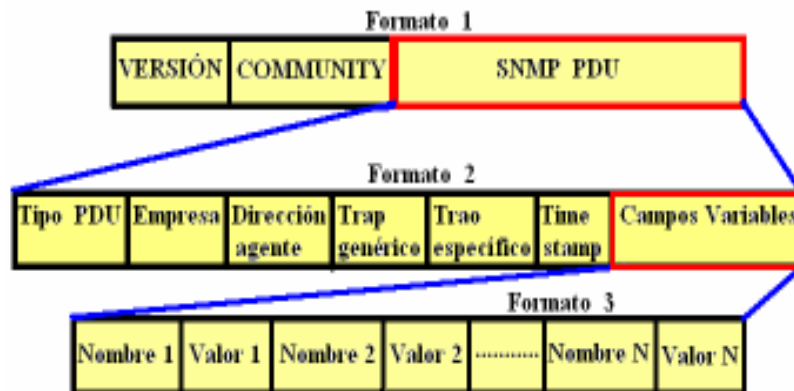


Figura 6.13 Formato de un Trap en SNMPv1



Enseguida se describirán los campos que contiene la PDU de un mensaje de tipo Trap enviado por un agente:

- *Empresa*: Tipo de objeto que generó el trap.
- *Dirección agente*: Dirección IP del objeto que generó el trap.
- *Trap genérico*: Devuelve un valor de alguno de los siguientes traps:

coldStar	(0)
warmStart	(1)
linkDown	(2)
linkUp	(3)
authenticationFailure	(4)
egpNeighborLoss	(5)
enterpriseSpecific	(6)

- *Trap específico*: Es un código específico de trap.
- *Time-stamp*: Tiempo transcurrido entre la última reinicialización de una entidad de red y la generación del trap.

Cabe hacer notar que el agente administrado es el único que puede enviar este tipo de mensajes con las dos operaciones mencionadas (GetResponse, Trap), se debe destacar que cada mensaje enviado por esta entidad, es para una sola operación.

### 6.10 Definición en lenguaje ANS.1 del mensaje SNMP

En seguida se muestra el código de un mensaje SNMP en ASN.1

```
RFC 1157 – SNMP ::= BEGIN
IMPORTS
ObjectName, OBJECTSyntax, NetworkAddress, IPAddress, TimeTicks
FROM RFC1155 – SMI;

--Mensaje

Message ::= SEQUENCE { version INTEGER {version-1 (0)},          -- version 1 para este RFC
Community OCTET STRING , -- Nombre comunidad data ANY} -- Es una autenticación usada
para la PDU

-- Unidades de datos del protocolo

PDUs ::= CHOICE {
get-request      GetRequest-PDU,          get-next-request  GetNextRequest-
PDU,          get-response      GetResponse-PDU,          set-request
SetRequest-PDU,          trap              Trap-PDU
}
```

### --PDU

GetRequest-PDU ::= [0] IMPLICIT PDU      GetNextRequest-PDU ::= [1] IMPLICIT PDU

GetResponse-PDU ::= [2] IMPLICIT PDU

SetRequest-PDU ::= [3] IMPLICIT PDU

PDU ::= SEQUENCE {

request-id INTEGER,  
error-status INTEGER {                    -- A veces ignorado  
noError                    (0)  
toobig                    (1)  
noSuchName                (2)  
badValue                  (3)  
readOnly                  (4)  
getError                  (5)

error-index INTEGER,                    -- A veces ignorado  
variable-binding VarBindList        -- A veces ignorado

}

Trap-PDU ::= [4] IMPLICIT SEQUENCE {

enterprise OBJECT IDENTIFIER -- objeto que genera el trap.

agent-addr NetworkAddress,            --dirección del objeto

    --que genero el trap

generic-trap INTEGER {

          coldStar                    (0)  
          warmStart                  (1)  
          linkDown                   (2)  
          linkUp                     (3)  
          authenticationFailure      (4)  
          egpNeighbortLoss          (5)  
          enterpriseSpecific         (6)

specific-trap INTEGER,                -- especifica un codigo si  
    -- se presenta un trap  
    -- que no sea  
    -- "enterpriseSpecific"

time-stamp TimeTicks                  -- tiempo agotado entre la  
    -- última reinicialización  
    -- de la entidad de red y  
    -- la generación de un trap.

```
Variable-binding (VarBindList) -- Información de
                                --variables
-- campo de variables

varBind ::= SEQUENCE {
name ObjectName, value ObjectSyntax
}

VarBindList ::= SEQUENCE OF VarBind

END
  }
  }
}
```

### 6.11 Interacción del protocolo SNMPv1

Una interacción del protocolo SNMPv1 consiste en una operación de petición de algún tipo (*Get*), seguida por una operación de respuesta (*Response*). Hay cuatro posibles resultados de una operación:

- Una respuesta sin excepción o error.
- Una respuesta con una o más excepciones.
- Una respuesta con error.
- Sobrepasar el tiempo de espera (*timeout*).

Como se puede ver la forma de operar del protocolo SNMPv1 no es complicada y es relativamente fácil de entender.

Debido a que el mensaje SNMP se trasmite en claro, es decir, no contiene mecanismos de seguridad, fue necesario implantar dichos mecanismos con la finalidad de hacerlo más confiable, esto dio origen a nuevas versiones del protocolo SNMP de las cuales se hablará en los dos capítulos siguientes.

## 7.1 Introducción

Debido a que SNMPv1 transmite en claro, es decir, sólo se requiere el nombre de la comunidad para tener acceso a los objetos de la MIB, se comenzaron en 1991 trabajos de revisión para mejorar la seguridad en el protocolo SNMPv1, tratando también de resolver problemas del ámbito administrativo, como eficiencia en la transferencia de información, permitir la comunicación entre estaciones de administración de redes, nuevas operaciones, entre otras. Esto dio origen de manera inevitable a una nueva versión del protocolo SNMP, denominada SNMPv2, la cual fue varias veces revisada, y estas revisiones derivaron en varias versiones del protocolo SNMPv2 como:

- SNMPv2
- SNMPv2c
- SNMPv2u

Pero no fue hasta 1996 que la versión de SNMPv2c fue aceptada de una manera reservada, pero sin sus características de seguridad debido a la complejidad que estas características agregaban a la administración.

A pesar de los esfuerzos por mejorar SNMPv2, la discreción de su éxito, debido entre otras cosas a la incompatibilidad con la versión SNMPv1 dieron origen a una nueva versión llamada SNMPv3 la cual tocaremos en el capítulo 8.

## 7.2 SNMPv2 (RFC del 1901,..., 1908)

Como se especificó anteriormente existen tres versiones del protocolo SNMP, en este apartado se dará una breve descripción de la versión 2 de dicho protocolo o también conocido como SNMPv2.

Este protocolo de administración se definió en 1993, es una versión más avanzada del protocolo SNMPv1.

SNMPv2 aporta una serie de ventajas respecto a la primera versión entre las cuales pueden destacarse:

- Permite una mayor eficiencia en la transferencia de información.
- Admite mecanismos de seguridad como la autenticación y el cifrado.
- Permite la comunicación entre entidades administradoras de red.
- Permite una señalización extendida de errores.
- Permite el uso de varios servicios de transporte.
- Nuevas operaciones.

El sistema de administración basado en SNMPv2 soluciona muchos de los problemas de su antecesor SNMPv1, sin embargo, su mayor complejidad cortó su desarrollo, su esquema de seguridad fue rechazado, así en 1996 se publica una revisión, la cual se acepta sin el esquema de seguridad.

Los mensajes enviados por la estación de administración de red a los agentes SNMP están formados por identificadores de objetos MIB junto con instrucciones, a fin de cambiar u obtener un valor.

### 7.3 Operaciones de SNMPv2.

El protocolo SNMPv2 incluye los mensajes de la primera versión SNMPv1, y a éste se le han agregado otros tipos de mensajes como se verá a continuación:

- GetRequest: Petición de valores específicos de la MIB.
- GetNextRequest: Proporciona un medio para moverse por la MIB, es la petición de un objeto siguiente a uno dado de la MIB.
- GetResponse: Devuelve los valores solicitados por las operaciones anteriores.
- GetBulkRequest: Petición de múltiples valores.
- Response: Devuelve los valores solicitados por las operaciones anteriores en la configuración de administrador a administrador ó de agente a administrador.
- SetRequest: Permite asignar un valor a una variable.
- InformRequest: Transmite información no solicitada (Administrador a administrador).
- SNMPv2-Traps: Permite a los agentes informar de sucesos inusuales como en la versión anterior de SNMP.

## 7.4 Secuencia de mensajes

La figura 7.1 ilustra la relación que existe entre los diversos tipos de operaciones de SNMPv2 y los nodos administrables, es decir, el papel de administrador y el papel de agente ó de administrador a administrador.

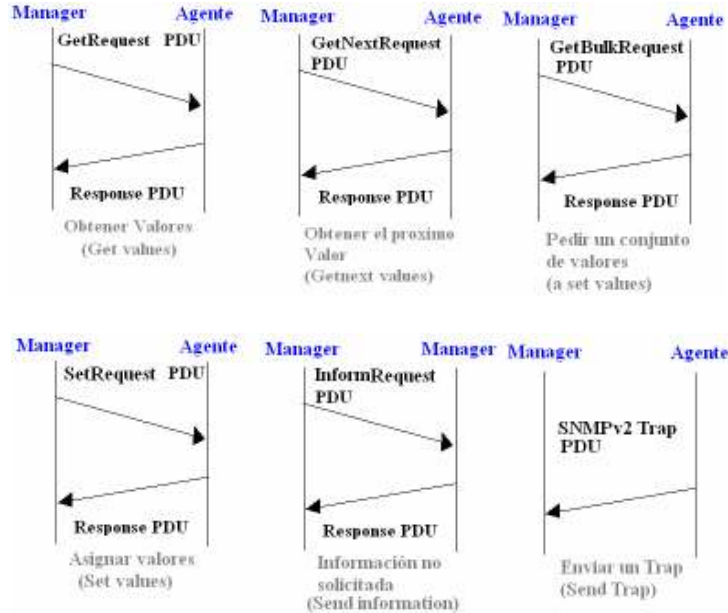


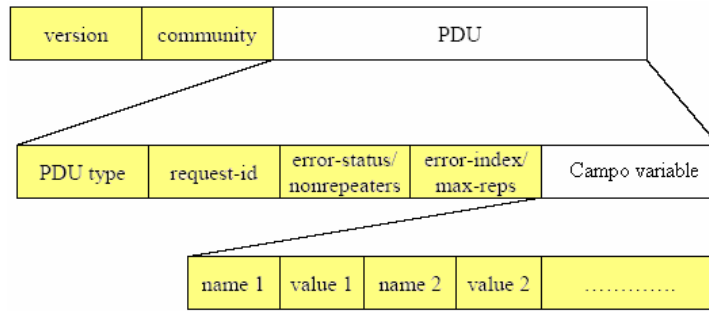
Figura 7.1 Secuencia de operaciones en SNMPv2

En la figura 7.1 se pueden observar las nuevas operaciones en SNMPv2 como lo son: *GetBulkRequest* e *InformRequest*; no obstante, también se puede observar la innovación de comunicación entre un administrador y otro administrador cualquiera.

En la misma figura se puede observar como el mensaje *GetResponse* de la primera versión de SNMP, fue sustituido por el mensaje *Response* en esta versión.

## 7.5 Formato de los mensajes SNMPv2

La figura 7.2 muestra las diferentes secciones que componen un mensaje del protocolo SNMPv2 de transmisión ó petición, es importante hacer notar que las líneas que unen un formato con otro, indican la expansión de una sección del mensaje SNMPv2.



**7.2 Formato del mensaje SNMPv2 de petición**

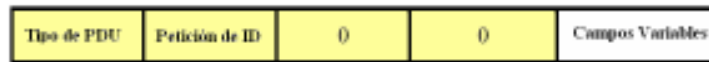
La figura 7.2 muestra un mensaje de transmisión de la entidad administradora de red, la cual está pidiendo la ejecución de alguna de las siguientes operaciones:

- GetRequest.
- GetNextRequest.
- GetBulkRequest
- SetRequest.
- InformRequest

El formato de cada una de las PDUs de las operaciones de SNMPv2 se muestra en las siguientes figuras:

La figura 7.3 muestra el formato de la PDU para las operaciones:

- GetRequest.
- GetNextRequest.
- SetRequest.
- SNMPv2 – Trap.
- InformRequest.



**Figura 7.3 Formato de PDU para peticiones**

La figura 7.4 muestra la PDU para la operación:

- GetBulkRequest.



**Figura 7.4 Formato de la PDU de GetBulkRequest.**

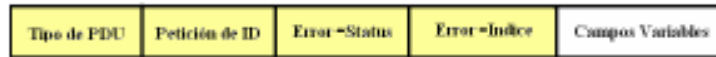
La descripción de los campos: “*No repetir*” y “*Máxima repetición*” se describe a continuación:

No repetir: Número de variables en la lista de “*Campos Variables*” (las primeras) en que se devuelve el siguiente elemento al indicado en orden lexicográfico.

Máxima repetición: Para el resto de variables en la lista de “*Campos Variables*”, este parámetro indica el número de variables sucesivas a las especificadas en la lista que son devueltas.

La figura 7.4 muestra la PDU de la operación:

- Response.



**Figura 7.4 Formato de la operación Response.**

Es importante destacar que con esta operación se responde a todo tipo de petición excepto a un SNMPv2-Trap.

La figura 7.5 muestra la PDU del Campo Variable



**Figura 7.5 Formato del Campo Variable.**

Sin embargo, el hecho de la incompatibilidad con la versión SNMP y la mayor complejidad añadida a las plataformas repercutieron de manera drástica, haciendo que esta versión no tuviera el éxito esperado y por ello no se tocará más en este trabajo.

El desacuerdo en las negociaciones sobre las recomendaciones acerca de seguridad propuesta en SNMPv2 propició la elaboración de SNMPv3.



## 8.1 Introducción

El SNMP es especialmente estable ya que sus definiciones se mantienen fijas aún cuando nuevos elementos de datos se añadan al MIB. La estructura SNMP ha evolucionado de SNMPv1, a través de SNMPv2, a SNMPv3; haciendo sus componentes arquitectónicos más ricos y claramente definidos; pero el principio de la arquitectura ha permanecido consistente. Como resultado, SNMPv3 puede pensarse como SNMPv2 con adicional seguridad y capacidad de administración.

La figura 8.1 nos ayuda a comprender mejor esta idea.



SNMPv3 = SNMPv2 + seguridad + administración

**Figura 8.1 El modelo SNMPv3**

La figura muestra la adición de elementos administrativos y seguridad a la versión de SNMPv2 dando como resultado, el protocolo SNMPv3.

Esto da una idea general de la innovación a la que fue sujeta la versión 2 de SNMP, para obtener una nueva versión, modular y más flexible al rediseño sobre todo de la parte que se refiere a seguridad.

## 8.2 El protocolo SNMPv3

Los documentos que se emitieron para las especificaciones de SNMPv3 son los siguientes:

- RFC 2271: Describe toda la arquitectura de la administración de SNMPv3, Enero 1998.
- RFC 2272: Describe el procesamiento de mensajes y despacho para SNMPv3, Enero 1998.
- RFC 2273: Describe una variedad de aplicaciones para SNMPv3, Enero 1998.

- RFC 2274: Describe un modelo de seguridad basado en el usuario, Enero 1998.
- RFC 2275: Describe un modelo de control de acceso basado en vistas (VACM) para SNMPv3, Enero 1998.

La tercera versión del protocolo SNMP se deriva y está sustentada sobre SNMPv1 y SNMPv2. Con el tiempo, la estructura ha evolucionado de SNMPv1, a través de SNMPv2, hasta SNMPv3, las definiciones de cada uno de los componentes de la arquitectura se han hecho más ricas, pero la arquitectura fundamental ha permanecido consistente.

Algunas de las amenazas clásicas, tales como la modificación de información, el descubrimiento, modificación del flujo de mensaje, etc.; son aplicables a problemas de administración de redes y por consiguiente aplicables a cualquier modelo de seguridad SNMP. Por lo que se describe al modelo de seguridad *User-based*, usando el concepto tradicional de un usuario con la información de seguridad asociada.

### 8.3 Arquitectura de SNMPv3

De igual forma que en las versiones anteriores de SNMP, los nodos administrados pueden ser PCs, routers, puentes, impresoras u otros dispositivos capaces de comunicar información al mundo exterior.

Las especificaciones de SNMPv3 se basan en una arquitectura modular. Esta estructura no es más que un protocolo para movimiento de información, y está formado por:

- Un lenguaje de definición de datos.
- Una base de administración de información.
- Definición de protocolo.
- Seguridad y administración.

La arquitectura de la estructura administrativa SNMPv1 y SNMPv2 poseen conceptos familiares con la estructura administrativa de SNMPv3, sin embargo en algunos casos la terminología puede ser algo diferente.

Esta arquitectura consiste en la distribución, interacción y colección de entidades SNMP. Cada entidad implanta una porción de las capacidades de SNMP y puede

actuar en un nodo con un agente, en un nodo con un administrador, o una combinación de ambos.

Cada entidad SNMP consiste en una colección de módulos que interactúan con cada servicio proporcionado.

Esta interacción podría ser modelada como un conjunto de primitivas y parámetros. En esta sección nosotros veremos primero la estructura interna de una entidad SNMP y después consideraremos la definición de los servicios definidos para los módulos de una entidad SNMP.

### **8.4 Entidad SNMP**

La figura 8.2 Muestra el diagrama a bloques de manera general de una entidad SNMP. Cada entidad incluye un motor. Un motor SNMP implementa funciones para mandar y recibir mensajes, autenticando, encriptando y desencriptando mensajes y controlando el acceso a los objetos administrados. Estas funciones son proporcionadas como servicio de una o más aplicaciones que están configuradas con el motor SNMP para formar una entidad SNMP.

La figura 8.2 esta dividida en dos secciones:

La sección inferior muestra el motor SNMP y la sección superior muestra el apartado de las aplicaciones. Ambas secciones están definidas como una colección de módulos.

Esta arquitectura proporciona diversas ventajas, una de ellas, es que el rol de una entidad SNMP esta determinada por lo módulos que están implantados dentro de dicha entidad. Por ejemplo, un conjunto de módulos son requeridos para un agente SNMP, y otro conjunto de módulos son requeridos para un administrador.

De manera conjunta la estructura modular de las especificaciones permite a ésta, definir diferentes versiones de cada módulo. Esto hace posible:

- Definir alternativas ó mejorar las capacidades de los aspectos de SNMP sin necesidad de realizar una nueva versión del protocolo.

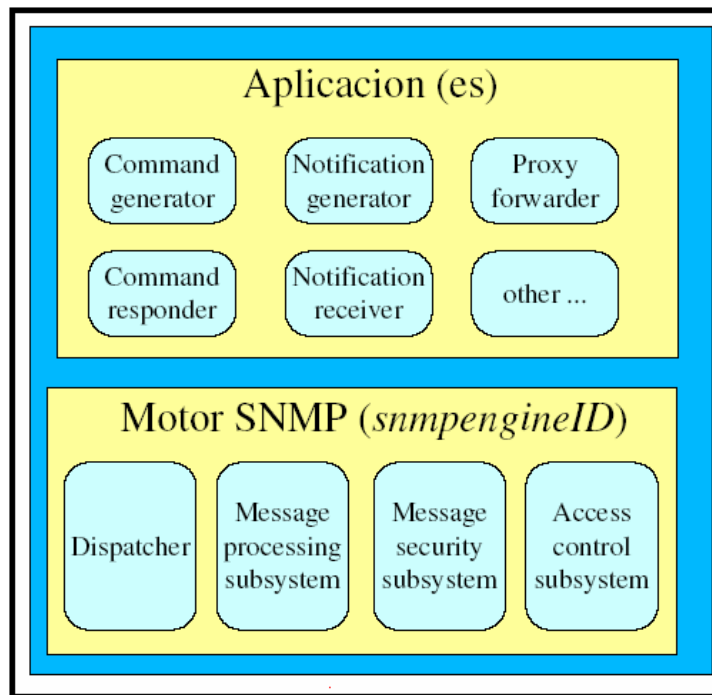


Figura 8.2 Entidad SNMP

En seguida pasaremos a dar una breve descripción de los elementos del nivel de aplicaciones en SNMPv3:

**Command Generator:**

- Inicializa los comandos *GetRequest*, *GetNextRequest*, *GetBulkRequest* ó *setRequest* y procesa las respuestas a las peticiones previamente generadas.

**Command Responder:**

- Recibe los comandos *GetRequest*, *GetNextRequest*, *GetBulkRequest* ó *setRequest*, con destino al sistema local (*engineID*) y realiza la acción solicitada, usando el control de acceso y generando un mensaje de respuesta.

**Notificacion Originator:**

- Monitoriza el sistema y genera *Trap* y/o *InformRequest*, según eventos o condiciones.

**Notification Receiver:**

- Escucha notificaciones y genera confirmaciones.

**Proxy Forwarder:**

- Reenvía mensajes SNMP.
- *snmpEngineID*: Es un identificador único para un motor SNMP, así como de la entidad SNMP correspondiente, Esta definida por una cadena de octetos.

La figura 8.3 muestra la interacción del motor SNMPv3 con la parte de la red (Parte inferior UDP), así como la relación con la sección de aplicaciones (PDUs SNMP).

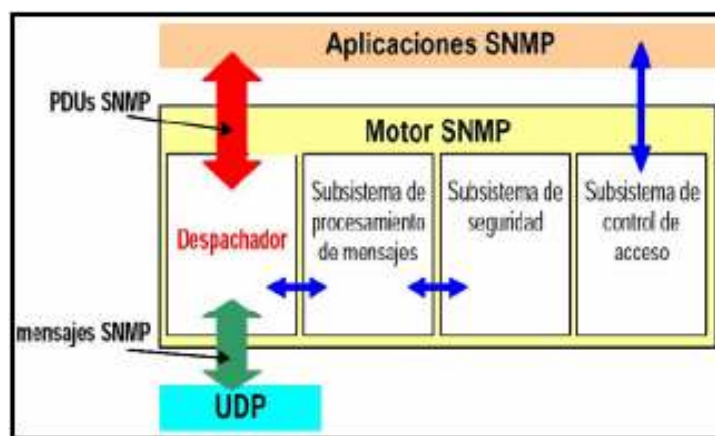


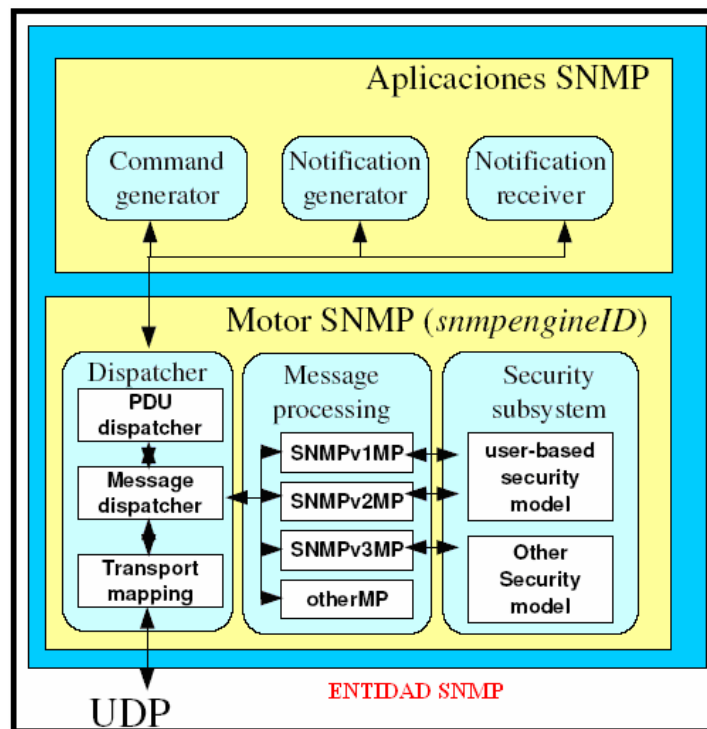
Figura 8.3 Interacción del motor SNMP

En esta figura se puede observar la interacción que el despachador (*Dispatcher*), que tiene tanto con los bloques superiores de aplicación, así como los bloques de procesamiento, seguridad y control de acceso a su lado derecho, sin olvidar la parte inferior que hace referencia a la capa de transporte.

Las funciones desempeñadas del motor SNMP (*SNMP engine*) serán descritas en las secciones siguientes.

## 8.5 Administrador tradicional SNMPv3

La figura 8.4 muestra a un administrador tradicional para SNMPv3.



La figura 8.4 Administrador tradicional SNMPv3

En seguida se dará una breve descripción de cada uno de los módulos del administrador tradicional SNMPv3.

Cuando se incluye la terminología en el protocolo SNMPv3 de “*TRADICIONAL*”, esto indica que se incluyen tres categorías de aplicaciones:

### 8.5.1 Categorías de aplicaciones (*Applications*)

#### 1. Generador de comandos (*Command generator*)

Monitorea y manipula datos de administración en agentes remotos, haciendo uso de las PDUs de SNMPv1 y SNMPv2, incluye las operaciones:

- *GetRequest*

- *GetNextRequest*
- *GetBulkRequest*
- *SetRequest*

Inicia los comandos anteriores y procesa las respuestas a las peticiones previamente generadas.

## **2. Originador de notificaciones (*Notification Originator*)**

Inicialización asíncrona de mensajes; en el caso de un mensaje tradicional como:

- *InformRequest*.

Es usado por la aplicación.

## **3. Receptor de notificaciones (*Notification Receiver*)**

Procesa el mensaje entrante asíncrono; este incluye “*InformRequest*”, SNMPv2-Trap y SNMPv1-Trap.

En el caso de “*InformRequest*” entrante, este responde con un “*Response*”.

## **8.5.2 Motor SNMP (SNMP engine)**

### **1. Despachador (*Dispatcher*)**

Permite el soporte de múltiples versiones del protocolo SNMP dentro del motor SNMP.

Es responsable de:

- Aceptar PDUs de las aplicaciones para transmitirlos a la red, así como entregar PDUs entrantes a las aplicaciones.
- Pasa las PDUs salientes al “*Message Processing Subsystem*” para prepararlas como mensajes. Del mismo modo pasa el mensaje entrante para extraer la PDU de dicho mensaje.
- Envía y recibe mensajes en la red.

### **2. Subsistema de procesamiento de mensajes (*Message Processing Subsystem*.)**

Es responsable de la preparación de los mensajes para ser enviados, y para extraer los datos de los mensajes recibidos.

### **3. Subsistema de seguridad (*Security Subsystem*)**

Proporciona los servicios de seguridad, tales como: La autenticación y privacidad de los mensajes. Este subsistema potencializa constantemente los modelos de seguridad.

### **4. Subsistema de control de acceso (*Access Control Subsystem*)**

Proporciona un conjunto de servicios de autenticación que en una aplicación pueden ser usados para revisar los derechos de acceso.

El control de acceso puede ser invocado para recuperar ó modificar operaciones de peticiones y para la notificación de generación de operaciones.

## **8.6 Agente tradicional SNMPv3**

El motor SNMP para un agente tradicional tiene todos los componentes encontrados en un administrador tradicional SNMP, más un mecanismo denominado Subsistema de Control de Acceso "*Access Control Subsystem*", el cual es propio del agente, y se encuentra después del bloque de subsistema seguridad.

Este subsistema proporciona servicios de autorización para controlar el acceso a las MIBs para la lectura y escritura de objetos administrados.

Una implantación del subsistema de seguridad puede soportar uno o más modelos de control de acceso. No obstante el único modelo de seguridad definido es el "*View – Based Access Control Model*" (VACM) para SNMPv3. La revisión del modelo de control de acceso basado en vistas, sale de los objetivos de este trabajo, sí el lector desea saber más a cerca de éste, se le recomienda consultar la obra "*SNMP, SNMPv2, SNMPv3 and RMON 1 and 2*" de William Stalling Third Edition de la editorial Addison Wesley.

Es importante notar que las funciones relacionadas con seguridad están organizadas en dos subsistemas separados:

- *Security subsystem.*
- *Access Control Subsystem.*

Este es un excelente ejemplo de un buen diseño modular, porque los dos subsistemas ejecutan distintas funciones, es por eso, que esto permite la



estandarización de estas dos áreas de manera independiente como se observa en la figura 8.5.

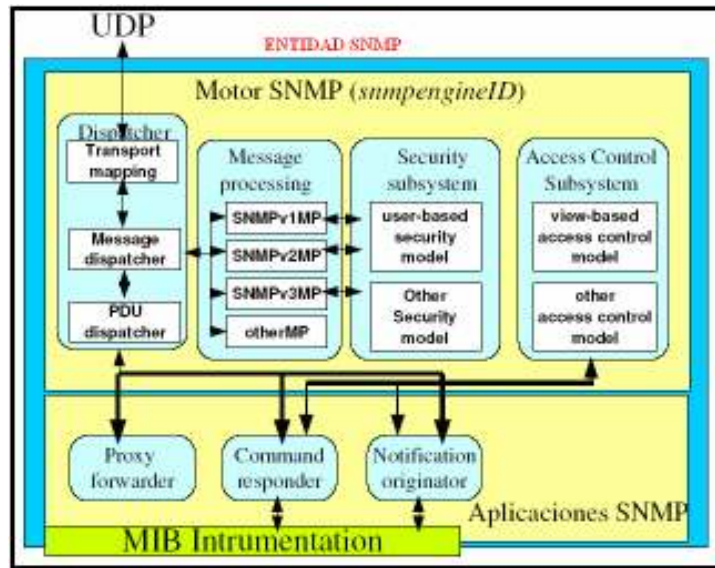


Figura 8.5 Agente tradicional SNMPv3

El subsistema de seguridad está relacionado con la privacidad y la autenticación y operaciones sobre los mensajes SNMP.

El subsistema de control de acceso está relacionado con el acceso autorizado a información de administración y operaciones sobre las PDUs de SNMP.

## 8.7 Comunicación entre módulos

Los servicios entre módulos dentro de una entidad SNMP se definen a través de:

- Primitivas: Especifican la función que va a ser ejecutada.
- Parámetros: Son usados para pasar datos e información de control.

## 8.8 Despachador de primitivas

Primitivas entre las aplicaciones SNMP y el Despachador:

- *sendPdu*: Usada por el generador de comandos (*command generator*) para enviar una *petición* PDU o una *notificación* PDU a otra entidad SNMP.

- *processResponsePdu*: Usada por el *dispatcher* para pasar una PDU *Response* SNMP entrante a una aplicación.
- *processPdu*: Usada por el *dispatcher* para pasar una PDU *request* o *notificación* SNMP a una aplicación.
- *returnResponsePdu*: usada por *command responder* para devolver una SNMP response PDU ante una PDU de *request* o *notificación*.
- *registerContextEngineID*: registra un determinado *engineID* para tratar determinados tipos de PDUs.
- *unregisterContextEngineID*: borra un *engineID* para determinados tipos de PDU.

## 8.9 Primitivas del subsistema del procesamiento de mensajes

Definen la interfaz entre el despachador y el subsistema de procesamiento de mensajes.

- *prepareOutgoingMessage*: Esta primitiva es usada por el despachador para solicitar la preparación de un mensaje que contiene una PDU *request* o *notificación*, de esto se devuelve error o éxito. Si es exitosa, el despachador recibe un mensaje que contiene dicha PDU.
- *prepareDataElements*: usada para extraer una PDU de un mensaje entrante. El despachador le da el mensaje como parámetro de entrada al subsistema de procesamiento de mensajes y recibe la PDU junto con la indicación del tipo de PDU, si es exitosa.
- *prepareResponseMessage*: Esta primitiva es usada por el despachador para pedir al subsistema de procesamiento de mensajes, la preparación de un mensaje que contenga una PDU saliente de tipo response en respuesta a una petición o notificación previa.

## 8.10 Primitivas del subsistema de seguridad

Primitivas de la interfase entre el subsistema de procesamiento de mensaje y el subsistema de Seguridad.

- *generateRequestMessage*: Esta primitiva es usada por el subsistema de procesamiento de mensajes para generar un mensaje que contiene una PDU saliente de *request* o *notificación*. Así el subsistema de seguridad puede devolver éxito o error. Si es exitoso, el subsistema de procesamiento de

mensajes, recibe una cabecera del mensaje y una PDU contextualizada como parámetros de entrada y recibe un mensaje preparado con autenticación y una posible encriptación, junto con parámetros asociados de seguridad.

- *processIncomingMessage*: usada para proveer procesamiento de seguridad para un mensaje entrante. Indica el éxito o fracaso del procesamiento de seguridad. De esta forma el subsistema de procesamiento de mensajes nuevamente recibe el mensaje y devuelve la PDU junto con su tipo y la indicación del resultado.
- *generateResponseMessage*: usada para generar un mensaje que contiene una PDU de tipo response en respuesta a una petición. Devuelve éxito o error.

En la figura 8.6 muestra el proceso de un mensaje cuando el generador de comandos u originador de notificaciones pasan una PDU al despachador.

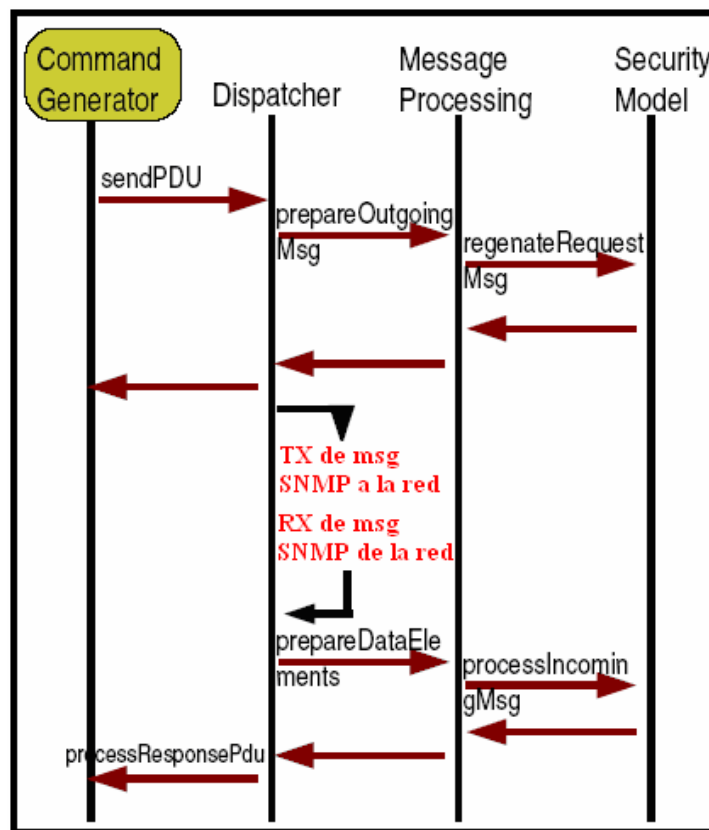


Figura 8.6 Generador de comandos y Originador de Notificaciones

En la figura 8.7 se muestra el proceso de un mensaje cuando el respondedor de comandos pasa una PDU al despachador.

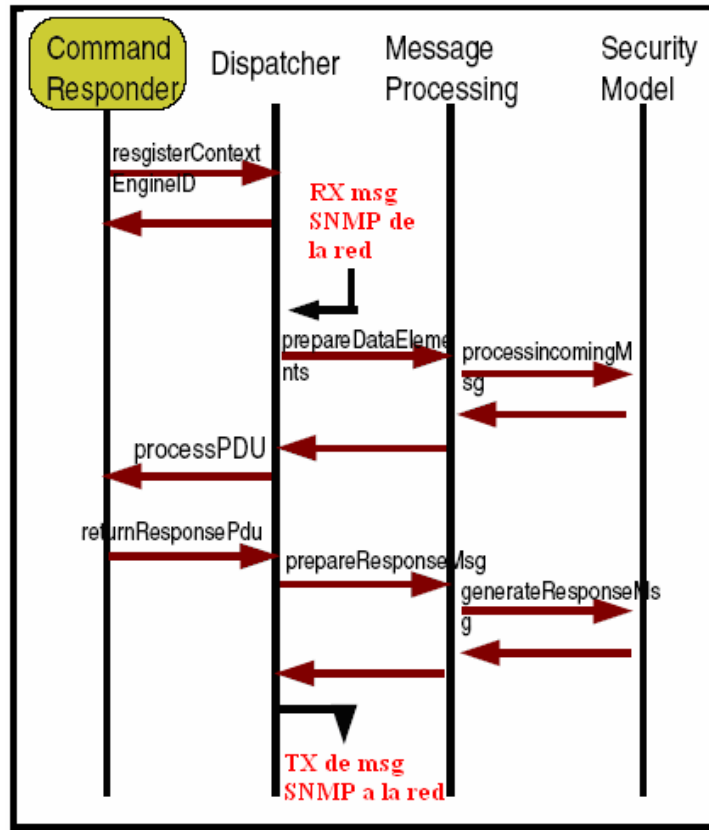


Figura 8.7 Respondedor de comandos

La figura 8.6 y 8.7 nos muestran la forma de operar de las PDUs dentro del motor SNMP.

La diferencia fundamental de la MIB de SNMPv3 es un grupo de objetos denominado *usmUser Grup*.

Cada entidad SNMP mantiene una MIB, con el grupo “*usmUser*”, este grupo consiste en una estructura escalar, como lo muestra la figura 8.8.

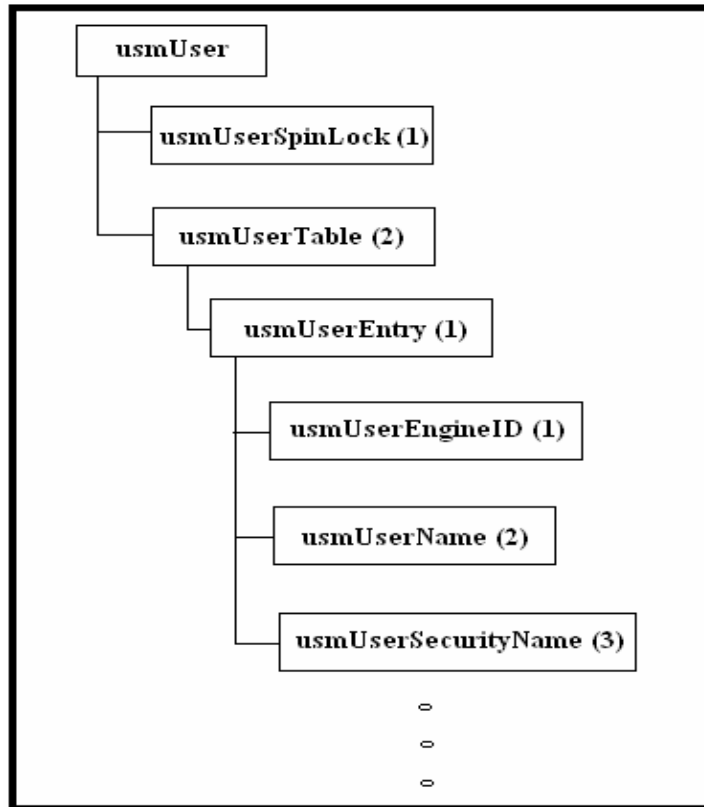


Figura 8.8 Parte del grupo usmUser

Para llegar al campo que nos interesa “*usmUserSecurityName*”, primero tenemos que pasar por “*usmUserSpinLock*”, luego por “*usmUserTable*”, para llegar a “*usmUserEntry*”, donde existen los parámetros que nos interesan “*usmUserEngineID*”, “*usmUserName*” y “*usmUserSecurityName*”.

A continuación se dará una breve descripción de los parámetros que son de interés para este trabajo; no obstante, si al lector le interesa conocer más a detalle los parámetros de este grupo se le recomienda ir a la obra ““*SNMP, SNMPv2, SNMPv3 and RMON 1 and 2*” de William Stallings Third Edition de la editorial Addison Wesley”.

- *usmUserEngineID*: Se refiere a la autorización de un motor SNMP en determinado nodo administrado con SNMPv3. En donde el agente identifica al *snmpEngineID*. Este valor puede también ser de un motor SNMP remoto con el cual el usuario puede comunicarse.

- *usmUserName*: Es una cadena que representa el nombre de un usuario dentro de los objetos USM, este valor funciona como un identificador o nombre de seguridad (*SecurityName*).
- *usmSecurityName*: Es una cadena que representa el nombre de usuario que es independiente al modelo de seguridad, este valor funciona como el identificador principal o nombre de seguridad (*SecurityName*).

Cuando se habla de seguridad en SNMPv3, existen dos parámetros que son fundamentales: *User security name* y *Security level*.

- *Security level*: Este parámetro hace referencia a la petición de servicios de seguridad los cuales son:
  - Ninguno.
  - Autenticación
  - Autenticación privada.

La autenticación permite el uso de una o dos alternativas en cuanto a protocolos de autenticación se refieren como el HMAC – MD5 – 96 y el HMAC – SHA – 96, los cuales no serán tratados en este trabajo.

## Capítulo 9

### Introducción Al Cableado Estructurado

---

#### 9.1 Introducción

El Instituto Americano Nacional de Estándares, la Asociación de Industrias de Telecomunicaciones y la Asociación de Industrias Electrónicas (ANSI/TIA/EIA) publican conjuntamente estándares para la manufactura, instalación y rendimiento de equipo y sistemas de telecomunicaciones y electrónico. Cinco de estos estándares de ANSI/TIA/EIA definen cableado de telecomunicaciones en edificios. Cada estándar cubre una parte específica del cableado del edificio. Los estándares establecen el cable, hardware, equipo, diseño y prácticas de instalación requeridas.

El cableado estructurado está diseñado para usarse en cualquier cosa, en cualquier lugar, y en cualquier momento. Elimina la necesidad de seguir las reglas de un proveedor en particular, concernientes a tipos de cable, conectores, distancias, o topologías. Permite instalar una sola vez el cableado, y después adaptarlo a cualquier aplicación, desde telefonía, hasta redes locales *Ethernet*.

Mediante la adopción bilateral de normas por parte de fabricantes de cable básico y de equipo electrónico, se hace posible la implantación de un cableado flexible. Si además el usuario final sigue esas mismas normas, entonces cualquier aplicación, cable, conector, o dispositivo electrónico construido bajo estas normas, trabajará en el mismo sistema.

#### 9.2 Cableado estructurado

El tendido de cable para una red de área local tiene cierta complejidad cuando se trata de cubrir áreas extensas tales como un edificio de varias plantas. En este sentido hay que tener en cuenta las limitaciones de diseño que impone la tecnología de red de área local que se desea implantar:

- La longitud máxima de cada segmento de red.
- La interferencia electromagnética.
- Etc.

Entendiendo estas limitaciones, la idea del cableado estructurado es simple:

- Tender cables en cada planta del edificio.
- Interconectar los cables de cada planta.

### **9.3 Cableado horizontal ó de planta**

En cada planta se instalan los JACKS RJ – 45 hembras (terminales de los cables o puntos) que sean necesarios en cada departamento de un piso o una planta de una determinada organización. De estos JACKS RJ – 45 hembras parten los cables que se tienden por el falso suelo o por el falso techo de la planta o piso, si existe.

Todos los cables se concentran en el denominado armario de distribución de planta.

**9.3.1 Armario de distribución de planta:** Se trata de un bastidor donde se realizan las conexiones eléctricas y de red de unos cables con otros.

En algunos casos, según el diseño que requiera la red, el armario puede tener elementos de tipo activo o pasivo de comunicaciones, es decir, concentradores, conmutadores, encaminadores, etc. En cualquier caso, este armario concentra todos los cables procedentes de una misma planta.

### **9.4 Elementos básicos del cableado horizontal**

#### **9.4.1 Cable Horizontal y Hardware de Conexión.**

Proporcionan los medios para transportar señales de telecomunicaciones entre el área de trabajo y el cuarto de telecomunicaciones. Estos componentes son los "contenidos" de las rutas y espacios horizontales.

#### **9.4.2. Rutas y Espacios horizontales:**

Las rutas y espacios horizontales son utilizados para distribuir y soportar cable horizontal y conectar hardware entre la salida del área de trabajo y el cuarto de telecomunicaciones. Estas rutas y espacios son los contenedores del cableado horizontal.



#### 9.4.2.1 El cableado horizontal incluye:

- Las salidas como: cajas, placas, conectores, etc. de telecomunicaciones en el área de trabajo.
- Cables y conectores de transición instalados entre las salidas del área de trabajo y el cuarto de telecomunicaciones.
- Paneles de empalme (*patch panel*) y cables de empalme utilizados para configurar las conexiones de cableado horizontal en el cuarto de telecomunicaciones.

#### 9.4.2.2 El cableado horizontal típico:

- Contiene más cable que el cableado del *backbone*.
- Es menos accesible que el cableado del *backbone*.

#### 9.4.2.3 Topología:

- La topología del cableado siempre será de tipo estrella.
- Un cable para cada salida en los puestos de trabajo.
- Todos los cables de la corrida horizontal deben estar terminados en JACKS RJ - 45 y paneles.

#### 9.4.2.4 Distancia del cable:

La distancia horizontal máxima es de 90 metros independiente del cable utilizado. Esta es la distancia máxima desde el área de trabajo de telecomunicaciones hasta el lugar donde se encuentra el RJ – 45 hembra. Al establecer la distancia máxima se hace la previsión de 10 metros adicionales para la distancia de cables de empalme, donde se recomienda que dichos cables no excedan los 3 metros.

La figura 9.1 ilustra la estructura del cableado horizontal que va desde la estación de trabajo hasta el armario donde se encuentran los dispositivos activos.



Figura 9.1 Estructura básica del cableado horizontal

Los elementos constitutivos de la figura 9.1 se describen a continuación:

- 1.- Tarjeta de red.
- 2.- Cable UPT con conectores RJ – 45.
- 3.- Tapa flaceplates
- 4.- Jack modular hembra.
- 5.- Cable UTP dentro de canaleta.
- 6.- Switch.
- 7.- Backbone (Cableado vertical)

### **9.5 Cableado vertical ó backbone**

Es la interconexión de todos los armarios de distribución de planta mediante otro conjunto de cables que deben atravesar verticalmente el edificio de planta a planta. Esto se hace a través de las canalizaciones existentes en el edificio. Si esto no es posible, es necesario habilitar nuevas canalizaciones, aprovechar aberturas existentes como: huecos de ascensor o escaleras.

Estos cables acaban en una sala donde, de hecho, se concentran todos los cables del edificio. Aquí se sitúa la electrónica de la red y otras infraestructuras de telecomunicaciones, tales como: puertas de enlace, *Firewall*, etc.

Es importante destacar que el cableado vertical agrega el ancho de banda de todas las plantas. Por tanto, suele utilizarse otra tecnología con mayor capacidad. Por ejemplo, *Gigabit - Ethernet*.

#### **9.5.1 Funciones del backbone**

- La función del cableado vertical es la interconexión de los diferentes cuartos de comunicaciones.
- El cableado vertical es típicamente menos costoso de instalar y debe poder ser modificado con más flexibilidad.

#### **9.5.2 Topología**

- La topología del cableado vertical debe ser típicamente una estrella.
- En circunstancias donde los equipos y sistemas solicitados exijan un anillo, este debe ser lógico y no físico.

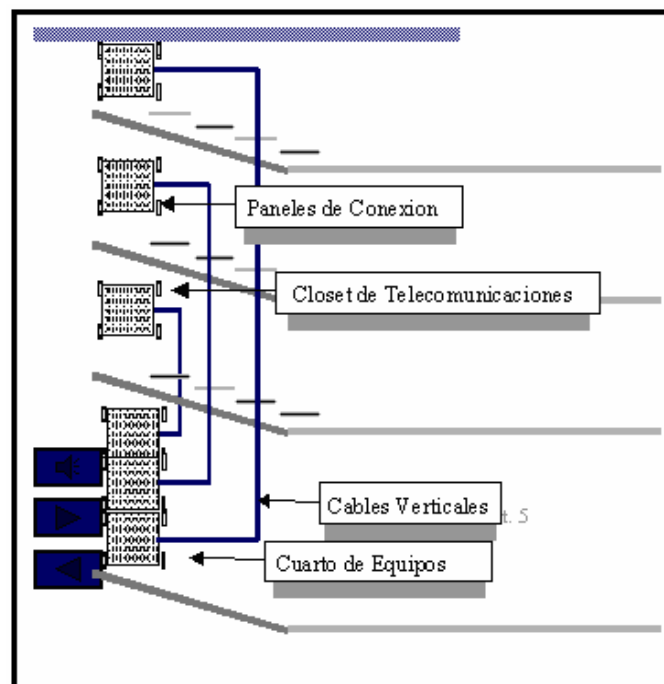
### 9.5.3 Cables Reconocidos:

- Cable UTP.
- Cable STP.
- Fibra Óptica.
- Combinaciones.

### 9.5.4 Distancias

- Dentro del Edificio
  - Cobre 90 mts
  - Fibra Óptica 500 m.
- Entre Edificios
  - Cobre 800 m.
  - Fibra Óptica Multimodo 2Km.
  - Fibra Óptica Monomodo 3Km.

La figura 9.2 ilustra el cableado estructural vertical, el cual se encuentra conectado a cada panel de conexión de cada planta ó piso para llevar los servicios de red de una organización determinada.



9.2 Estructura básica del cableado vertical

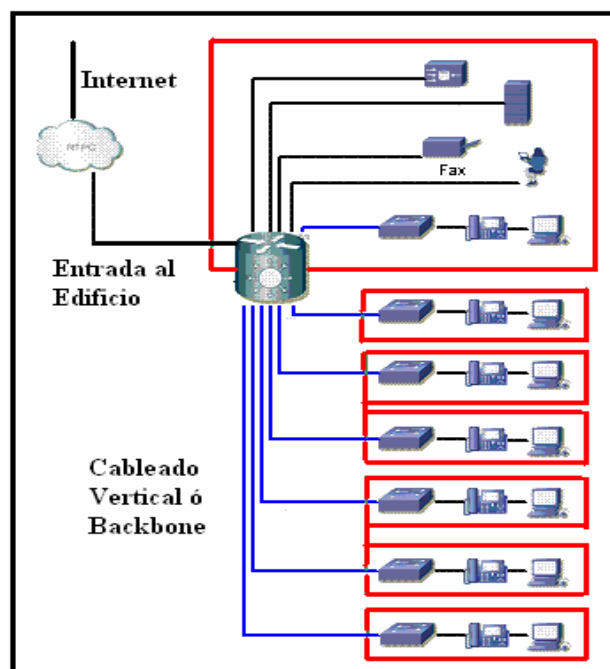
El panel de conexión de la figura 9.2 hace referencia a los conectores contenidos en los armarios, mientras que el closet de telecomunicaciones hace referencia a los armarios propios de cada planta ó piso.

El cableado vertical es conectado a cada armario ó closet de cada piso para llevar todas y cada una de las telecomunicaciones desde el **Cuarto de Equipos** ó también llamado: **Cuarto de telecomunicaciones**.

## 9.6 Aterrizaje del cableado estructurado

Para evitar descargas por acumulación de estática se recomienda hacer lo siguiente:

- Todos los componentes metálicos tanto de la estructura, como: tuberías, canaletas, etc. Del mismo modo el blindaje del cableado, los paneles y equipo, deben ser debidamente llevados a tierra.
- Todas las salidas eléctricas para computadoras deben ser polarizadas y llevadas a una tierra común.



9.3 Cableado estructurado común

La figura 9.3 ilustra un cableado estructurado de una organización, en donde se observa el cableado horizontal delimitado con pequeños rectángulos, mientras que el cableado vertical ó *backbone* se encuentra representado con las líneas que entran a dichos rectángulos.

El acceso a redes o de redes externas se hace a través del equipo necesario representado por un cilindro en la figura 9.3, el cual se encuentra como ya se mencionó en el cuarto de telecomunicaciones.

### 9.7 Subsistemas de la norma ANSI/TIA/EIA-568

La norma ANSI/TIA/EIA-568 especifica los requisitos mínimos para cableado de telecomunicaciones dentro de edificios, incluyendo salidas y conectores, así como entre edificios de conjuntos arquitectónicos.

De acuerdo a la norma ANSI/TIA/EIA-568, un sistema de cableado estructurado consiste de 6 subsistemas funcionales:

1. **Instalación de entrada:** Es el punto donde la instalación exterior y dispositivos asociados entran al edificio. Este punto puede ser utilizado por servicios de redes públicas, redes privadas del cliente, o ambas, y es en donde están ubicados los dispositivos de protección para sobrecargas de voltaje. Debe ubicarse cerca del los cableados verticales.

Si existen enlaces privados entre edificios, los extremos de dichos enlaces deben terminar en este punto.

2. **El cuarto, local, o sala de máquinas o equipos:** es un espacio centralizado para el equipo de telecomunicaciones como: equipos de cómputo, *routers*, conmutadores, concentradores, etc. que da servicio a los usuarios en el edificio.

En este cuarto sólo se admiten equipos directamente relacionados con los sistemas de telecomunicaciones

En su diseño se debe prever lugar suficiente para los equipos actuales y para los futuros crecimientos.

3. **El eje de cableado central:** tiene como misión proporciona interconexión entre los gabinetes de telecomunicaciones, locales de equipo, e instalaciones de entrada. Consiste de cables centrales, interconexiones principales e intermedias, terminaciones mecánicas, y puentes de interconexión. Los cables centrales conectan gabinetes dentro de un edificio o entre edificios.

4. **Gabinete de telecomunicaciones:** Es el espacio que actúa como punto de transición entre el cableado vertical (*backbone*) y las canalizaciones horizontales.

5. **El cableado horizontal:** Consiste en el medio físico usado para conectar cada toma o salida a un gabinete. Se pueden usar varios tipos de cable para la distribución horizontal. Cada tipo tiene sus propias limitaciones de desempeño, tamaño, costo, y facilidad de uso.

6. **El área de trabajo,** sus componentes llevan las telecomunicaciones desde la unión de la toma o salida y su conector donde termina el sistema de cableado horizontal, al equipo o estación de trabajo del usuario. Todos los adaptadores, filtros, o acopladores usados para adaptar equipo electrónico diverso al sistema de cableado estructurado, deben ser ajenos a la toma o salida de telecomunicaciones, y están fuera del alcance de la norma 568-A.

Una vez vistos los elementos constitutivos del cableado estructurado, los cuales nos permitirán llevar a cabo un diseño óptimo de la red, en su parte física; También es necesario conocer los mecanismos que nos permitan llegar a la realización de la red lógica a través del direccionamiento IP, lo cual es materia del siguiente capítulo.

## 10.1 Introducción

Las direcciones IP son el mecanismo a través del cual los equipos pueden identificarse en una red en específico, no obstante para llevar a cabo la interconexión de diversas redes, son necesarios equipos de interconexión de red.

Las direcciones IP se pueden clasificar por clases, las cuales nos permiten saber el número de redes y de equipos que pueden estar en cada clase.

Una red se puede dividir de tal forma que genera subredes, las cuales son más fáciles de administrar.

Las direcciones IP pueden ser de tipo público lo que indica que los equipos que posean una dirección de este tipo son visibles en toda la Internet.

Las direcciones IP pueden ser de tipo privado lo cual indica que los equipos que posean una de estas direcciones sólo se pueden ver por los equipos que pertenezcan a su misma red

## 10.2 Direccionamiento IP

La dirección IP es el identificador de cada equipo dentro de una red, la cual debe ser distinta a todas las demás direcciones que estén vigentes en ese momento en el conjunto de redes visibles por el equipo. En el caso de Internet, no puede haber dos ordenadores con 2 direcciones IP públicas iguales. Pero sí podríamos tener dos ordenadores con la misma dirección IP siempre y cuando pertenezcan a redes independientes entre sí, es decir, sin ningún camino posible que las comunique.

## 10.3 Clasificación de las direcciones IP

- **Direcciones IP públicas:** Son visibles en todo Internet. Es por ello que un equipo con una dirección IP pública es accesible desde cualquier otro equipo conectado a Internet.
- **Direcciones IP privadas:** Son visibles únicamente por otros equipos de su propia red o de otras redes privadas interconectadas por medio de equipos de interconexión como: *routers*. Los ordenadores con direcciones IP

privadas pueden salir a Internet por medio de un *router* ó *proxy* que tenga una IP pública.

**A su vez, las direcciones IP pueden ser:**

- **Direcciones IP estáticas (fijas).** Un equipo que se conecte a la red con dirección IP estática siempre lo hará con una misma dirección IP. Las direcciones IP públicas estáticas son las que utilizan los servidores de Internet con objeto de que estén siempre localizables por los usuarios de Internet.
- **Direcciones IP dinámicas.** Un equipo que se conecte a la red mediante una dirección IP dinámica, cada vez lo hará con una dirección IP distinta. Las direcciones IP públicas dinámicas son las que se utilizan en las conexiones a Internet mediante un módem.

## 10.4 Estructura de las direcciones IP

Las direcciones IP están formadas por 4 bytes (32 bits). Se suelen representar de la forma A.B.C.D. Por ejemplo la dirección IP 129.42.18.99.

Las direcciones IP también se pueden representar en binario y van del:

00000000.00000000.00000000.00000000

al

11111111.11111111.11111111.11111111.

Esto en decimal es:

0.0.0.0 al 255.255.255.255

Las direcciones IP se encuentran divididas en cuatro clases, las cuales se muestran en la siguiente sección.



### 10.5 Clases de direcciones IP:

La **clase A** está estructurada de forma que el primer *byte* A, se refiere al identificador de la red, mientras que los tres bytes restantes identifican al equipo en la red. Por ejemplo. La dirección IP 35.23.45.9, el *byte* que representa en decimal el número 35 se refiere a la red 35, mientras que los bytes .23.45.9 identifican al equipo en la red.

De esto, se observa que el número de redes que se pueden direccionar en la clase A son 128, es decir, de la '0' a la '127' con un total de 16, 777,214 de equipos por red, como lo muestra la tabla 10.2.

De igual forma la clase 'B' ocupa los primeros dos bytes A.B para la red y los otros dos restantes C.D para identificar al equipo en la red.

De esta forma resulta obvio que la clase 'C' destine los primeros tres bytes A.B.C. Para la red y el último byte D. Para identificar al equipo en la red como lo muestra la tabla 10.1.

La **clase D** está formada por direcciones que identifican no a un equipo, sino a un grupo de ellos.

Las direcciones de **clase E** no se pueden utilizar, se consideran reservadas como lo muestra la figura 10.1.

	0	1	2	3	4	8	16	24	31	
<b>Clase A</b>	0	red				Host				
<b>Clase B</b>	1	0	red			host				
<b>Clase C</b>	1	1	0	red			host			
<b>Clase D</b>	1	1	1	0	grupo de multicast (multidifusión)					
<b>Clase E</b>	1	1	1	1	(direcciones reservadas: no se pueden utilizar)					

Tabla 10.1 Clases de direcciones IP

Clase	Formato R = Red E=Equipo	Número de redes	Equipos por red	Rango de direcciones de redes	Máscara de subred
A	R.E.E.E	128	16.777.214	0.0.0.0 - 127.0.0.0	255.0.0.0
B	R.R.E.E	16.384	65.534	128.0.0.0 - 191.255.0.0	255.255.0.0
C	R.R.R.E	2.097.152	254	192.0.0.0 - 223.255.255.0	255.255.255.0
D	grupo	-	-	224.0.0.0 - 239.255.255.255	-
E	no válidas	-	-	240.0.0.0 - 255.255.255.255	-

**Tabla 10.2 Rangos de las direcciones IP**

Es importante hacer hincapié en que las direcciones IP se dividen en dos partes:

La parte de identificador de red y la parte de identificador de equipo. Por ejemplo:

De la dirección 192.168.45.21, es de clase 'C', de ésta se obtiene:

La parte correspondiente al identificador de red es: 192.168.45. y la parte correspondiente al equipo es: 21.

### 10.5.1 La máscara de subred

Una máscara de subred es aquella dirección que enmascarando nuestra dirección IP, nos indica si otra dirección IP pertenece a nuestra subred o no.

La siguiente tabla 10.3 muestra las máscaras de subred default correspondientes a cada clase:

Clase	Máscara de subred
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

**Tabla 10.3 Tabla de máscaras según la clase**

Si expresamos la máscara de subred de clase A en notación binaria, tenemos:

11111111.00000000.00000000.00000000

El grupo de los unos indican los bits de la dirección correspondientes a la red y los ceros indican todos los bits correspondientes al equipo.

Se debe destacar que para configurar subredes, los únicos *bytes* que pueden variar son los correspondientes al identificador de equipo de la clase de máscara que se desee procesar para hacer una subred.

### 10.6 Direcciones IP Reservadas

Las direcciones IP reservadas más importantes son:

- **La dirección de identificación de la red:** Es una estructura de cuatro A.B.C.D, con la característica de que por ejemplo, si la dirección IP es de clase B, esto indica que los primeros dos bytes identifican a la red, pero los dos bytes restantes deben estar en cero, por ejemplo, 135.48.0.0.
- **La dirección de difusión ó broadcast:** Si tomamos la dirección del ejemplo anterior tenemos que su dirección de difusión es: 135.48.255.255.
  - **Broadcast.-** Manda un mensaje a todos los equipos de una red.
- **Loopback:** Es una dirección que sirve para verificar el correcto funcionamiento de la torre de protocolos TCP/IP en un equipo en particular.

Significado	Ejemplo
Red indicada	192.168.1.0
Difusión a la red indicada	192.168.1.255
Loopback	127.0.0.1

Tabla 3.3 Ejemplo de direcciones IP reservadas

La tabla 3.3 muestra las direcciones IP reservadas, se debe tener cuidado de no asignar a un equipo alguna de estas direcciones debido a que son reservadas para la descripción de la tabla citada.

### 10.7 Subredes

Cuando una red de computadoras se vuelve muy grande, conviene dividirla en subredes, por los siguientes motivos:

- Reducir el tamaño de los dominios de *broadcast*.
- Hacer la red más manejable, administrativamente.
- Controlar de tráfico entre diferentes subredes.
- Etc.

Existen diversas técnicas para conectar diferentes subredes entre sí, como por ejemplo:

- A nivel físico mediante repetidores o concentradores.
- A nivel de enlace de datos, mediante puentes o conmutadores.
- A nivel de red mediante *routers*.
- A nivel de aplicación mediante *gateways*.
- Etc.

Para hacer subredes a partir de una red dada se tiene que partir de la idea de que una subred no es más que la división de una red con máscara *default*, por ejemplo tenemos la dirección IP 192.168.1.0 con su máscara *default* 255.255.255.0 como lo muestra la tabla 10.2.

Esta red puede dividirse en diferentes subredes cada una con un número diferente de equipos tal y como lo muestra la tabla 10.

Máscara de subred	Binario	Número de subredes	Equipos por subred	Subredes (x=a.b.c por ejemplo, 192.168.1)
255.255.255.0	00000000	1	254	x.0
255.255.255.128	10000000	2	126	x.0, x.128
255.255.255.192	11000000	4	62	x.0, x.64, x.128, x.192
255.255.255.224	11100000	8	30	x.0, x.32, x.64, x.96, x.128, ...
255.255.255.240	11110000	16	14	x.0, x.16, x.32, x.48, x.64, ...
255.255.255.248	11111000	32	6	x.0, x.8, x.16, x.24, x.32, x.40, ...
255.255.255.252	11111100	64	2	x.0, x.4, x.8, x.12, x.16, x.20, ...
255.255.255.254	11111110	128	0	ninguna posible
255.255.255.255	11111111	256	0	ninguna posible

**Tabla 10.4 Subredes de la red 192.168.1.0**

En la tabla 10.4 se puede observar la nueva máscara de red así como el número de subredes y el número de equipos de cada subred generada, no obstante al número de equipos se le deben de restar 2 direcciones IP ya que la primera será la dirección de red y la segunda y última será el *broadcast* de la nueva subred.

## 10.8 Redes Privadas

Cuando se requiere que un servidor por ejemplo este disponible en Internet bajo una misma dirección IP, es necesario contratar dicha dirección IP del tipo público. Debido a que esta contratación implica un costo a la organización que las desea contratar, se recurrieron a diversas estrategias; una de ellas fue el concepto de las subredes, ya que éstas nos permiten tener un número muy reducido de direcciones IP públicas, las cuales tienen un precio mucho menor si hablamos de contratar seis direcciones IP, a todo un segmento de 256 direcciones IP.

Por otro lado una vez contratado un pequeño segmento de direcciones IP, es necesario un servidor *Proxy* el cual tiene dos direcciones IP, una de la red privada y otra de la red pública.

La misión del *Proxy* es dar salida a Internet a la red privada, pero no permitir los accesos desde el exterior a la zona privada de la organización o empresa.

A manera de ilustrar la diferencia e importancia de las direcciones IP públicas, así como, la importancia de una red privada con sus direcciones IP privadas, se explicará la figura 10.1.

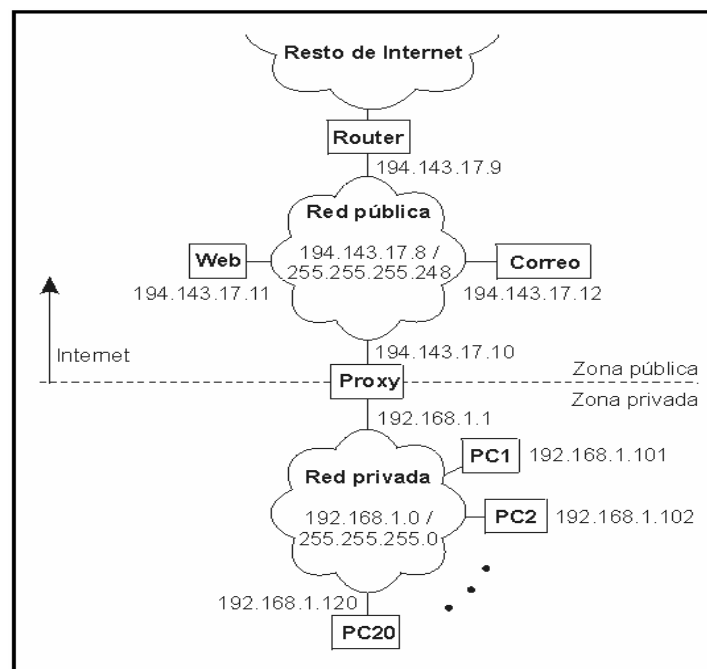


Figura 10.1 Diferencias entre IP públicas E IP privadas

La figura 10.1 muestra un servidor de correo, un servidor Web y un *router*, que funciona como puerta de enlace. Todos ellos con el identificador de red 194.143.17, el cual hace referencia a una red de clase 'C'. Las direcciones IP 194.143.17.9, 194.143.17.11 y 194.143.17.9 son públicas.

En la misma figura se puede observar al servidor Proxy, el cual tiene dos direcciones, una pública 194.143.17.10 y otra privada 192.168.1.1 para dejar salir a las estaciones de trabajo de la red privada a Internet, las cuales pertenecen a la misma red del Proxy en la parte privada.

De esta forma sólo se utilizaron 4 direcciones públicas y 21 direcciones privadas que van de la 192.168.1.101 hasta la 192.168.1.120, para las 20 estaciones de trabajo, más la del servidor *Proxy*, que es la dirección 192.168.1.1, de esta forma sólo se paga por las tres direcciones IP públicas dejando al administrador de la red hacer uso de las direcciones IP privadas que se necesiten para hacer funcionar una red privada.

Si el lector requiere saber más acerca de las direcciones IP y su estructura se le recomienda ir al RFC 1166.

El direccionamiento IP es clave a la hora de diseñar una red física, es por ello que se debe de tener el mayor cuidado posible a la hora de direccionar equipos, sin olvidar levantar el inventario de direcciones IP correspondiente, con la finalidad de evitar conflictos de direccionamiento IP en la red.

## **11.1 Introducción**

En este capítulo se dará una breve reseña de la utilización de la aplicación para el monitoreo de redes *MG – Soft MIB Browser*.

En este software se puede descubrir a los agentes SNMP previamente configurados en la red.

La aplicación permite entre otras cosas poder monitorear interfaz por interfaz de cada dispositivo y poner cada objeto monitoreado en la misma gráfica para hacer comparaciones y tomar decisiones para el rediseño de redes.

## 11.2 Interfaz de MG – SOFT MIB Browser

La ventana principal de la aplicación la muestra la figura 11.1.  
A continuación se procederá a dar una breve y concisa descripción de las partes que la componen.

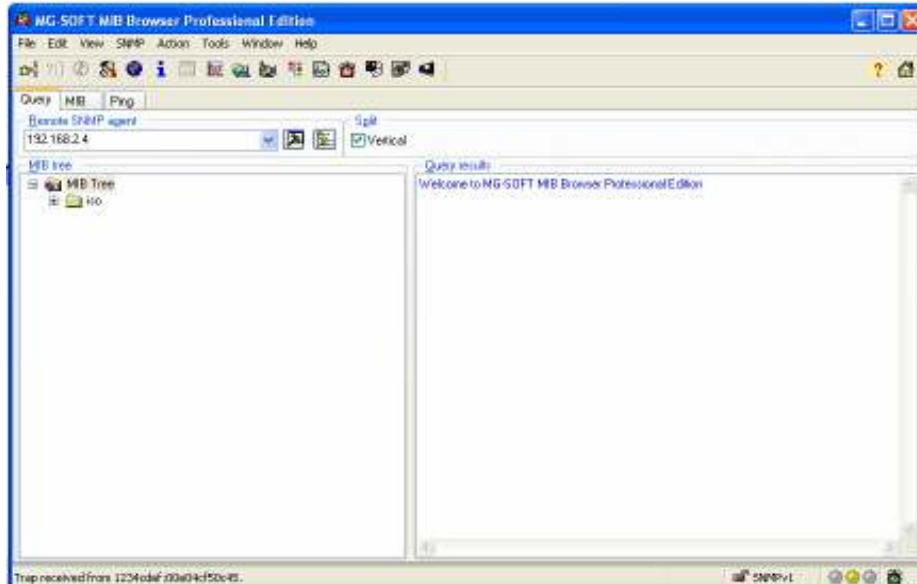


Figura 11.1 Venta principal de “MG – SOFT MIB Browser”

## 11.3 Barra de menús

Esta barra contiene los menús de: “File”, “Edit”, “View”, “SNMP”, “Action”, “Tools”, “Window” y “Help”. Estos menús pueden ser expandidos para mostrar una lista de comandos propia de cada menú. Los comandos de la lista de menú son usados para ejecutar operaciones de la aplicación como lo muestra la figura 11.2.

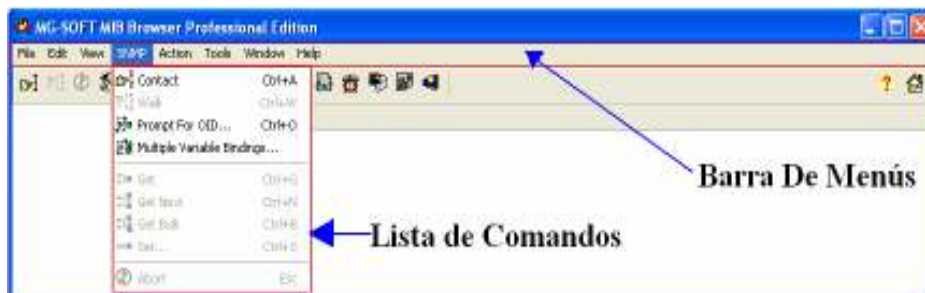


Figura 11.2. Barra de Menús y Lista de Comandos



## 11.4 Barra de herramientas

Esta barra contiene los botones que llevan a cabo las operaciones de ejecución de comandos más importantes del programa.

En la figura 11.3 se observa la barra de herramientas.



Figura 11.3. Barra de herramientas.

## 11.5 La barra de estados

La figura 11.4 muestra la barra de estados, esta barra contiene 5 campos que despliegan diferentes tipos de información.

El campo 1 informa acerca de los últimos cambios ó acciones en la MIB Browser. Por ejemplo, informa que una búsqueda de un agente SNMP ha concluido, que el tiempo del petición se ha agotado o cual nodo de la MIB ha sido seleccionado, etc. El campo 2 muestra el número de paquetes SNMP mandados de la MIB Browser. Este valor es reiniciado cada nueva búsqueda.

El tercer campo muestra la versión de SNMP que se esta usando en el momento de la solicitud.

El cuarto campo es un indicador de estado.

El quinto campo muestra un reloj de alarma, el cual notifica de algún *TRAP* SNMP recibido.

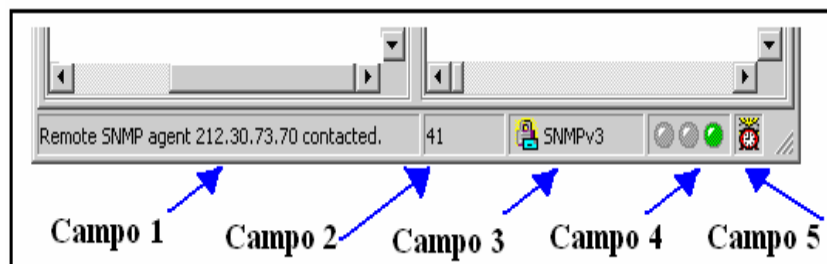


Figura 11.4. Barra de Estados

## 11.6 El área de trabajo

El área de trabajo se encuentra entre la barra de tareas y la barra de estados como lo muestra la figura 10.5.

Adviértase que para que el área de trabajo se pueda ver como lo muestra la figura 11.5, se debe tener palomeada la caja “*Vertical*”.

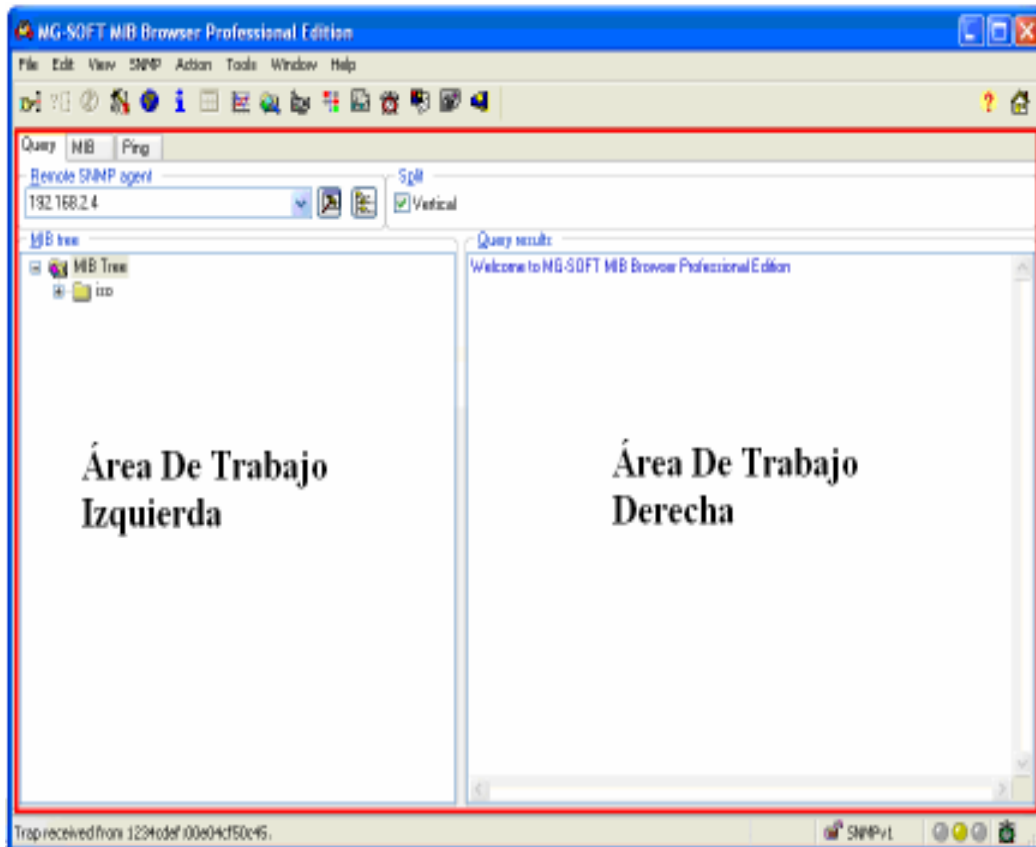


Figura 11.5. Área de trabajo.

Esta área de trabajo contiene tres pestañas: “*Query*”, “*MIB*” y “*Ping*”. La pestaña de “*Query*” muestra el área de trabajo, ilustrada en la figura 11.5, en esta se puede observar el campo de “*Remote SNMP agent*”, en donde se introduce la dirección IP del agente que va a ser consultado por el MIB Browser. Una vez escrita la dirección IP, el área de trabajo izquierda mostrara el árbol donde se encuentra el nodo “*MIB-2*” con los grupos correspondientes. En el área de trabajo derecha se observan datos de la conexión con el agente.

## 11.7 La pestaña Query

La pestaña de “*Query*” tiene delante 2 botones adicionales: “*SNMP Protol Preferences*” como lo muestra la figura 11.6. Dando un clic sobre este botón se obtiene la ventan “*SNMP Protol Preferences*”. La cual nos permite seleccionar la versión de protocolo SNMP que deseamos utilizar, así como la comunidad pública y privada entre los datos más importantes.

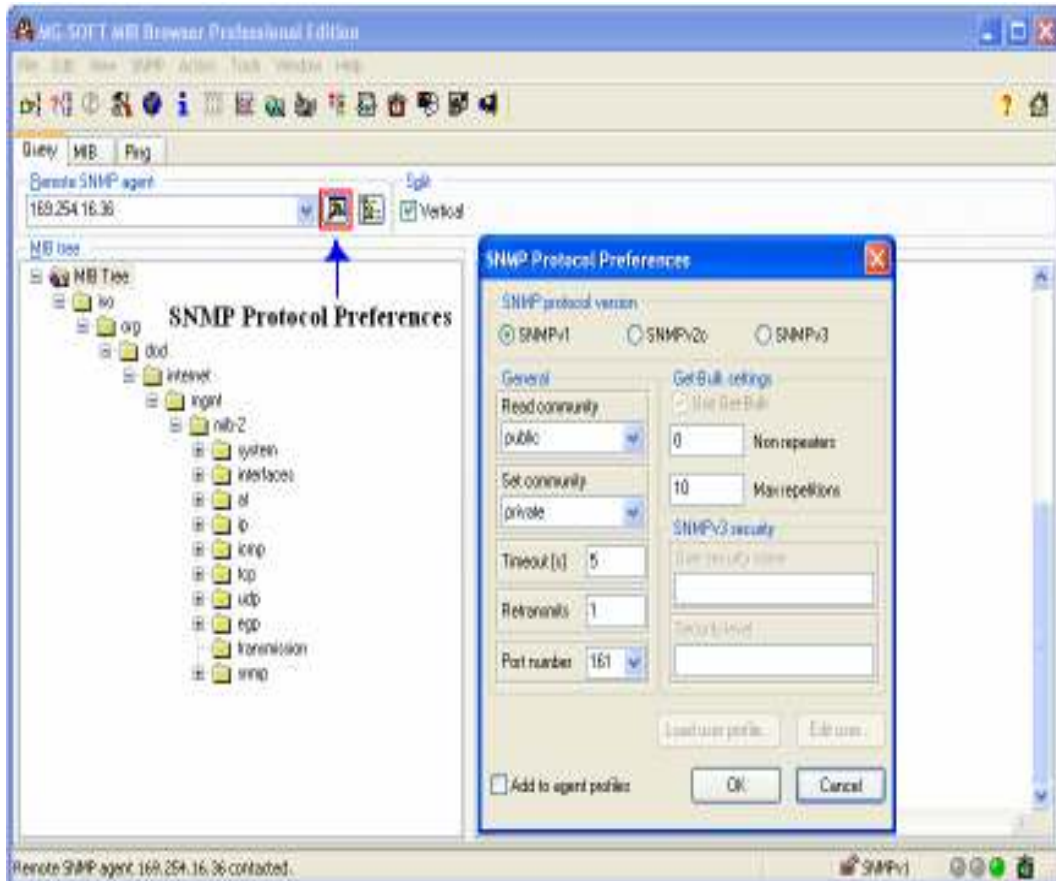


Figura 11.6. Ventana “SNMP Protocol Preferences”.

La siguiente opción que nos ofrece la pestaña de “*Query*” es la de “*Agents Profiles*”, la cual nos permite conocer información más detallada del agente en cuestión. Esta ventana también nos permite entre otras cosas, configurar la comunidad a la que pertenece el equipo que se esta monitoreando, como se puede ver en la figura 11.7.

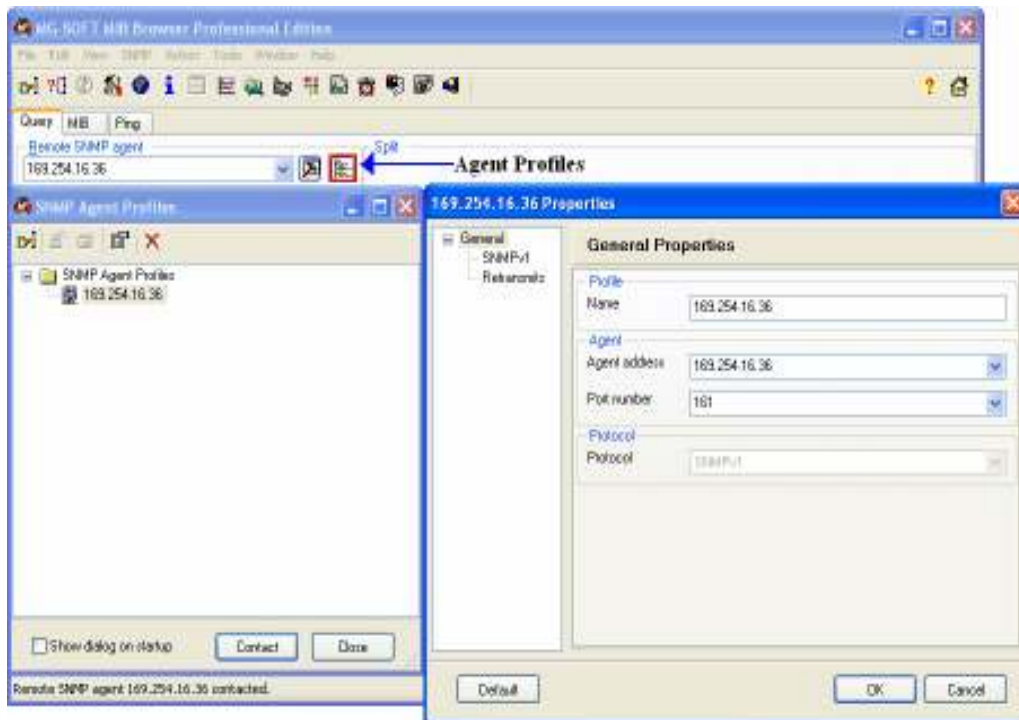


Figura 11.7. Ventana de “Agent Profiles”

## 11.8 Contactar con un agente SNMP

En la ventana principal de MG- SOFT verificar que la pestaña de “*Query*” esté activada. En el campo de “*Remote SNMP agent*” introducir la dirección IP del equipo remoto que se desea contactar, posteriormente dar un clic sobre el botón “*Contact Remote SNMP Agent*”, el cual se encuentra en la barra de herramientas y es ilustrado en la figura 11.8.

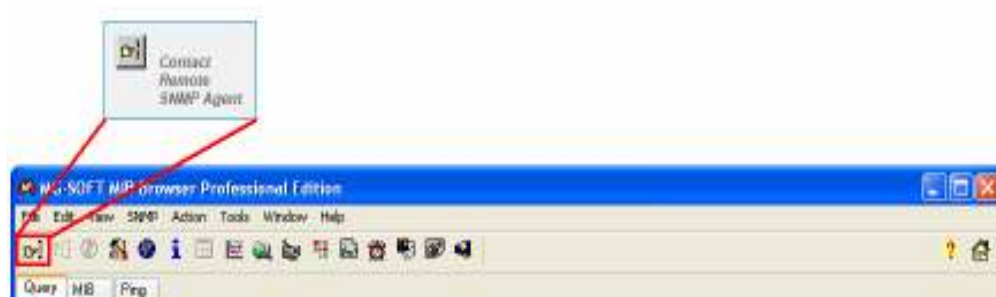


Figura 11.8. Botón “Contact Remote SNMP”

Hecho esto, el MIB Browser contactará al agente SNMP y desplegará, si éste responde, la información correspondiente a dicho agente, es decir en el panel izquierdo del área de trabajo, mostrará el árbol MIB del agente y en el panel derecho la notificación de que el agente fue contactado.

### 11.9 Selección de nodos en el Árbol MIB

La estructura del árbol puede desplegarse de dos formas: la primera es dando un clic derecho sobre el nodo “MIB Tree”, para hacer aparecer a un menú contextual donde seleccionaremos la opción de “Expand”, la cual expandirá en su totalidad el árbol, y la segunda es dar clic izquierdo sobre el signo “+” en la parte izquierda de cada nodo (cuando no se ha ejecutado la opción “Expand”).

La figura 11.9, muestra la expansión del árbol MIB.



Figura 11.9. Estructura del Árbol MIB

## 11.10 Organización del árbol MIB

El Árbol MIB esta organizado de la siguiente manera:

**Nodo Raíz (MIB Tree).**- Es el nodo principal del árbol MIB, de él se desprenderán todos y cada uno de los grupos de objetos del agente SNMP.

**El Nodo Raíz de Sub-Árbol.**- Representa a un grupo de objetos con sus instancias.

### Tipos de objetos:

- **Objetos Columnares.**- Son todos aquellos que tienen instancias.
- **Objetos Escalares.**- Son aquellos que carecen de instancias.

La figura 11.10 muestra como se organiza el árbol MIB, con la respectiva clasificación de sus nodos y objetos.

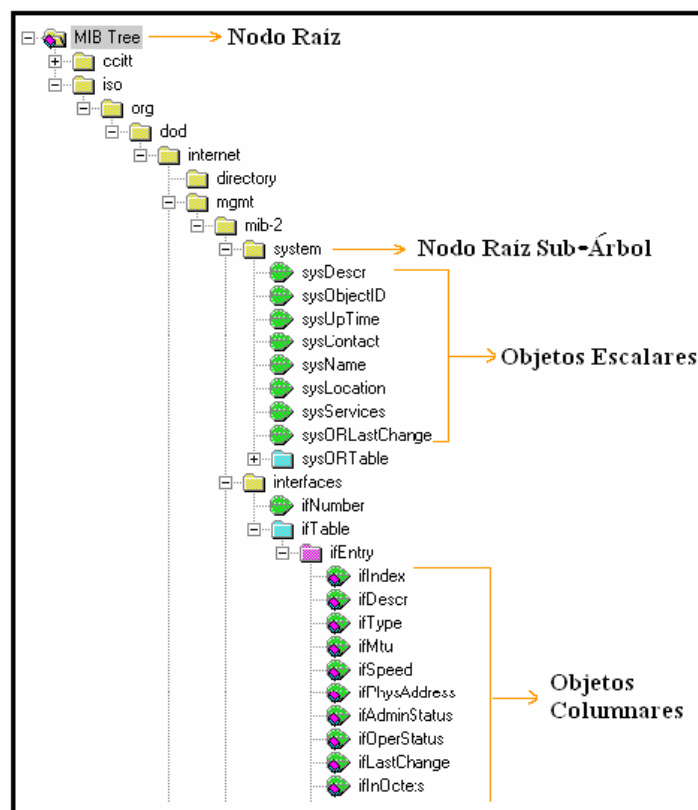


Figura 11.10. Organización del Árbol MIB

## 11.11 Propiedades de un nodo

Si se requiere ver las propiedades de un nodo, simplemente se selecciona el nodo en el árbol y se da un clic derecho sobre éste, cuando salga el menú contextual seleccione propiedades para que se genere la ventana “*MIB Node Properties*”, para este ejemplo se seleccionó el objeto escalar “*sysUpTime*”, su ventana de propiedades se muestra en la figura 11.11.

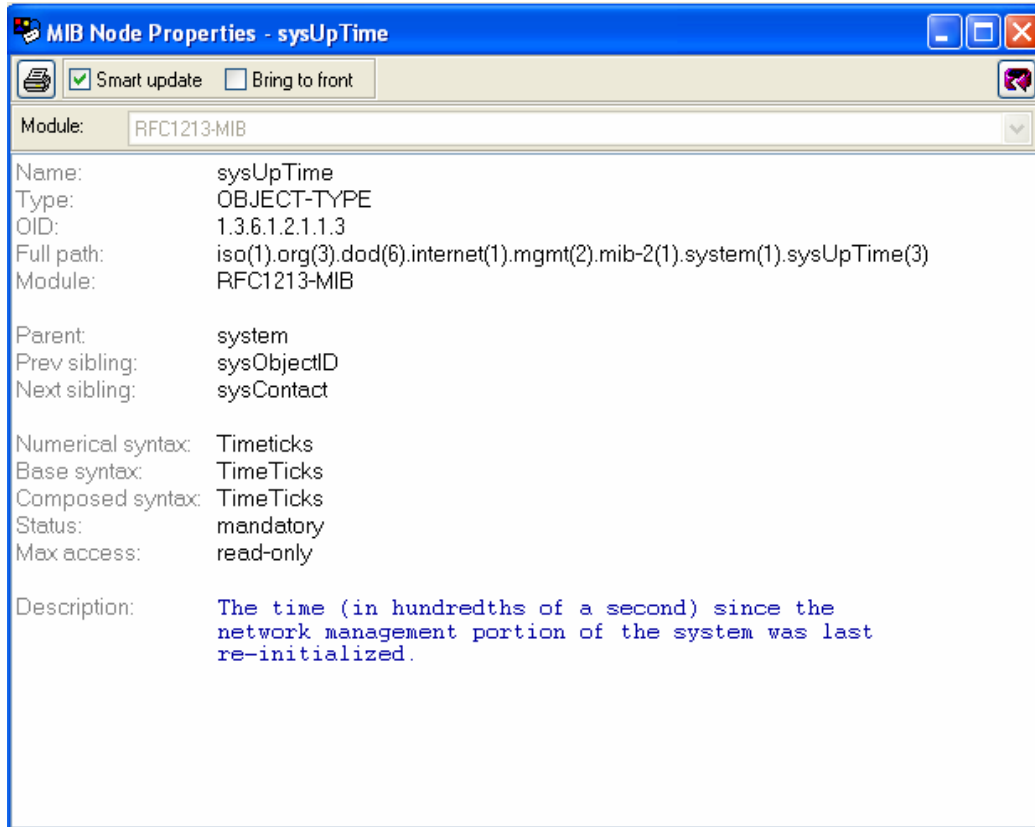


Figura 11.11. Ventana “MIB Node Properties - sysUpTime”

## 11.12 Especificación de los parámetros del protocolo SNMPv1

En esta sección se describirá como configurar los parámetros del protocolo SNMPv1 que el MIB Browser usa cuando se comunica con un agente SNMP remoto.

1.- Para especificar los parámetros seleccionar “View” / “SNMP Protocol Preferences”, una vez hecho esto la ventana “SNMP Protocol Preferences” aparecerá, como lo muestra la figura 11.12.

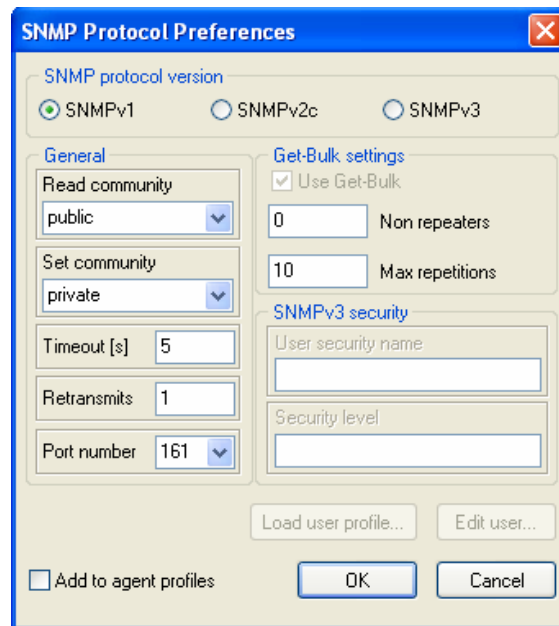


Figura 11.12 Venta “SNMP Protocol Preferences”

Se puede seleccionar entre las tres versiones del SNMP disponibles, con solo dar un clic sobre el “Radio” de alguna de ellas.

### 11.12.1 Configuración de SNMPv1.

Para usar SNMPv1, se requiere dar un clic sobre el “Radio” correspondiente y especificar los siguientes parámetros.

1.- En el campo “Read community”, se activa con un clic el menú flotante, para especificar la cadena que identifica la comunidad de lectura: Por ejemplo, “Public”.

- Este parámetro es usado por las operaciones del tipo “Get”, las cuales se describieron en el capítulo 6.

2.- En el campo “Set community”, se activa con un clic, el menú desplegable, para especificar la cadena de la comunidad que puede hacer cambios.



- Este parámetro es usado únicamente por la operación “SetRequest”.

3.- Dentro del campo “*Timeout[s]*”, colocar un valor en segundos que indica cuanto tiempo se debe esperar la respuesta de un agente SNMP sometido a una petición SNMP.

4.- En el campo “*Retransmits*”, introducir el número de retransmisiones, es decir, cuantas veces el programa repetirá la búsqueda, en dado caso que el agente no haya respondido en el tiempo especificado.

5.- En el campo “*Port number*” se especifica el número de puerto por el cual el agente remoto escucha, por omisión se utiliza el 161 debido a que este puerto corresponde al protocolo UDP.

7.- Para salvar los cambios efectuados dar un clic en la caja “*Add agent profiles*”.

8.- Dar un clic en el botón “OK” para cerrar la ventana de diálogo y aplicar los cambios.

Adviértase que para este trabajo se utilizará el protocolo SNMPv1 debido a que las otras versiones solo agregan un algoritmo de seguridad el cual no es necesario para la demostración del funcionamiento del protocolo SNMP.

### 11.13 Configuración del un perfil de agente

Un perfil de agente almacena toda la información requerida para contactar y administrar a un agente SNMP en particular sobre la red.

Una vez configurado el perfil de agente, se puede contactar y buscar a un agente SNMP simplemente escogiendo su perfil en la ventana “*SNMP Agent Profiles*”.

Para crear y configurar un perfil de agente SNMP, se debe hacer lo siguiente:

1.- Seleccionar de la barra de menús la opción ***View / SNMO Agent Profiles*** y dar un clic sobre este comando, para que abra la ventana de “*SNMP Agent Profiles*” como lo muestra la figura 11.13.

Esta ventana contiene una estructura jerárquica compuesta de iconos que representan fólder y perfiles de agentes SNMP.

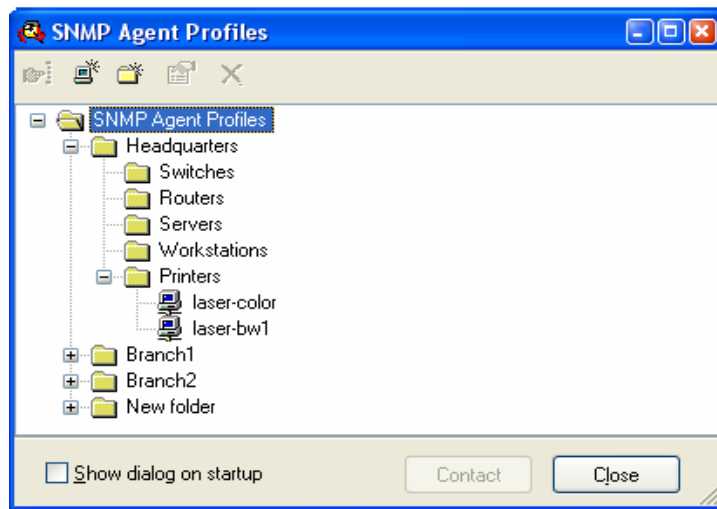


Figura 11.13 Ventana “SNMP Agent Profiles”

3.- Para crear un nuevo perfil de agente dentro de un f3lder en particular, dar un clic derecho y seleccionar el comando “*New SNMP Agent Profile*”.

4.- Aparecer3 el icono del Nuevo perfil de agente, al cual se le debe de asignar un nombre. Como lo muestra la figura 11.14.



Figura 11.14. Creaci3n de un nuevo perfil de agente SNMP

5.- Para configurar las propiedades del agente, se requiere seleccionar el icono creado, y dar un clic derecho para hacer aparecer en men3 contextual y de 3ste seleccionar el comando “*Properties*”, de esta forma aparecer3 la ventana de

propiedades de nuestro dispositivo, como lo muestra la figura 11.15, en esta ventana se pueden configurar las propiedades básicas del agente:

- El campo “*Name*”, se refiere al nombre que se seleccionó para el dispositivo, éste es simplemente una etiqueta.
- El campo “*Agent Address*”, se refiere a la dirección IP del agente SNMP que se desea sea administrado.
- El campo “*Port Number*”, especifica el número de puerto sobre el cual el agente escuchará una petición SNMP entrante.
- El campo “*Protocol*”, hace referencia a la versión del protocolo SNMP que se utilizará.

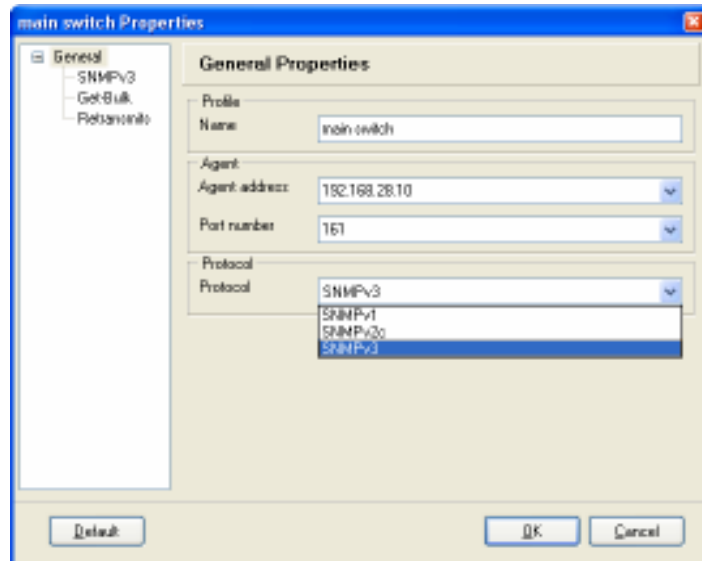


Figura 11.15 Ventana de propiedades del dispositivo

## 11.14 Configuración del protocolo SNMPv1

La configuración del protocolo SNMPv1 se lleva a cabo mediante la elección de la opción “*SNMPv1*”, la cual se encuentra en la parte izquierda de la ventana de propiedades de perfil del agente en cuestión, justo debajo de la opción “*General*”.

Para usar el protocolo SNMPv1, se tienen que introducir los siguientes parámetros en la ventana de propiedades:

- Read community: ***public***
- Set community: ***private***

En el campo “*Read community*”, se especifica el nombre de la comunidad de lectura, en la cual el parámetro “*public*” será incluido en las operaciones SNMP del tipo “*Get*”, que el MIB Browser mandará al agente.

En el campo “*Set community*”, se especifica el nombre de la comunidad de escritura, en la cual el parámetro “*private*” será incluido en la operación SNMP del tipo “*SetRequest*” que el MIB Browser mandará al agente.

A manera de ejemplo se utilizó “*public*” y “*private*” para cada comunidad respectivamente, pero pueden escribirse cualquier cadena que el administrador de redes crea conveniente. De tal forma que la configuración quedaría como lo muestra la figura 11.16.

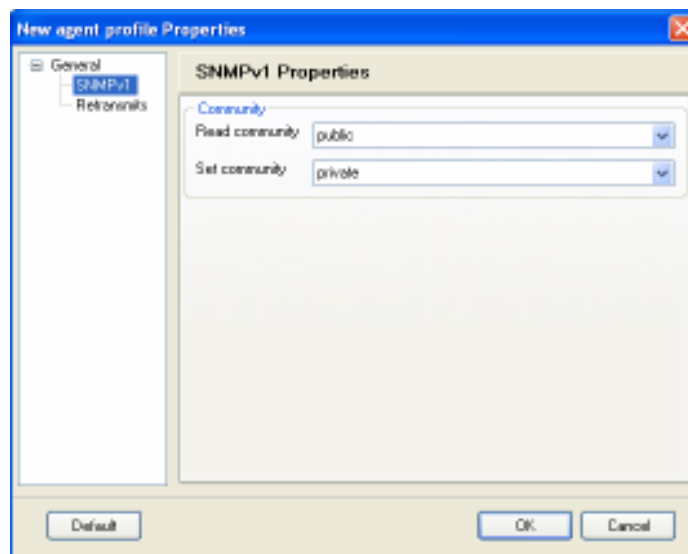


Figura 11.16. Propiedades de perfil del agente SNMPv1

## 11.15 Descubrimiento de agentes SNMP

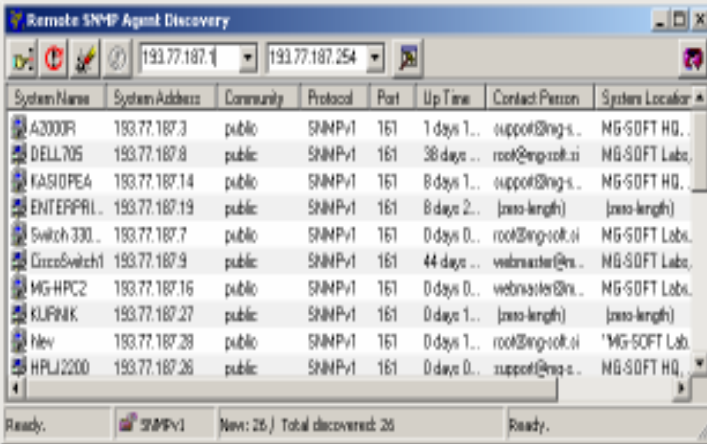
Para descubrir un agente activo en la red, seguir la siguiente ruta: **Tools / Discover Agents**, en la barra de menús. La ventana “*Remote SNMP Agent Discovery*” aparecerá, esta ventana cuenta con dos campos, los cuales indican el rango de direcciones IP donde se buscarán agentes activos.

Dentro de la misma ventana se encuentra el botón de “*SNMP Protol Preferences*”. Al dar un clic sobre este botón aparecerá la ventana correspondiente, en la cual se deben tomar en cuenta los datos que aparecen en ésta, como: la versión del

protocolo SNMP, la comunidad, y el número de puerto, este paso es importante ya que el MIB Browser descubrirá sólo agentes que respondan a estos parámetros.

Para empezar a descubrir agentes, dar un clic en el botón “*Start Remote SNMP Agent Discovery*”, que se encuentra en la barra de herramientas de la ventana principal.

El MIB Browser descubrirá y desplegará una lista de los agentes descubiertos con el nombre del equipo, dirección IP, entre otros parámetros como lo muestra la figura 11.17.



The screenshot shows a window titled "Remote SNMP Agent Discovery". At the top, there are two IP address input fields, both containing "193.77.187.1". Below the input fields is a table with the following columns: System Name, System Address, Community, Protocol, Port, Up Time, Contact Person, and System Location. The table contains several rows of data, including entries like "A2000R", "DELL705", "KASIOPE4", "ENTEPPRI...", "Switch 330...", "CiscoSwitch1", "MG-HPC2", "KUFNIK", "New", and "HPLJ2200". At the bottom of the window, there is a status bar that reads "Ready." on the left, "SNMPv1" in the middle, and "New: 26 / Total discovered: 26" on the right.

System Name	System Address	Community	Protocol	Port	Up Time	Contact Person	System Location
A2000R	193.77.187.3	public	SNMPv1	161	1 days 1..	support@mg.s...	MG-SOFT HQ..
DELL705	193.77.187.8	public	SNMPv1	161	38 days ..	root@mg-soft.i	MG-SOFT Labo
KASIOPE4	193.77.187.14	public	SNMPv1	161	8 days 1..	support@mg.s...	MG-SOFT HQ..
ENTEPPRI...	193.77.187.19	public	SNMPv1	161	8 days 2..	(zero-length)	(zero-length)
Switch 330...	193.77.187.7	public	SNMPv1	161	0 days 0..	root@mg-soft.i	MG-SOFT Labo
CiscoSwitch1	193.77.187.9	public	SNMPv1	161	44 days ..	webmaster@mg...	MG-SOFT Labo
MG-HPC2	193.77.187.16	public	SNMPv1	161	0 days 0..	webmaster@mg...	MG-SOFT Labo
KUFNIK	193.77.187.27	public	SNMPv1	161	0 days 1..	(zero-length)	(zero-length)
New	193.77.187.28	public	SNMPv1	161	0 days 1..	root@mg-soft.i	MG-SOFT Labo
HPLJ2200	193.77.187.26	public	SNMPv1	161	0 days 0..	support@mg.s...	MG-SOFT HQ..

Figura 11.17. Agentes descubiertos

## 11.16 Monitoreo, Gráficas y Estadísticas:

Para llevar a cabo un monitoreo de un agente en específico lo primero que se tiene que hacer es contactar con éste.

Una vez hecho el contacto con el agente deseado, se debe dar un clic sobre el botón “*Graph*”, que se encuentra en la barra de herramientas, este acto hará aparecer la ventana “*Graph*” la cual se muestra en la figura 11.18. En la barra de herramientas de esta ventana se encuentra un botón denominado “*New Graph*”, él cual, al darle un clic, mandará a llamar a la ventana “*Graph Properties*”. Figura 11.19. En esta ventana se debe seleccionar entre otras cosas el objeto el cual se desea monitorear.

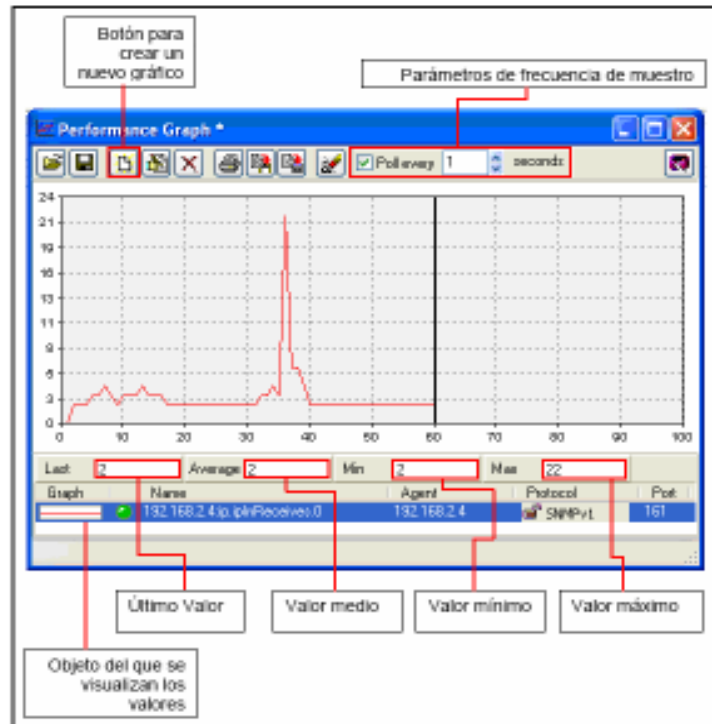


Figura 11.18. Ventana “Graph”

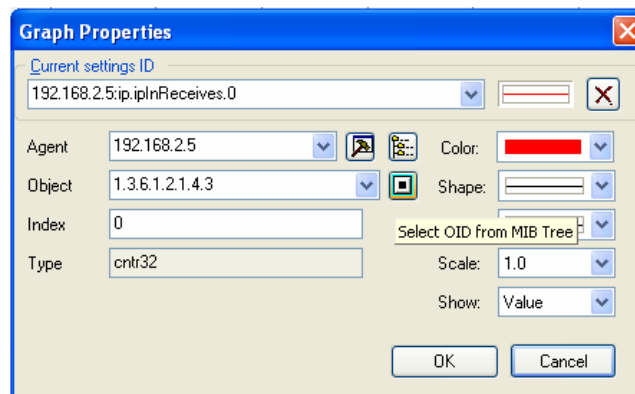
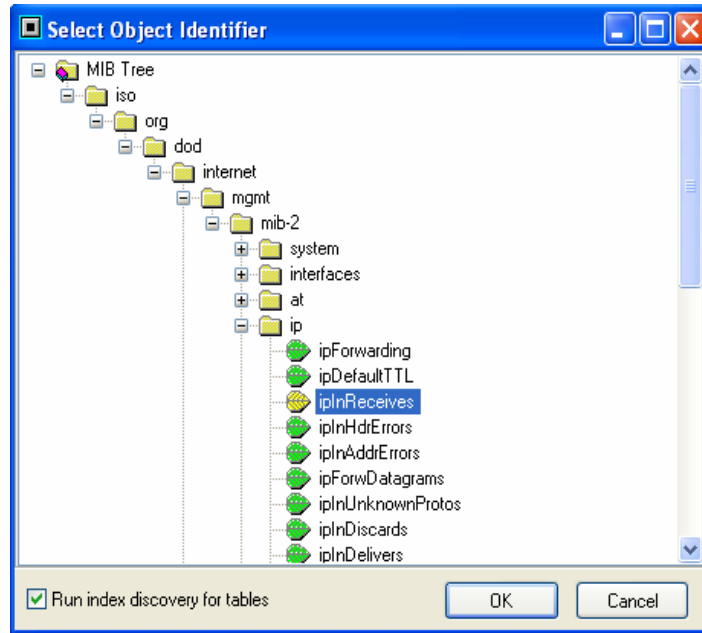


Figura 11.19. Ventana “Graph Properties”

El objeto deseado puede ser seleccionado del árbol MIB, si se da un clic en el botón “*Select OID From MIB Tree*”, el cual llevará a la ventana “*Select Object Identifier*”. figura 11.20, donde se podrá desplegar el árbol MIB y en éste seleccionar el objeto deseado. Si se selecciona un objeto columnar, la ventana “*Select Table Instance*” aparecerá, una vez seleccionada la instancia dando doble

clic sobre ésta (Es el índice), se regresa a la ventana “*Graph Properties*”, para continuar la configuración.



**Figura 11.20.** “Select Object Identifier”

En la ventana “*Graph Properties*”. figura 11.19, en el lado derecho se pueden observar propiedades que se pueden configurar para la gráfica que se obtendrá en el monitoreo, entre éstas, se encuentran las siguientes:

**Value.-** La gráfica muestra el valor actual recuperado del agente SNMP.

- **Delta/Interval.-** La gráfica muestra las diferencias entre el actual y el previamente valor sondeado.
- **Delta/Sec.-** La gráfica muestra la diferencia entre el actual y el previamente sondeado valor dividido por la longitud del sondeo del intervalo.

Adviértase que la línea vertical (eje de las ordenadas) de la gráfica indica la frecuencia del número de paquetes y la línea horizontal (eje de las abscisas) hace referencia al tiempo como se puede observar en la figura 11.18.

Se pueden monitorear dos o más objetos del mismo o diferentes agentes en una misma gráfica, para ello, sólo se tienen que ir colocando la dirección IP de cada

agente, en la ventana “*Graph Properties*”, donde después de indicar la dirección IP del nuevo agente, se podrá seleccionar uno ó más objetos del mismo.

Como se mencionó al principio de este capítulo, este es uno de las muchas herramientas de software que sirven para mandar mensajes SNMP, se recomienda seleccionar una acorde a las necesidades de la organización para la cual se esta llevando el análisis.



## **Capítulo 12**

### **Análisis De La Red Del CAE504**

---

#### **12.1 Introducción**

En este capítulo se adentrará a la estructura y configuración actual de la red del CAE504. Se hablará de los objetivos y misión del CAE504, así como de sus necesidades.

Se documentarán sus dimensiones, con el objetivo de adecuar sus instalaciones de red según los estándares del cableado estructurado.

Se construirá un mapa de la red con la finalidad de conocer su topología, equipos de interconexión y su tamaño.

Se procederá a hacer un inventario de hardware con el objetivo de saber con qué equipo se cuenta, si es que es necesaria alguna modificación ó expansión de la red.

Se elaborará un inventario de direcciones IP con la finalidad de saber qué direcciones IP se pueden o no se pueden asignar a otros equipos en caso de reconfigurar o expandir la red, así como registrar aquellas direcciones que sean externas a la red privada del CAE504.

Se construirá un mapa de la conexión de los equipos de interconexión del CAE504 para llevar a cabo un análisis de eficiencia, en cuanto a su tasa de transferencia y como se administra el ancho de banda entre dispositivos de interconexión.

## 12.2 Objetivos del CAE504

El centro de apoyo extracurricular CAE504 es un espacio perteneciente a la carrera de Ingeniería en Computación creado para satisfacer las necesidades de actividades prácticas que presenta la carrera de Ingeniería en Computación, así como apoyar al proceso enseñanza – aprendizaje de los alumnos y académicos, además de apoyar a los alumnos con cursos que complementen su formación profesional. En el CAE504 se prestan servicios a la comunidad de las licenciaturas de ingeniería de la facultad<sup>1</sup>.

## 12.3 Misión

Apoyar y complementar el proceso de enseñanza-aprendizaje de las asignaturas teórico-prácticas de los mapas curriculares de las licenciaturas de ingeniería pertenecientes a la FES Aragón de la UNAM, así como impartir cursos complementarios de actualización y formación profesional.

## 12.4 Visión

Formar profesionales de alta calidad capaces de resolver problemáticas y necesidades presentes y/o futuras que el país requiere, tanto en el contexto nacional como internacional dentro del marco de la Ingeniería Mecánica Eléctrica, Ingeniería en Computación e Ingeniería Civil.

El Centro de Apoyo Extracurricular CAE504 cuenta con tres áreas de importancia:

- Telecomunicaciones.
- Hardware.
- Software.

Para este trabajo nos orientaremos en el área de telecomunicaciones.

---

<sup>1</sup> Manual de calidad del CAE504

## 12.5 Necesidades de redes en el CAE504

- Internet.
- Optimizar el ancho de banda.
- Dar acceso a cuentas de correo electrónico para los estudiantes y académicos.
- Alojamiento de páginas Web.
- Acceso a la red inalámbrica para laptops.

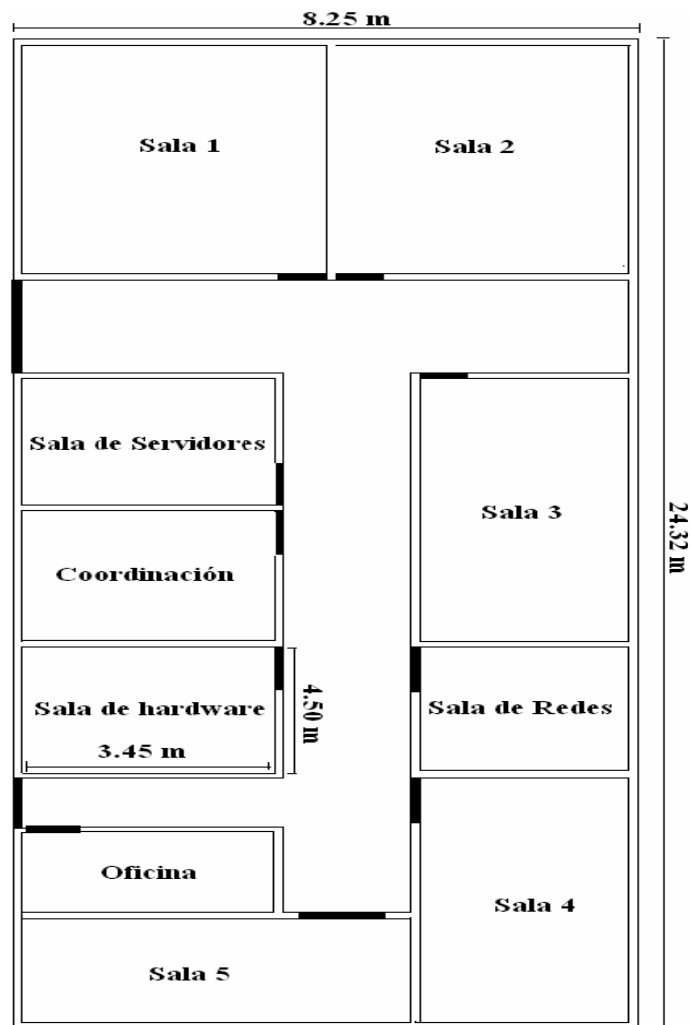


Figura 12.1 Plano del CAE504

## 12.6 Distribución del CAE504

El CAE504 cuenta con 5 salas de computadoras, una sala de hardware, una sala de redes, una sala de servidores y la coordinación.

La figura 12.1 muestra el plano del CAE504, donde se observa la distribución de cada una de las salas que lo componen.

En el plano mostrado en la figura 12.1 se puede observar que la única sala a la que se le tomaron medidas, es la sala de hardware debido a que esta sala será la única modificada en la propuesta que se llevará a cabo en el capítulo 13.

En el capítulo 13 se hablará del modificación propia de la sala de hardware debido a que las recomendaciones del cableado estructurado hacen referencia a que se debe de tener una sala dedicada a las telecomunicaciones.

## 12.7 Topología de la red del CAE504

Las topologías seleccionadas para el diseño de la red del CAE504 fueron las de estrella, utilizando para ello *Switches* y concentradores los cuales fueron conectados en cascada generando un gran árbol.

Es importante destacar que no en todas las salas se cuenta con los servicio de telecomunicaciones, es decir, en la sala 1 sólo se pueden encontrar estaciones de trabajo sin ningún servicio de telecomunicaciones ya sea local ó remoto.

La figura 12.2 muestra el mapa de la red del CAE504. En esta figura se observa que la sala 1 no forma parte de la red. En esta misma figura se puede ver a un conjunto de máquinas conectadas a un equipo de interconexión y este a su vez esta conectado a otro equipo de interconexión y así sucesivamente hasta llegar al *Switch* principal en donde llega la fibra óptica produciendo una gran cascada.

## 12.8 Mapa de la red del CAE504

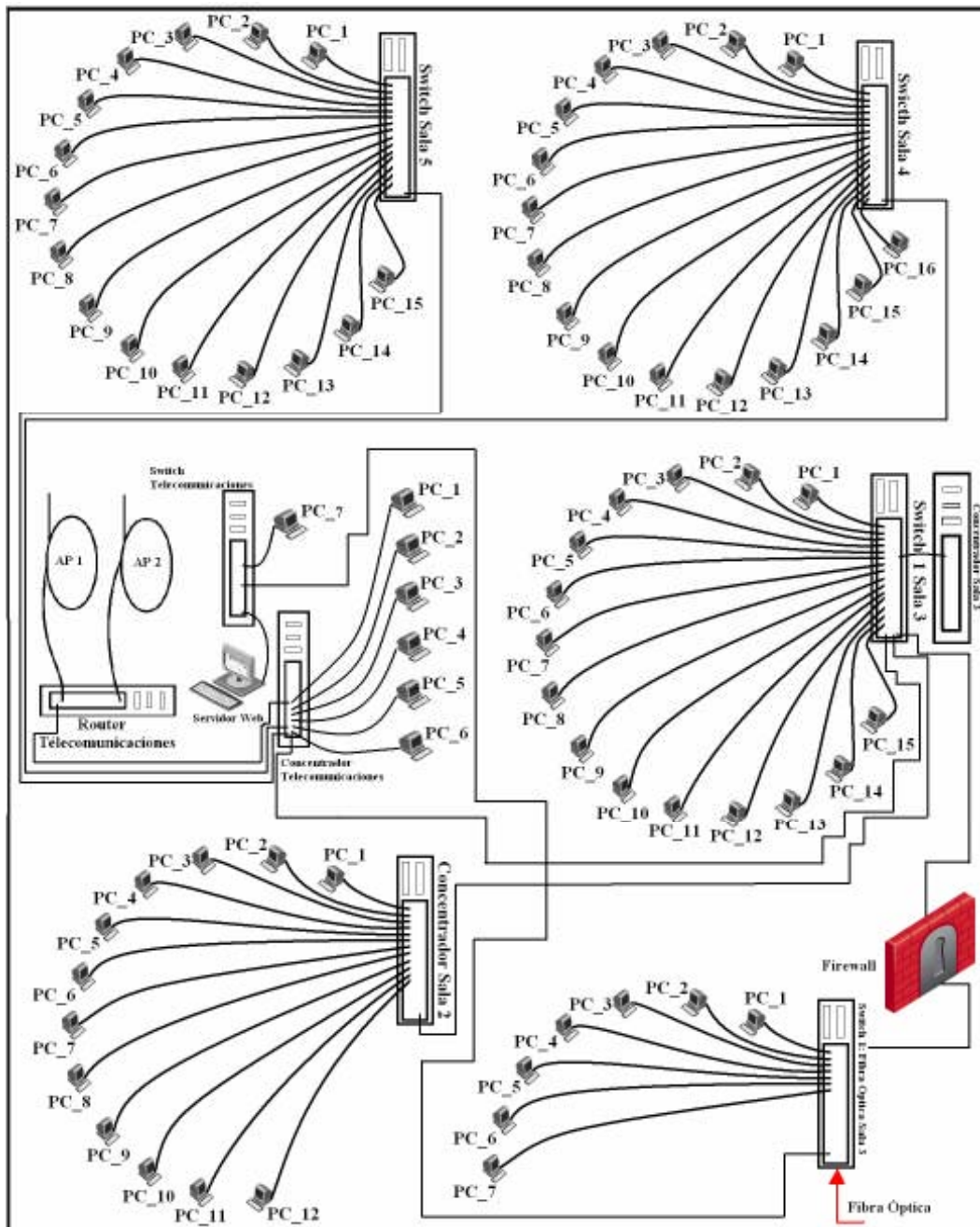


Figura 12.2 Mapa de la red del CAE504

La figura 12.2 muestra a cada dispositivo de interconexión y su relación ya sea con otros equipos de interconexión ó estaciones de trabajo.

La configuración de los equipos de interconexión del CAE504 se muestra en la figura 12.3 donde se aprecia la conexión de los equipos de interconexión dentro de dicho centro de apoyo extracurricular.

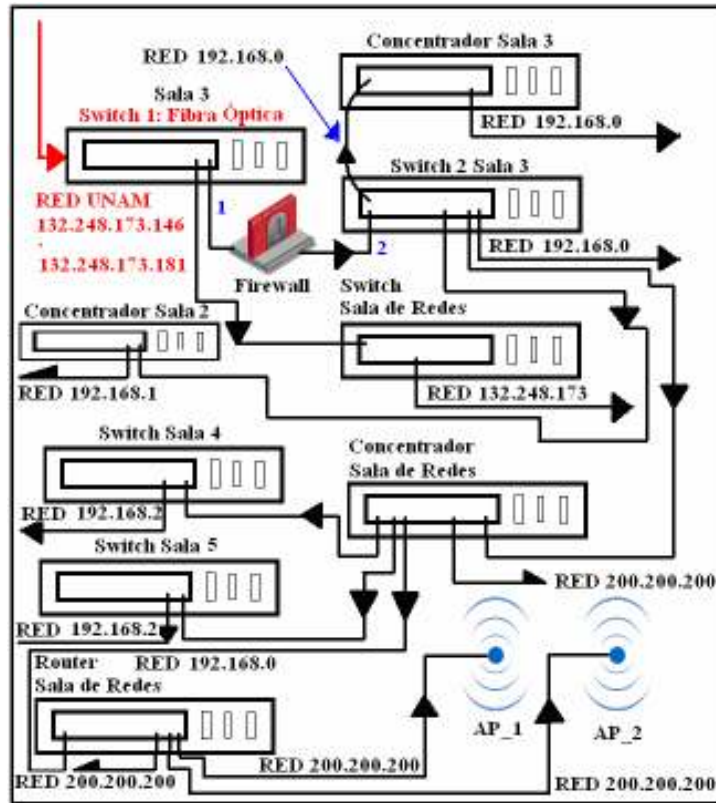


Figura 12.3 Configuración de los equipos de interconexión

La figura 12.3 ilustra como llega la señal de telecomunicaciones del *Backbone* de la UNAM (132.248.173.) a través de la fibra óptica, en el *Switch 1* ubicado en la sala 3, el cual se encarga de llevar las telecomunicaciones al *Firewall* donde éste tiene instalado el servidor *Proxy*, tomando por un lado las telecomunicaciones del *backbone* de la red UNAM etiquetada con un '1' y devolviendo por el otro lado las telecomunicaciones en la red 192.168.0, etiquetada con el número '2', ya como red privada.

El mismo *Switch 1*, también proporciona servicio de telecomunicaciones al *Switch* ubicado en la sala de telecomunicaciones. Este *Switch* se encarga de suministrar

los servicios de telecomunicaciones de manera directa del *backbone* de la red UNAM a un servidor *Web* y otros equipos de propósito general ubicados en la sala de telecomunicaciones.

El *Switch* de la sala de telecomunicaciones suministra servicios de telecomunicaciones a un concentrador ubicado en la misma sala, él cual a su vez distribuye dichos servicios al *Switch* de la sala 4 y al *Switch* de la sala 5, teniendo con esto, los servicios de telecomunicaciones en dichas salas.

Es importante hacer notar que el concentrador de la sala de telecomunicaciones suministra de servicios de telecomunicaciones a un *Router*, el cual se encuentra ubicado en la misma sala, que éste a su vez sirve de puerta de enlace a los *Access Point* para la red inalámbrica.

Como se puede observar en la figura 12.3 el *firewall* tiene la responsabilidad de filtrar tráfico como: la mensajería instantánea (*Messenger*), páginas indeseables de contenido violento y pornográfico, etc.

## 12.9 Inventario de hardware

Para llevar a cabo el inventario de hardware es necesario tomar en cuenta la siguiente información:

**Marca.-** Se refiere al identificador del fabricante.

**Ubicación.-** hace referencia al lugar físico donde se encuentra el dispositivo.

**SO.-** Se refiere al sistema operativo del dispositivo.

**MAC.-** Es la dirección física del dispositivo.

**Interacción.-** Señala una MAC de los dispositivos con los cuales está conectado de manera directa el dispositivo en cuestión.

**Descripción.-** Detalla las características más relevantes de un dispositivo, como el número de puertos.

En seguida se mostrarán una serie de tablas que van de la 12.1 a la 12.11 y en cada una de ellas se hace referencia a un equipo de interconexión y su interacción ya sea con otro equipo de interconexión o con estaciones de trabajo.

Sala 1					
Marca	Ubicación	SO	MAC	Interacción	Descripción
Genérica	Sala 1	WinXp	00-13-20-57-D7-25		Computadora personal
Genérica	Sala 1	WinXp	00-13-20-57-40-4F		Computadora personal
Genérica	Sala 1	WinXp	4C-00-01-73-00-49		Computadora personal
Genérica	Sala 1	WinXp	00-13-20-57-CF-DB		Computadora personal
Genérica	Sala 1	WinXp	0-13-20-57-D6-EB		Computadora personal
Genérica	Sala 1	WinXp	00-08-54-DD-7A-59		Computadora personal
Genérica	Sala 1	WinXp	00-13-20-57-D7-05		Computadora personal
Genérica	Sala 1	WinXp	00-13-20-57-3F-CB		Computadora personal
Genérica	Sala 1	WinXp	00-13-20-57-3F-A7		Computadora personal
Genérica	Sala 1	WinXp	00-08-54-D6-7F-E6		Computadora personal
Genérica	Sala 1	WinXp	00-13-20-57-D6-D6		Computadora personal
Genérica	Sala 1	WinXp	00-13-20-57-D7-11		Computadora personal

Tabla 12.1 Sala 1

Marca	Ubicación	SO	MAC	Interacción	Descripción
3 COM	Sala 2	-	-	Switch sala 3 00-0D-54-C0-87-80	Concentrador de 12 puertos
Genérica	Sala 2	WinXP	00-11-11-39-57-12	Concentrador Sala 2	Computadora personal
Genérica	Sala 2	WinXP	00-11-1139-50-98	Concentrador Sala 2	Computadora personal
Genérica	Sala 2	WinXP	00-11-11-39-51-0C	Concentrador Sala 2	Computadora personal
Genérica	Sala 2	WinXP	00-11-11-39-51-65	Concentrador Sala 2	Computadora personal
Genérica	Sala 2	WinXP	00-11-11-39-56-05	Concentrador Sala 2	Computadora personal
Genérica	Sala 2	WinXP	00-11-11-39-4E-87	Concentrador Sala 2	Computadora personal
Genérica	Sala 2	WinXP	00-11-11-39-56-4E	Concentrador Sala 2	Computadora personal
Genérica	Sala 2	WinXP	00-11-11-39-57-0E	Concentrador Sala 2	Computadora personal
Genérica	Sala 2	WinXP	00-11-11-39-52-2A	Concentrador Sala 2	Computadora personal
Genérica	Sala 2	WinXP	00-11-11-39-55-E1	Concentrador Sala 2	Computadora personal
Genérica	Sala 2	WinXP	00-11-11-39-51-94	Concentrador Sala 2	Computadora personal
Genérica	Sala 2	WinXP	00-11-11-63-66-96	Concentrador Sala 2	Computadora personal

Tabla 12.2 Concentrador Sala 2



Switch Sala 3					
Marca	Ubicación	S.O	MAC	Interacción	Descripción
3 COM	Sala 3	-	00-0D-54-CC-87-80	Firewall 00-10-5A-99-15-8B, Concentrador Sala 2, Concentrador Sala 3, Concentrador Sala de Redes	Switch 24 puertos.
Genérica	Sala 3	WinXP	00-E0-06-09-55-66	00-0D-54-CC-87-80	Computador a personal
Genérica	Sala 3	WinXP	00-01-02-C9-F3-37	00-0D-54-CC-87-80	Computador a personal
Genérica	Sala 3	WinXP	00-0A-E6-A0-9C-48	00-0D-54-CC-87-80	Computador a personal
Genérica	Sala 3	WinXP	00-01-02-C9-F3-1A	00-0D-54-CC-87-80	Computador a personal
Genérica	Sala 3	WinXP	00-10-4B20D3-42	00-0D-54-CC-87-80	Computador a personal
Genérica	Sala 3	WinXP	00-40-F4-14-05-D8	00-0D-54-CC-87-80	Computador a personal
Genérica	Sala 3	WinXP	00-01-02-C1-1026	00-0D-54-CC-87-80	Computador a personal
Genérica	Sala 3	WinXP	00-E0-7DA7B461	00-0D-54-CC-87-80	Computador a personal
Genérica	Sala 3	WinXP	00-01-02-C1-1D-28	00-0D-54-CC-87-80	Computador a personal
Genérica	Sala 3	WinXP	00-16-EC-35-9F-FF	00-0D-54-CC-87-80	Computador a personal
Genérica	Sala 3	WinXP	00-10-4B-20-D8-56	00-0D-54-CC-87-80	Computador a personal
Genérica	Sala 3	WinXP	00-D0-093F-D3-7B	00-0D-54-CC-87-80	Computador a personal

Tabla 12.3 Switch de la sala 3

Concentrador Sala 3					
Marca	Ubicación	S.O	MAC	Interacción	Descripción
3 COM	Sala 3	-	-	Switch sala 3 00-0D-54-CC-87-80	Concentrador 24 puertos.
Genérica	Sala 3	WinXP	00-D0-09-3F-E2-5A	Concentrador 24 puertos	Computadora personal
Genérica	Sala 3	WinXP	00-14-2A-F5-65-89	Concentrador 24 puertos	Computadora personal
Genérica	Sala 3	WinXP	00-01-02-C9-31-A4	Concentrador 24 puertos	Computadora personal

Tabla 12.4 Concentrador sala 3

Switch Sala 4					
Marca	Ubicación	SO	MAC	Interacción	Descripción
CISCO	Sala 4	-	00-0B-BE-5F-E4-40	Concentrador Sala de redes	Switch de 24 puertos
Genérica	Sala 4	WinXP	00-13-D3-15-62-73	00-0B-BE-5F-E4-40	Computadora personal
Genérica	Sala 4	WinXP	00-13-D3-15-61-59	00-0B-BE-5F-E4-40	Computadora personal
Genérica	Sala 4	WinXP	00-13-D3-15-5E-8F	00-0B-BE-5F-E4-40	Computadora personal
Genérica	Sala 4	WinXP	00-13-D3-15-5E-A1	00-0B-BE-5F-E4-40	Computadora personal
Genérica	Sala 4	WinXP	00-13-D3-15-62-8F	00-0B-BE-5F-E4-40	Computadora personal
Genérica	Sala 4	WinXP	00-13-D3-15-60-01	00-0B-BE-5F-E4-40	Computadora personal
Genérica	Sala 4	WinXP	00-13-D3-15-62-6E	00-0B-BE-5F-E4-40	Computadora personal
Genérica	Sala 4	WinXP	00-13-D3-15-62-6D	00-0B-BE-5F-E4-40	Computadora personal
Genérica	Sala 4	WinXP	00-13-D3-15-62-77	00-0B-BE-5F-E4-40	Computadora personal
Genérica	Sala 4	WinXP	00-13-D3-15-5E-98	00-0B-BE-5F-E4-40	Computadora personal
Genérica	Sala 4	WinXP	00-13-D3-15-62-7A	00-0B-BE-5F-E4-40	Computadora personal
Genérica	Sala 4	WinXP	00-13-D3-15-5F-C5	00-0B-BE-5F-E4-40	Computadora personal
Genérica	Sala 4	WinXP	00-13-D3-15-5E-93	00-0B-BE-5F-E4-40	Computadora personal
Genérica	Sala 4	WinXP	2D-FF-FF-FF-FF-FF	00-0B-BE-5F-E4-40	Computadora personal
Genérica	Sala 4	WinXP	00-13-D3-15-61-5A	00-0B-BE-5F-E4-40	Computadora personal
Genérica	Sala 4	WinXP	00-13-D3-15-5F-F8	00-0B-BE-5F-E4-40	Computadora personal

Tabla 12.5 Switch de la sala 4

Switch Sala 5					
Marca	Ubicación	S.O	MAC	Interacción	Descripción
3COM	Sala 5	-	00-0A-04-6F-0B-80	Concentrador Sala de Redes	Switch de 24 puertos
Genérica	Sala 5	WinXP	00-11-09-18-7B-08	00-0A-04-6F-0B-80	Computadora personal
Genérica	Sala 5	WinXP	00-13-D3-C1-E7-2B	00-0A-04-6F-0B-80	Computadora personal
Genérica	Sala 5	WinXP	00-13-03-A6-A3-E5	00-0A-04-6F-0B-80	Computadora personal
Genérica	Sala 5	WinXP	00-13-03-A6-A4-05	00-0A-04-6F-0B-80	Computadora personal
Genérica	Sala 5	WinXP	00-13-D3-A6-A3-FF	00-0A-04-6F-0B-80	Computadora personal
Genérica	Sala 5	WinXP	00-13-D3-C1-E6-54	00-0A-04-6F-0B-80	Computadora personal
Genérica	Sala 5	WinXP	00-0C-76-CB-52-C5	00-0A-04-6F-0B-80	Computadora personal
Genérica	Sala 5	WinXP	00-13-D3-C1-E5-D4	00-0A-04-6F-0B-80	Computadora personal
Genérica	Sala 5	WinXP	00-13-20-57-3C-47	00-0A-04-6F-0B-80	Computadora personal
Genérica	Sala 5	WinXP	00-13-D3-A6-A4-A6	00-0A-04-6F-0B-80	Computadora personal
Genérica	Sala 5	WinXP	00-13-D3-C1-E6-58	00-0A-04-6F-0B-80	Computadora personal
Genérica	Sala 5	WinXP	00-13-D3-C1-E6-50	00-0A-04-6F-0B-80	Computadora personal
Genérica	Sala 5	WinXP	00-13-D3-A6-A4-04	00-0A-04-6F-0B-80	Computadora personal
Genérica	Sala 5	WinXP	00-13-D3-A6-A3-F9	00-0A-04-6F-0B-80	Computadora personal
Genérica	Sala 5	WinXP	00-E0-7D-D0-BB-FD	00-0A-04-6F-0B-80	Computadora personal

Tabla 12.6 Switch de la sala 5

Switch 1 Sala de Redes					
Marca	Ubicación	S.O	MAC	Interacción	Descripción
Trendnet	Sala de Redes	-	-	Switch 1 Sala 3	Switch 12 puertos.
Hubnet Packrat	Sala de Redes	WinXP	00-14-2A-EC-F2-4E	Switch 1 Sala de Redes	Servidor Web
Genérica	Sala de Redes	WinXP	00-14-2A-F5-46-1A	Switch 1 Sala de Redes	Computadora personal
Genérica	Sala de Redes	WinXP	00-14-2A-EC-F594	Switch 1 Sala de Redes	Computadora personal
Genérica	Sala de hardware	WinXP	40-E0-7D-D0-BB-EF	Switch 1 Sala de Redes	Computadora personal

Tabla 12.7 Switch 1 Sala de Redes

Concentrador 1 Sala de Redes					
Marca	Ubicación	SO	MAC	Interacción	Descripción
3COM	Sala de Redes	-	-	Router 1 Sala de Redes 00:04:E2:B8:25:96, Switch 2 Sala 3 00-0D-54-CC-87-80	Concentrador de 12 puertos
Genérica	Sala de Redes	WinXP	00:07:E9:59:B1:65	Concentrador Sala de Redes	Computadora personal
Genérica	Sala de Redes	WinXP	00:08:54:DD:7A:4B	Concentrador Sala de Redes	Computadora personal
Genérica	Sala de Redes	WinXP	00:14:2A:EC:F2:4E	Concentrador Sala de Redes	Computadora personal
Genérica	Sala de Redes	WinXP	00:14:2A:EC:F5:94	Concentrador Sala de Redes	Computadora personal
Genérica	Sala de Redes	WinXP	00:40:F4:B2:0C:D7	Concentrador Sala de Redes	Computadora personal
Genérica	Sala de Redes	WinXP	00:14:2A:F5:4C:1A	Concentrador Sala de Redes	Computadora personal
Genérica	Sala de Redes	WinXP	00:14:2A:ED:6D:65	Concentrador Sala de Redes	Computadora personal

Tabla 12.8 Concentrador de la Sala de Redes

Router 1 Sala de Redes					
Marca	Ubicación	SO	MAC	Interacción	Descripción
MS	Sala de Redes	NOS	00:04:E2:B8:25:96	Concentrador, Access Point 1, 00-12-A9-D5-27-00, Access Point 2 00-12-A9-B8-43-EF	4 puertos RJ45, Un puerto COM, Un puerto WAN

Tabla 12.9 El Router 1 en la Sala de Redes

Marca	Ubicación	SO	MAC	Interacción	Descripción
3COM	Sala de Redes	NOS	00:04:E2:B8:25:96	Router 1 Sala de Redes 00:04:E2:B8:25:96	Access Point para 250 equipos inalámbricos

Tabla 12.10 El Access Point 1 en la Sala de Redes

Switch 1 Fibra Óptica					
Marca	Ubicación	SO	MAC	Interacción	Descripción
3COM	Sala 3		00-12-A9-2E-1B-E0	Firewall 00-10-5A-99-15-8B, Switch Sala de redes	Switch 24 puertos
Genérica	Sala de Servidores	WinXP	00:40:F4:CB:6C:51	00-12-A9-2E-1B-E0	Computadora personal
Genérica	Sala de Servidores	WinXP	00-00-20-C0-CC-FE	00-12-A9-2E-1B-E0	Computadora personal
Genérica	Sala de Servidores	WinXP	00-01-02-C1-1B-F2	00-12-A9-2E-1B-E0	Computadora personal
Genérica	Sala de Servidores	WinXP	00-0D-87-C6-65-2E	00-12-A9-2E-1B-E0	Computadora personal
Genérica	Sala de Servidores	WinXP	00-13-10-57-D6-DE	00-12-A9-2E-1B-E0	Computadora personal
Genérica	Sala de Servidores	Linux	00-10-5A-99-15-8B	00-12-A9-2E-1B-E0	Computadora personal
Genérica	Sala de Servidores	WinXP	00-01-02-C1-1B-F2	00-12-A9-2E-1B-E0	Computadora personal

Tabla 12.11 Switch 1 Fibra Óptica en Sala 3

## 12.10 Inventario de direcciones IP

Para llevar a cabo el inventario de direcciones IP es necesario tomar en cuenta la siguiente información:

**MAC.-** Es la dirección física del dispositivo.

**Dirección IP.-** Se refiere al nombre lógico de un equipo dentro de una determinada red.

**Descripción.-** Detalla las características más relevantes de un dispositivo, como el número de puertos.

En seguida se mostrara una serie de tablas que van de la 12.12 a la 12.17 y en cada una de ellas se hace referencia a la dirección IP relacionada con la dirección MAC correspondiente de cada equipo.

<b>Sala 2</b>		
<b>MAC</b>	<b>Dirección IP</b>	<b>Descripción</b>
00-11-11-39-57-12	192.168.1.130	Computadora personal
00-11-1139-50-98	192.168.1.131	Computadora personal
00-11-11-39-51-0C	192.168.1.132	Computadora personal
00-11-11-39-51-65	192.168.1.133	Computadora personal
00-11-11-39-56-05	192.168.1.134	Computadora personal
00-11-11-39-4E-87	192.168.1.135	Computadora personal
00-11-11-39-56-4E	192.168.1.141	Computadora personal
00-11-11-39-57-0E	192.168.1.136	Computadora personal
00-11-11-39-52-2A	192.168.1.140	Computadora personal
00-11-11-39-55-E1	192.168.1.137	Computadora personal
00-11-11-39-51-94	192.168.1.139	Computadora personal
00-11-11-63-66-96	192.168.1.138	Computadora personal

**Tabla 12.12 Direcciones IP de la sala 2**

<b>Sala 3</b>		
<b>MAC</b>	<b>Dirección IP</b>	<b>Descripción</b>
00-E0-06-09-55-66	192.168.0.152	Computadora personal
00-01-02-C9-F3-37	192.168.0.153	Computadora personal
00-0A-E6-A0-9C-48	192.168.0.154	Computadora personal
00-01-02-C9-F3-1A	192.168.0.156	Computadora personal
00-10-4B20D3-42	192.168.0.157	Computadora personal
00-40-F4-14-05-D8	192.168.0.158	Computadora personal
00-01-02-C1-1026	192.168.0.159	Computadora personal
00-E0-7DA7B461	192.168.0.160	Computadora personal
00-01-02-C1-1D-28	192.168.0.161	Computadora personal
00-16-EC-35-9F-FF	192.168.0.164	Computadora personal
00-10-4B-20-D8	192.168.0.167	Computadora personal
00-D0-093F-D3-7B	192.168.0.168	Computadora personal
00-D0-09-3F-E2-5A	192.168.0.169	Computadora personal
00-14-2A-F5-65-89	192.168.0.162	Computadora personal
00-01-02-C9-81-A4	192.168.0.163	Computadora personal

**Tabla 12.13 Direcciones IP de la sala 3**

<b>Sala 4</b>		
<b>MAC</b>	<b>Dirección IP</b>	<b>Descripción</b>
00-0B-BE-5F-E4-40	-	Switch de 24 puertos
00-13-D3-15-62-73	192.168.2.55	Computadora personal
00-13-D3-15-61-59	192.168.2.54	Computadora personal
00-13-D3-15-5E-8E	192.168.2.53	Computadora personal
00-13-D3-15-5E-A1	192.168.2.52	Computadora personal
00-13-D3-15-62-9E	192.168.2.51	Computadora personal
00-13-D3-15-60-01	192.168.2.50	Computadora personal
00-13-D3-15-62-6E	192.168.2.49	Computadora personal
00-13-D3-15-62-6D	192.168.2.48	Computadora personal
00-13-D3-15-62-77	192.168.2.43	Computadora personal
00-13-D3-15-5E-98	192.168.2.42	Computadora personal
00-13-D3-15-62-7A	192.168.2.41	Computadora personal
00-13-D3-15-5F-CB	192.168.2.40	Computadora personal
00-13-D3-15-5E-93	192.168.2.47	Computadora personal
2D-FF-FF-FF-FF-FF	192.168.1.169	Computadora personal
00-13-D3-15-61-5A	192.168.2.46	Computadora personal
00-13-D3-15-5F-F8	192.168.2.44	Computadora personal

**Tabla 12.14 Direcciones IP de la sala 4**



<b>Sala 5</b>		
<b>MAC</b>	<b>Dirección IP</b>	<b>Descripción</b>
00-0A-04-6F-0B-80	192.168.2.70	Switch de 24 puertos
00-11-09-18-7B-08	192.168.2.62	Computadora personal
00-13-D3-C1-E7-2B	192.168.2.63	Computadora personal
00-13-03-A6-A3-E5	192.168.2.69	Computadora personal
00-13-03-A6-A4-05	192.168.2.67	Computadora personal
00-13-D3-A6-A3-FF	192.168.2.68	Computadora personal
00-13-D3-C1-E6-64	192.168.2.66	Computadora personal
00-0C-76-CB-52-C5	192.168.2.58	Computadora personal
00-13-D3-C1-E5-D4	192.168.2.64	Computadora personal
00-13-20-57-3C-47	192.168.2.59	Computadora personal
00-13-D3-A6-A4-06	192.168.2.60	Computadora personal
00-13-D3-C1-E6-58	192.168.2.56	Computadora personal
00-13-D3-C1-E6-50	192.168.2.61	Computadora personal
00-13-D3-A6-A4-04	192.168.2.65	Computadora personal
00-13-D3-A6-A3-F9	192.168.1.57	Computadora personal

**Tabla 12.15 Direcciones IP de la sala 5**

<b>Sala de Redes</b>		
<b>MAC</b>	<b>Dirección IP</b>	<b>Descripción</b>
00-14-2A-EC-F2-4E	132.248.173.56	Switch de 24 puertos
00-14-2A-F5-46-1A	132.248.173.57	Computadora personal
00-14-2A-EC-F5-94	132.248.173.58	Computadora personal
00-E0-7D-D0-BB-EF	132.248.173.59	Computadora personal
00-07-E9-59-B1-65	Servidor DHCP en la red: 200.200.200.0	Computadora personal
00-08-54-DD-7A-4B		Computadora personal
00-14-2A-EC-F5-94	El servidor DHCP también proporciona direcciones IP a los Access Point	Computadora personal
00-40-F4-B2-0C-D7		Computadora personal
00-14-2A-F5-4C-1A		Computadora personal
00-14-2A-ED-6D-65		Computadora personal

**Tabla 12.16 Direcciones IP de la sala de redes**

<b>Sala de Servidores</b>		
<b>MAC</b>	<b>Dirección IP</b>	<b>Descripción</b>
00-12-A9-2E-1B-E0	-	Switch de 24 puertos
00-40-F4-CB-6C-52	132.248.173.151	Computadora personal
08-00-20-C0-CC-FE	132.248.173.146	Computadora personal
00-01-02-C1-1B-F2	132.248.173.148	Computadora personal
00-0D-87-C6-65-2E	192.168.0.151	Servidor
00-13-20-57-D6-DE	132.248.173.150	Servidor
00-10-5A-99-15-8B	132.248.173.152	Firewall
00-01-02-C1-1B-F2	132.248.173.148	Computadora personal

**Tabla 12.17 Direcciones IP de la sala de servidores**

Con el inventario de direcciones IP se da por terminado el análisis de la red del CAE504, dando paso a las propuestas del siguiente capítulo.

## **Capítulo 13**

### **Propuestas Para la Implantación De Mecanismos De Administración Para la Red Del CAE504**

---

#### **13.1 Introducción**

En este capítulo se llevarán a cabo dos propuestas para la optimización de la red del CAE504. Una explicará una reconfiguración tratando de que los gastos y cambios sean mínimos y otra buscará la normalización del cableado estructurado, así como una óptima reconfiguración. Ambas apoyándose en el análisis del capítulo 12.

Con estas nuevas configuraciones, se busca implantar los objetivos de la administración de redes, así como el uso de las metodologías expuestas en este trabajo, según las necesidades y resultados del análisis del CAE504.

Para la primer propuesta se buscará una reconfiguración, la cual sea viable de manera que se utilice al máximo lo que ya está instalado y buscando que el costo económico sea el menor posible.

Para la segunda propuesta, en donde se pretende llevar a cabo la normalización, según los estándares del cableado estructurado. Se hará obvia la búsqueda de un espacio de telecomunicaciones, la optimización del ancho de banda, lectura de tráfico o monitoreo de la red, así como la reconfiguración de la conexión de los equipos de interconexión, con la finalidad de optimizar los servicios de telecomunicaciones.

Por último se buscará en el inventario de hardware, el o los equipos necesarios para llevar a cabo la implantación de las nuevas configuraciones propuestas por este trabajo, de no encontrarse todos los recursos de hardware en dicho inventario, se listarán los equipo o tecnologías faltantes, con la finalidad de obtener un presupuesto, para llevar a cabo la adquisición de dichos equipos, con la finalidad de optimizar los servicios de telecomunicaciones de dicho centro.

### 13.2 Propuesta 1:

Reconfiguración al mínimo costo y máximo beneficio.

#### 13.2.1 Análisis de la configuración de los equipos de interconexión

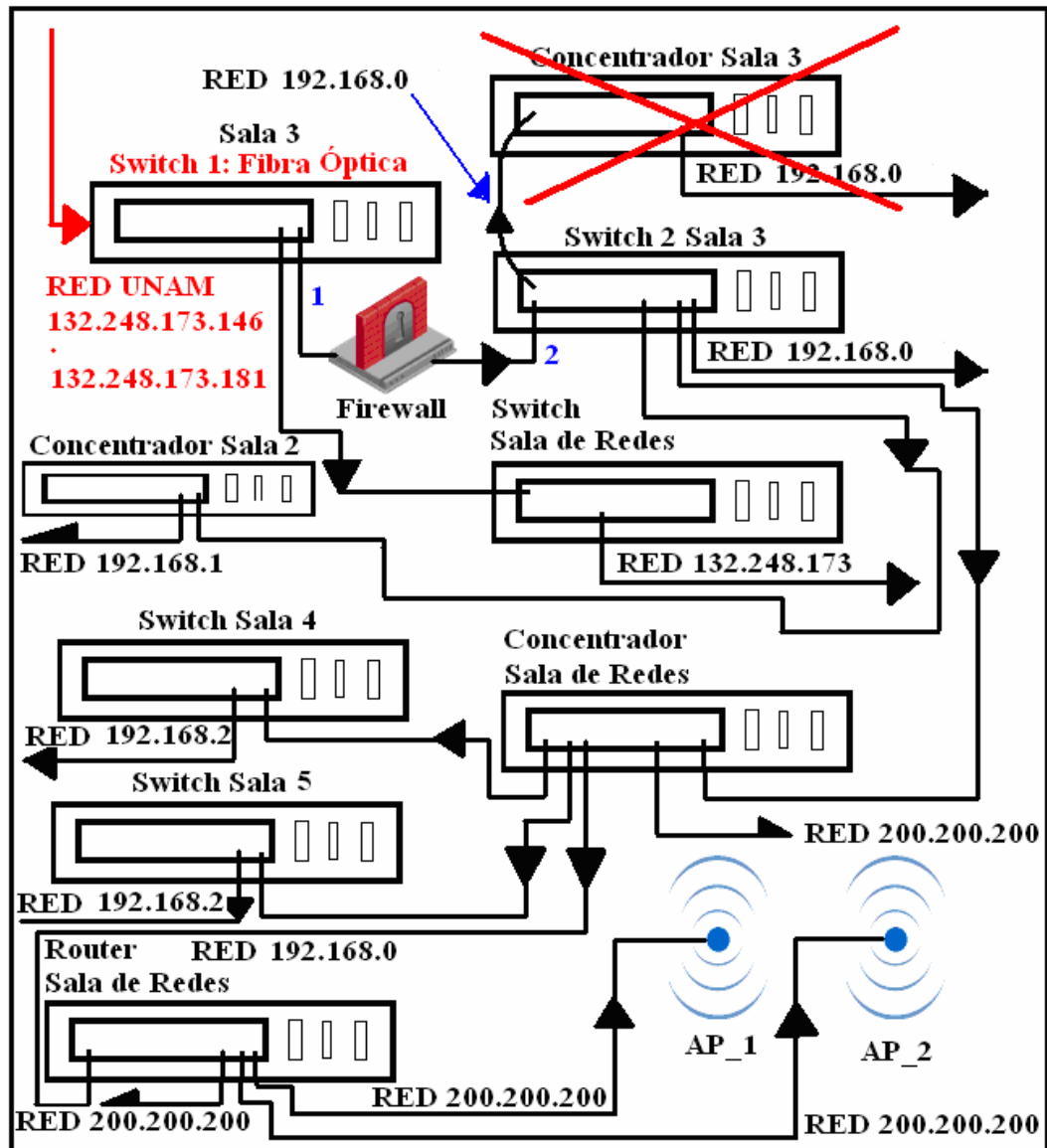


Figura 13.1 Eliminación de un concentrador en cascada

Al hacer el análisis de la configuración de conexión de los equipos de interconexión debemos buscar optimizar el ancho de banda, así como, a medida de lo posible evitar la configuración en cascada de equipos de interconexión.

En la figura 13.1 se observa tachado el concentrador de la sala 3, debido a que se encuentra conectado en cascada con el *Switch* 2 de la sala 3 y según nuestro inventario de hardware, el *Switch* 2 de la sala 3 dispone de 24 puertos los cuales son suficientes para dar servicio de telecomunicaciones a las 16 estaciones de trabajo de dicha sala. De esta forma nos queda una nueva configuración como lo muestra la figura 13.2.

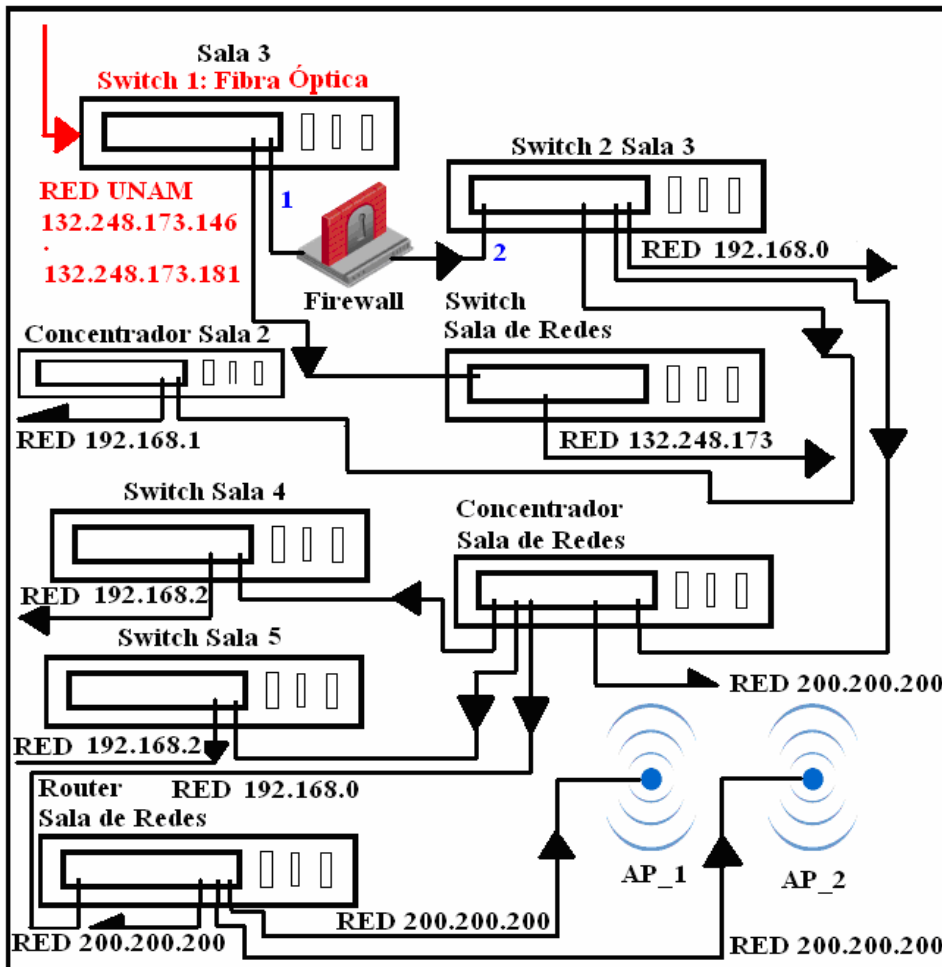


Figura 13.2 Nueva configuración del CAE504

Del mismo modo se observa al concentrador de la sala de redes que se encuentra conectado en cascada con el *Switch* 2 de la sala 3 y este a su vez suministra

servicios de telecomunicaciones al *Switch* de la sala 4 y al *Switch* de la sala 5 nuevamente en cascada y a su vez proporciona de estos servicios a un *Router* que da entrada a los *Access Point* de la red inalámbrica del CAE504. Como se puede observar en la figura 13.3, esta es una configuración muy poco recomendable. Es por ello que en aras de aumentar la velocidad de transferencia se recomienda prescindir de él.

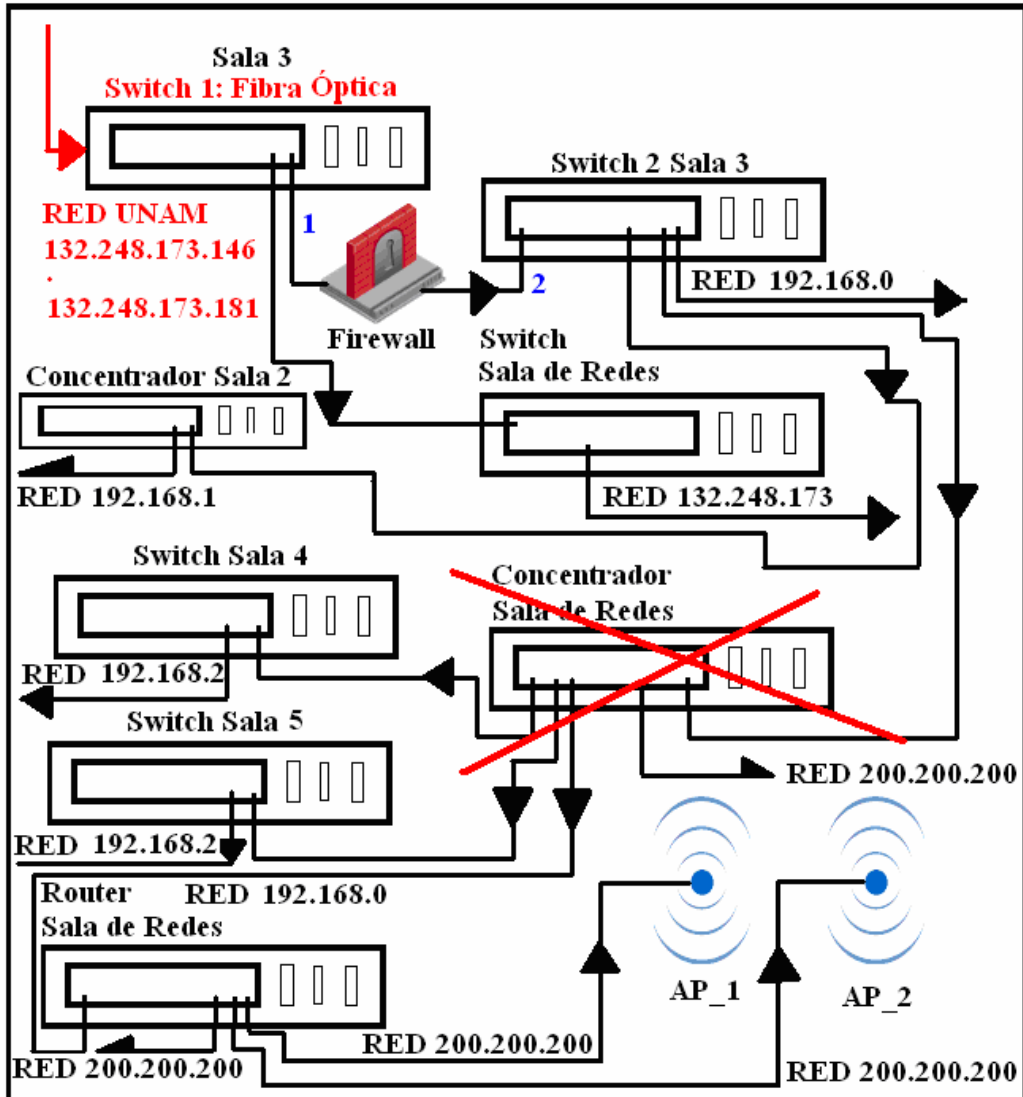


Figura 13.3 El concentrador no es eficiente en esa posición

La figura 13.4 muestra la nueva configuración, la cual pareciera dejar sin conexión a la sala 4 y a la sala 5 y con ello también sin acceso a la red inalámbrica del CAE504, no obstante al final del análisis se verá que no es así.

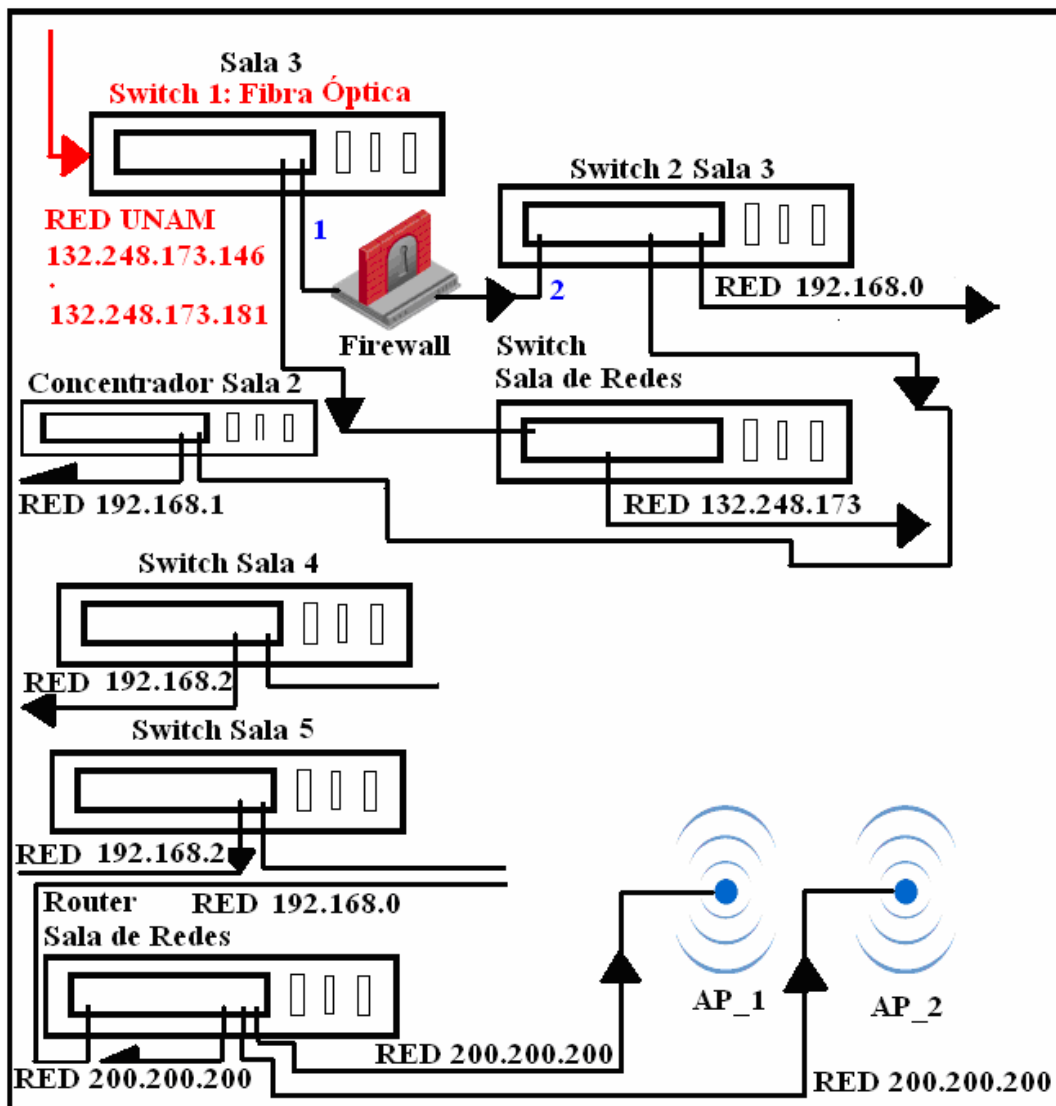


Figura 13.4 Concentrador de la sala de redes eliminado

Como se puede apreciar en la figura 13.4 en la sala 2 tenemos como distribuidor de los servicios de telecomunicaciones a un concentrador, el cual no sería un gran problema si no se estuviera buscando llevar a la red del CAE504 a un estado más

optimo. Es por ello que se recomienda que sea cambiado por un *Switch* debido al siguiente análisis:

Se sabe que un concentrador de N puertos distribuye su tasa de transferencia de manera ideal de la siguiente manera:

$$T_{tp} = \frac{\text{Taza de transferencia}}{\text{Número de puertos}}$$

Donde  $T_{tp}$  equivale a la tasa de transferencia por puerto.

Es por esto que si tenemos un concentrador de 12 puertos y una tasa de transferencia de 150 *Kbps* (kilo bits por segundo) nos dará el rendimiento mostrado en la figura 13.5.

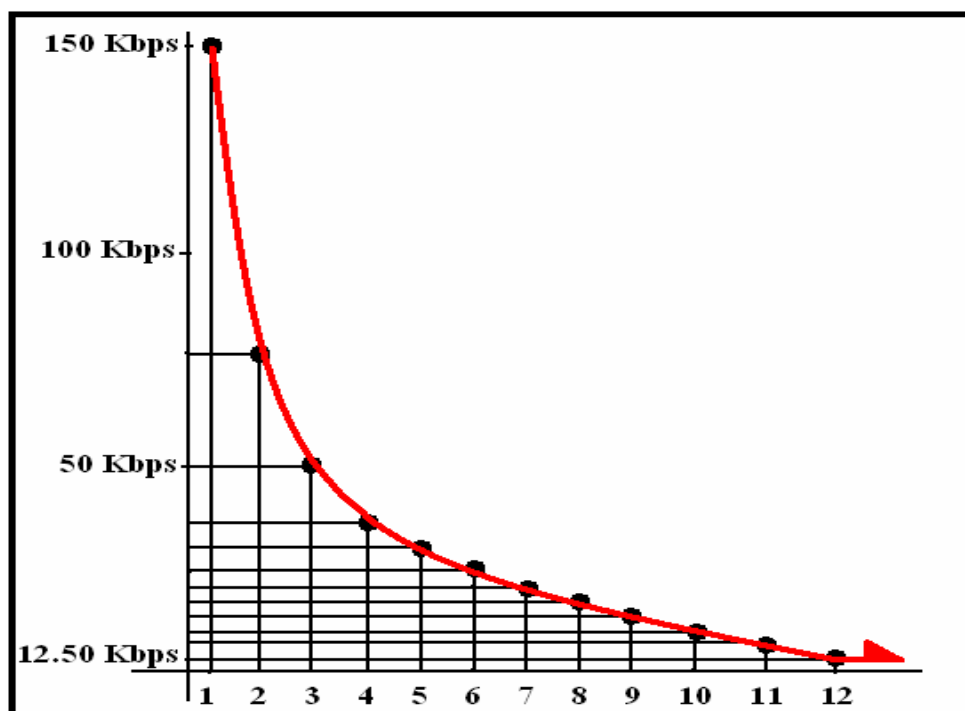


Figura 13.5 Rendimiento del concentrador de 12 puertos

En la figura 12.5, se puede ver que si un sólo equipo desea transmitir, utilizará todo el ancho de banda disponible. Por ello de la gráfica se deduce que si dos equipos desean transmitir al mismo tiempo, el ancho de banda será dividido para este caso entre dos y así sucesivamente. El ancho de banda será dividido entre el



número de equipos que transmitan al mismo tiempo, liberándose éste, después de que un determinado equipo termina de transmitir.

Los valores que adopta cada puerto en donde es conectada una estación de trabajo, se muestran en la tabla 13.1.

Es de destacarse, que estos valores son ideales, es decir, suponiendo que no hubiese colisiones, ya que con la ocurrencia de colisiones, la eficiencia disminuye aún más cuando el número de equipos a transmitir en un tiempo  $t$  aumenta.

<b>Puerto</b>	<b>Taza de transferencia</b>	<b>T<sub>tp</sub></b>
1	150 Kbps	150.00 Kbps
2	150 Kbps	75.00 Kbps
3	150 Kbps	50.00 Kbps
4	150 Kbps	37.50 Kbps
5	150 Kbps	30.00 Kbps
6	150 Kbps	25.00 Kbps
7	150 Kbps	21.40 Kbps
8	150 Kbps	18.75 Kbps
9	150 Kbps	16.67 Kbps
10	150 Kbps	15.00 Kbps
11	150 Kbps	13.63 Kbps
12	150 Kbps	12.50 Kbps

**Tabla 13.1 Taza de transferencia por puerto del concentrador**

Al cambiar este dispositivo por un *Switch*, la tasa de transferencia se vera muy beneficiada debido a que la tasa de transferencia de un *Switch* no se divide como lo hace con el concentrador al aumentar el número de equipos conectados a éste, es decir, el *Switch* nos garantiza un ancho de banda entre la estación de trabajo y el *Switch*, por ejemplo, el cable UTP categoría 5E permite una velocidad de transferencia de hasta 100 Mbps, sí la tarjeta de red también lo permite. Esta velocidad se garantiza por estación de trabajo, siempre y cuando la transmisión sea entre equipos que se encuentren conectados al mismo *Switch*.

La figura 13.6 ilustra el rendimiento del *Switch*.

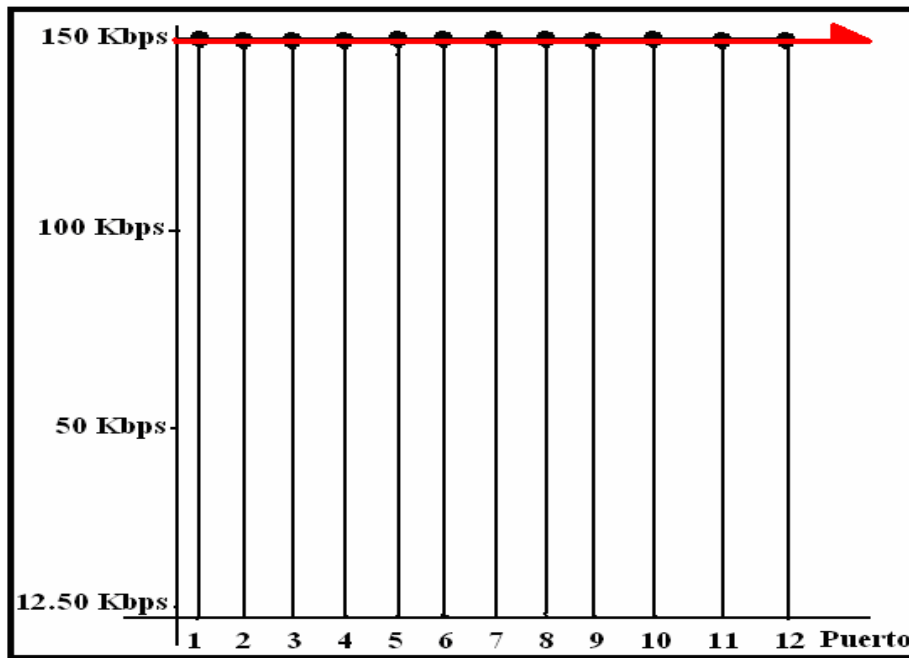


Figura 13.6 Rendimiento de un Switch en diferentes tiempos

Se debe destacar que este rendimiento mostrado en la figura 13.6, se obtiene siempre y cuando los equipos sólo transmitan información en un tiempo  $t$  a equipos conectados al Switch en cuestión, como lo muestra la figura 13.7.

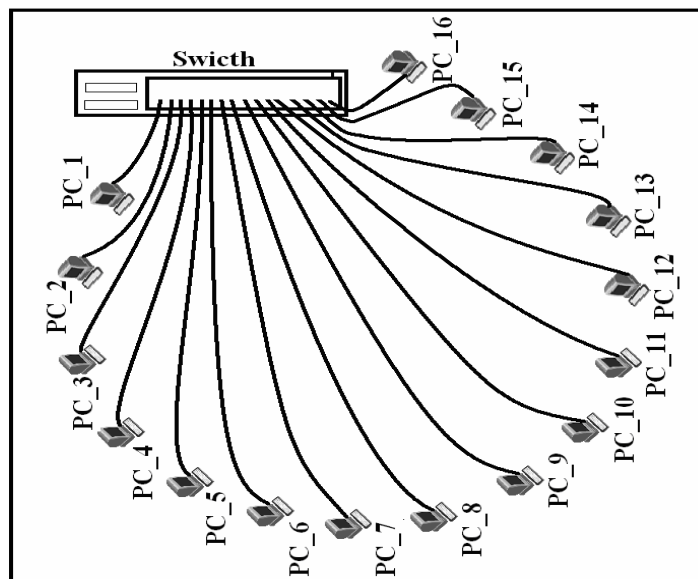


Figura 13.7 Switch interactuando con estaciones de trabajo

De esta forma se garantiza una velocidad de transferencia constante, entre cada equipo interconectado al Switch. No obstante, sí se tiene la necesidad de transmitir información a algún equipo que no esté conectado a este Switch, entonces el medio por el cual se llevan los servicios de telecomunicaciones fuera del ámbito del Switch de la figura 13.8, se convertirá en un cuello de botella disminuyendo la velocidad de transferencia sólo en el medio que lleva los servicios de telecomunicaciones fuera del ámbito del Switch en cuestión, de esto se entiende que la velocidad de transferencia entre equipos conectados al mismo Switch sigue siendo la misma según las características de hardware asociadas a estos equipos.

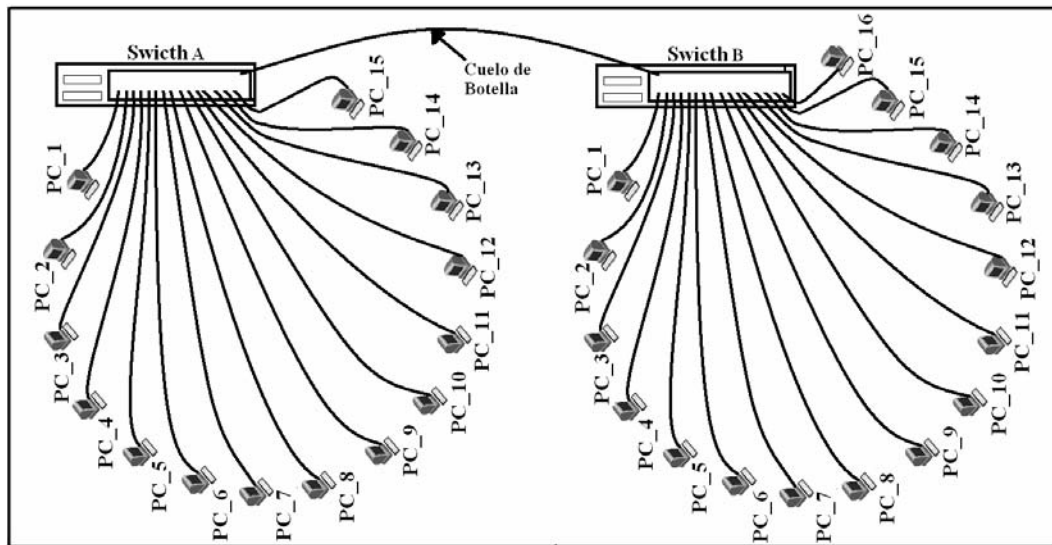


Figura 13.8 Cuello de botella

Una vez entendidas las ventajas de cambiar el concentrador de la sala 2 por un *Switch*; también se necesitará desconectar este dispositivo del *Switch 2* de la sala 3 con la finalidad de evitar la conexión en cascada tal como lo muestra la figura 13.9.

De esta forma se han eliminado casi todas las conexiones en cascada a excepción de la conexión del *Router* con los *Access Point*, y el *Switch* de la sala de redes con el *Switch 1* de la sala 3.

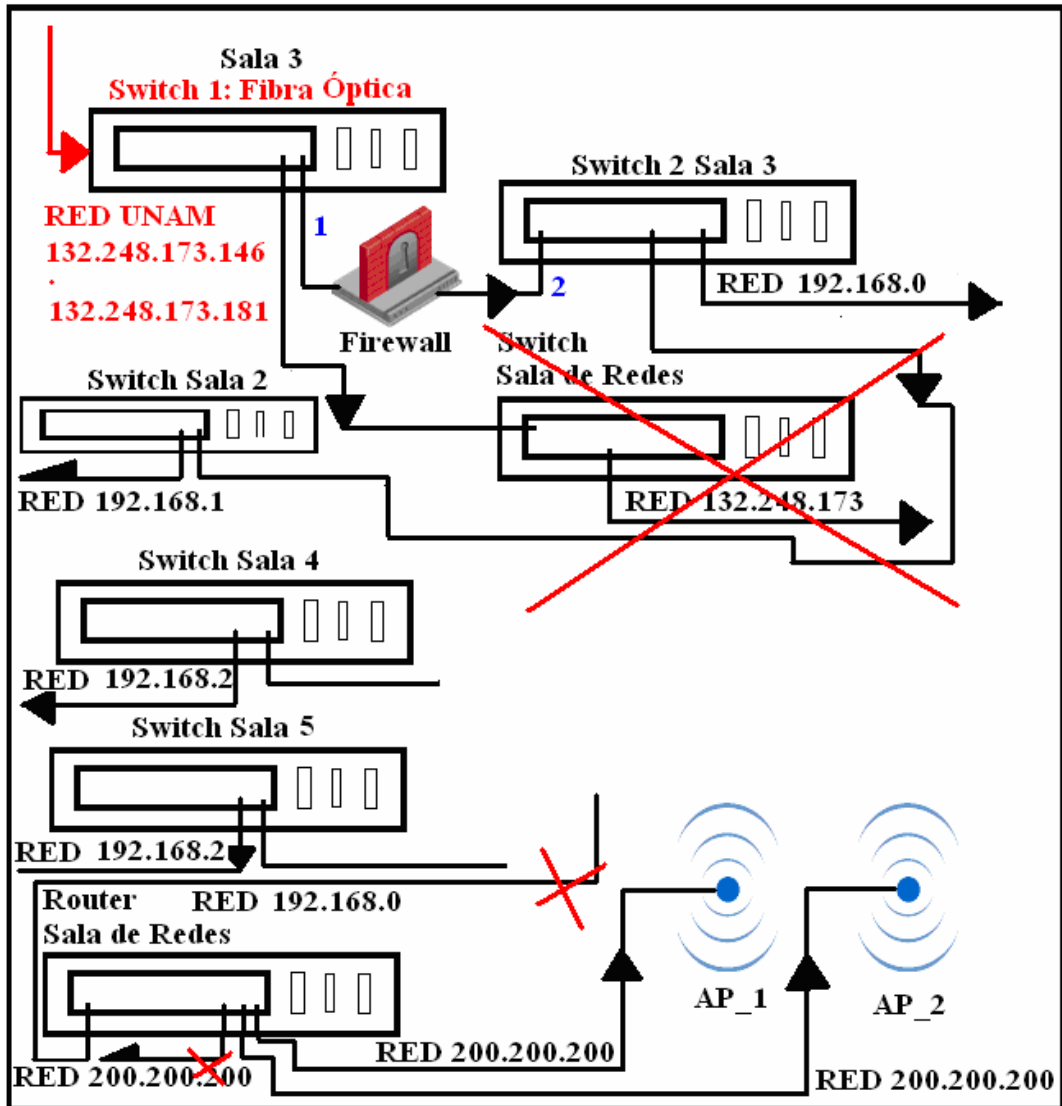


Figura 13.9 Eliminando las cascadas de la configuración

En este momento se hace necesario explicar la forma de eliminar las dos conexiones en cascada restantes.

La justificación para eliminar el *Switch* de la sala de redes consiste en que en el *Switch* de la sala 3 no es administrable y la cantidad de puertos que posee no es suficiente para dar los servicios de telecomunicaciones a los equipos dispuestos en esta sala.

Por otra parte, el *Router* puede seguirse utilizando ahora sólo como servidor *DHCP* y como puerta de enlace, pues los equipos conectados a los *Access Point*, necesitarán de éste para hacerse de una dirección IP, así como de una puerta de enlace.

Entendido lo anterior, el diagrama restante de la configuración de los dispositivos de interconexión queda en un arreglo mostrado por la figura 13.10.

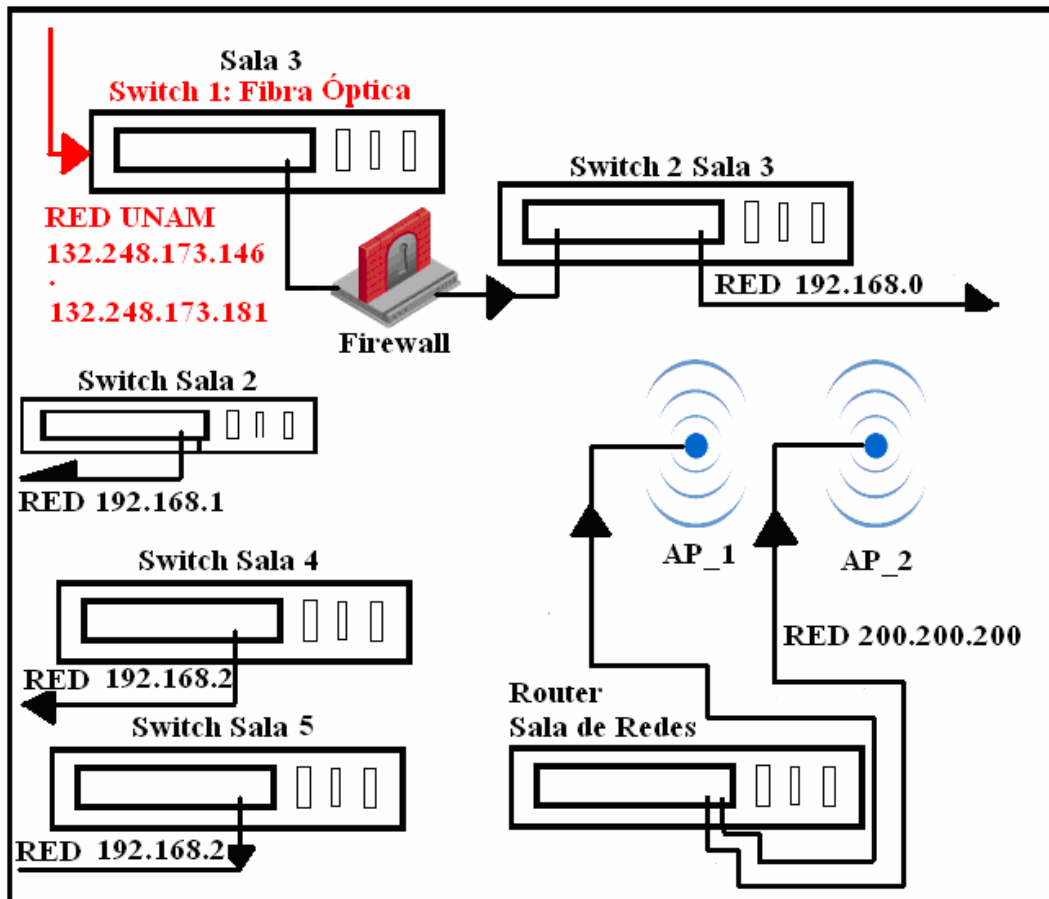


Figura 13.10 Configuración sin cascadas

Se puede observar que el *Switch 1* de la sala 3 está aún conectado en cascada con el *Switch 2* de la sala 3, pero en este caso, debido a que el *Switch 1* de la sala 3 recibe los servicios de telecomunicaciones en su parte posterior utilizando una tarjeta con conectores de fibra óptica. En esta misma figura se observa que el *Firewall* hace como intermediario y es el encargado de la seguridad de la red.

Al eliminar esta relación entre el *Firewall* y el Switch 1 de la sala 3 se hace imprescindible otra estrategia de conexión.

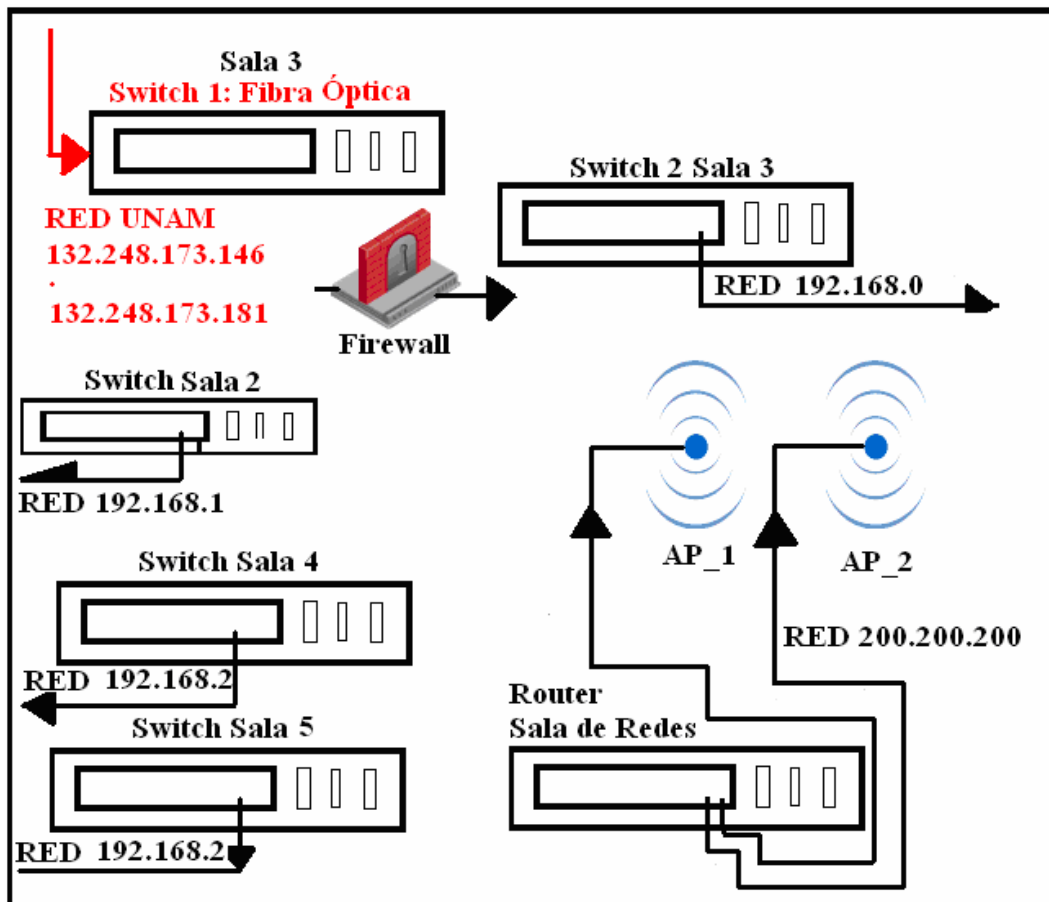


Figura 13.11 Cascadas eliminadas

La figura 13.11 parece que deja sin servicios de telecomunicaciones al CAE504, pero se tiene que recordar que es parte del análisis.

En la figura 13.12 se muestra la propuesta de cómo conectar los equipos de interconexión, de tal forma que se mejoran en gran medida los servicios de telecomunicaciones a un costo muy bajo, ya que para llevar a cabo esta propuesta bastaría sólo con recablear las conexiones entre los equipos de interconexión y prescindir de un concentrador, así como, llevar a cabo el cambio de un concentrador por un Switch. Lo cual es factible ya que el CAE504 cuenta con todo lo necesario en su inventario de hardware, para llevar a cabo esta propuesta.

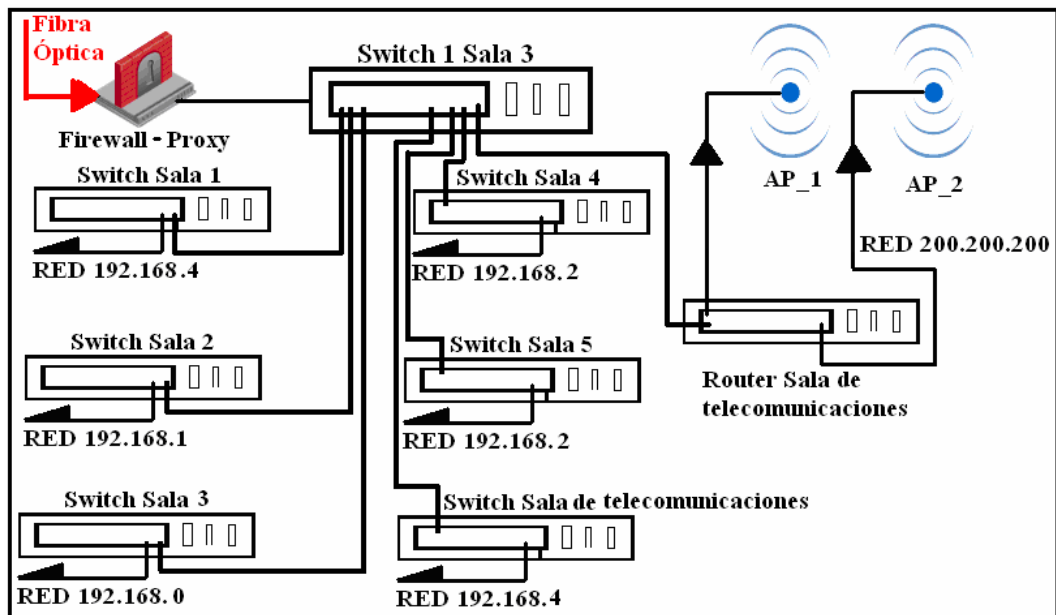


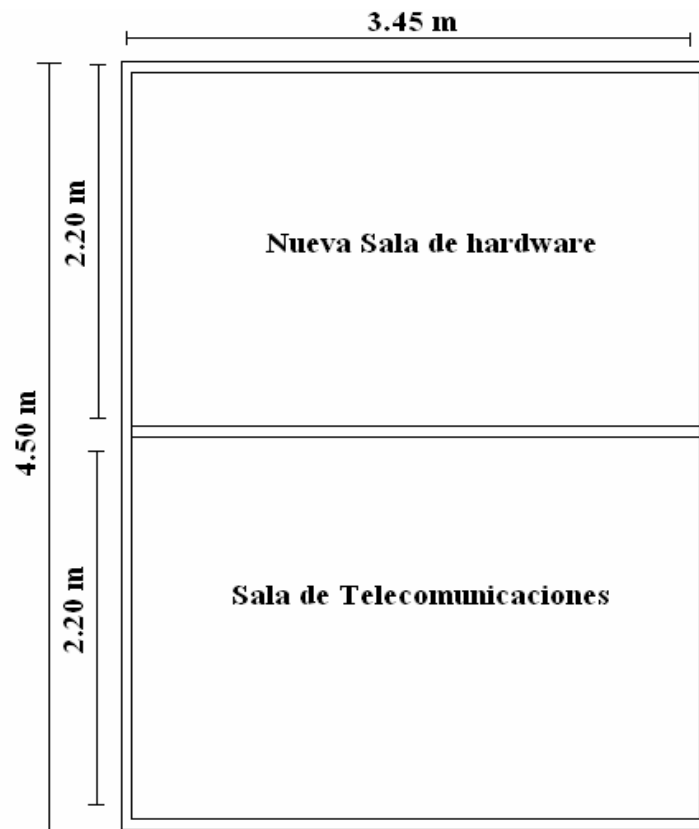
Figura 13.12. Nueva configuración de equipos de interconexión del CAE504

Como se puede observar en la figura 13.12. El impacto de implantar esta propuesta es mínimo, no obstante esta propuesta no es la óptima. Es por ello que en la siguiente sección se tratará una propuesta óptima para la red del CAE504. No obstante el costo de implantación es mucho más elevado que para la propuesta anterior, así como el impacto en el funcionamiento del CAE504 a tal grado que se tendría que suspender las actividades por un lapso de tiempo mientras se implanta la propuesta descrita en la siguiente sección.

### **13.3 Propuesta 2: Implantación óptima para la red del CAE504, siguiendo los lineamientos del cableado estructurado.**

#### **13.3.1 Redistribución del CAE504**

Para implantar el modelo de administración de redes sugerido en este trabajo, es importante redistribuir el CAE504 para diseñar una sala de telecomunicaciones. Se sugiere que se rediseñe la sala de hardware como lo muestra la figura 13.13



**Figura 13.13 Redistribución de la sala de hardware**

En la figura 13.13 se muestra como redistribuir la sala de hardware para obtener dos pequeñas salas: una de hardware y otra de telecomunicaciones.

Se seleccionó la sala de hardware para ser redistribuida por diversas causas, entre las importantes destacan:



- Tiene una posición estratégica respecto a las demás salas (Su ubicación es céntrica).
- Al dividirla por la mitad, las dimensiones obtenidas son suficientes para adecuar una sala de telecomunicaciones, sin sacrificar la sala de hardware (aunque de tamaño menor).
- La sala de hardware tiene menos demanda que las otras salas.
- Etc.

### 13.3.2 Adopción de los estándares del cableado estructurado

Una vez que se puede contar con una necesaria sala de telecomunicaciones se pueden adoptar los estándares del cableado estructurado. La introducción de estos estándares fue tratada en el capítulo 9.

La primera recomendación según estos estándares que debe hacerse, es la concentración de todos los equipos de interconexión, ya sean concentradores *Switches*, *Routers*, *Access Point*, etc. en la sala de telecomunicaciones dispuestos cada uno de ellos en un armario (*Rack* en inglés). La figura 13.14 muestra los elementos constitutivos de un *Rack* y la figura 13.15 muestra como los dispositivos de interconexión se colocan en un *Rack* determinado.

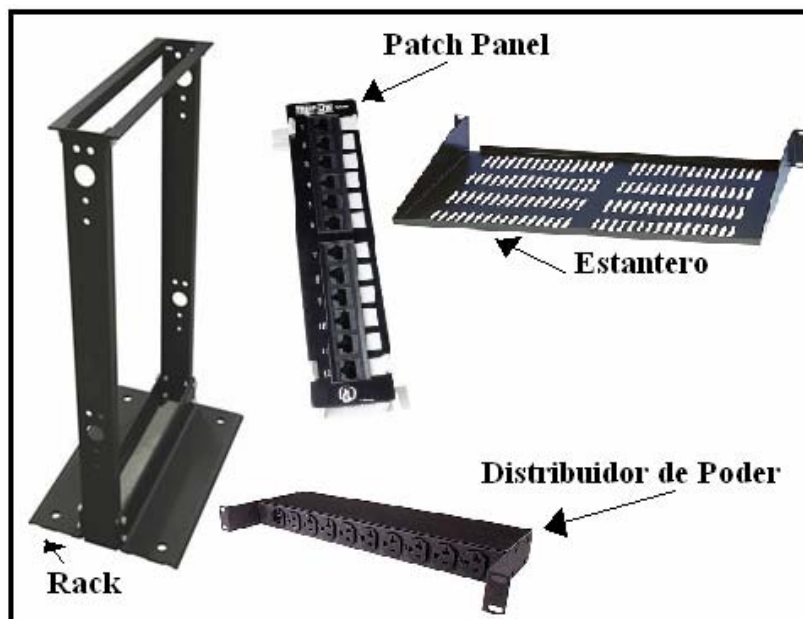


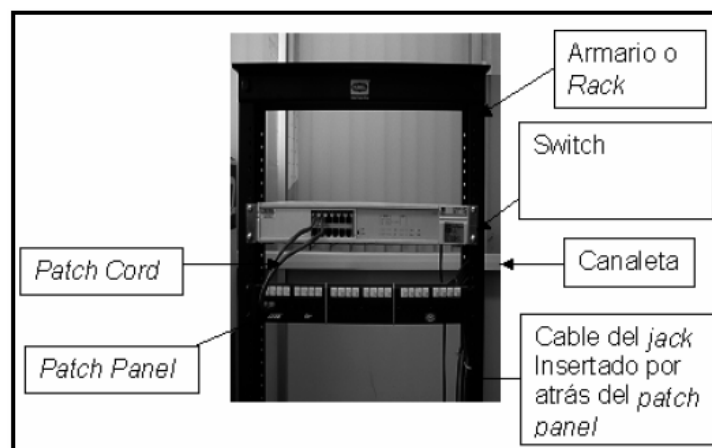
Figura 13.14 Componentes básicos de un armario o Rack



**Figura 13.15 Lado posterior de un Armario**

La segunda recomendación va dirigida a la adopción del cableado horizontal. Ya que el CAE504 es una entidad de un solo nivel, su cableado vertical será muy discreto.

Para llevar a cabo el tendido del cableado horizontal, se pueden aprovechar las canalizaciones ya instaladas previamente, no obstante todo el cableado tendrá que ser removido debido a su longitud, pues cada RJ – 45 hembra instalado debe estar directamente conectado al *patch panel* del armario, ubicado de acuerdo al estándar en la sala de telecomunicaciones.



**Figura 13.16 Dispositivos de red montados en un Armario**

Después de haber tendido el cableado correspondiente a la norma ANSI/EIA/TIA 568 B, la cual se recomienda más que la ANSI/EIA/TIA 568 A, debido a que es la

más utilizada. Es de suma importancia analizar la configuración ó forma de conexión de los equipos de interconexión.

Se tiene que recordar que existen 5 salas de computadoras, más la sala de redes y la sala de hardware, sin olvidar las oficinas y la sala de servidores.

La recomendación para el mejoramiento del ancho de banda consiste en un apilado de *Switches*, el cual consta en colocar a los *Swicthes* que se vayan a apilar en un *Rack* y conectarlos por su parte posterior con tarjetas y cables especiales para hacerlos funcionar como un sólo *Switch*. En este caso se requiere de 4 *Switches* 3COM de 24 puertos cada uno, para obtener una capacidad de 96 puertos disponibles. Tomando en cuenta que en el inventario de hardware se registró el número de 73 estaciones de trabajo. Estos 4 *Switches* serán suficientes para dotar de servicios de telecomunicaciones a todo el CAE504 y soportar un crecimiento de hasta 16% sin necesidad de apilar otro *Switch*.

Para llevar a cabo el apilamiento, cada uno de estos *Switches* será dotado con dos tarjetas de apilamiento: una tarjeta será para apilar hacia arriba y otra para apilar hacia abajo (UP, DOWN) y un cable que llevará a cabo la interconexión.

Este apilamiento traerá como consecuencia la unión de los cuatro *Switches* como si fueran uno solo, es decir, a diferencia de la configuración por cascada que divide en el caso de los *Switches* de manera arbitraria el ancho de banda, el apilamiento hace funcionar a los *Switches* como una sola entidad. Es por esto que cualquier puerto del apilado tendrá la misma jerarquía eliminándose con esto divisiones innecesarias del ancho de banda.

La figura 13.17 muestra como quedaría el apilado del *Switch* 3COM serie 4400, por la parte frontal y posterior.

El apilamiento mostrado en la figura 13.17 se encargará de suministrar todos y cada uno de los servicios de telecomunicaciones a cualquiera de las estaciones de trabajo que así lo soliciten. Pero aún falta la parte de cómo hacer llegar todos los servicios de telecomunicaciones al apilamiento. Para llevar a cabo esta tarea de manera óptima es importante dotar al *Switch* 1 del apilamiento con una tarjeta, la cual cuente con conectores para fibra óptica. De igual manera se debe de dotar a la estación en la cual se está ejecutando el *firewall* con dos tarjetas que integren en su estructura conectores de fibra óptica, con la finalidad de que el ancho de banda no sea disminuido por ninguna entidad intermedia entre el apilado y la fibra óptica entrante al *Switch* 1.

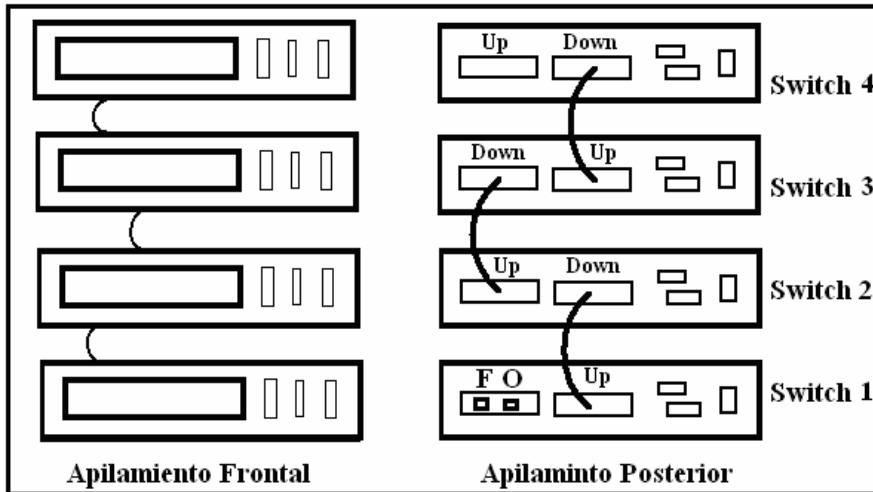


Figura 13.17 Apilamiento del Switch 3COM 4400

La figura 13.18 ilustra esta configuración, donde el *Switch 1* recibe los servicios de telecomunicaciones del *backbone* de la UNAM a través de una tarjeta con conectores de fibra óptica, la cual se encuentra en el lado posterior a este *Switch*. En esta misma figura se puede observar cómo el *firewall* es conectado en la parte posterior del *Switch 1*, justo en la tarjeta de conexión de fibra óptica. El *firewall* filtrará los servicios de Internet no permitidos por las políticas del CAE504. El *firewall* es responsable también de suministrar todos los servicios de telecomunicaciones y es por ello que éste será conectado al apilamiento en el *Switch 1* en su tarjeta de fibra óptica para un óptimo ancho de banda.

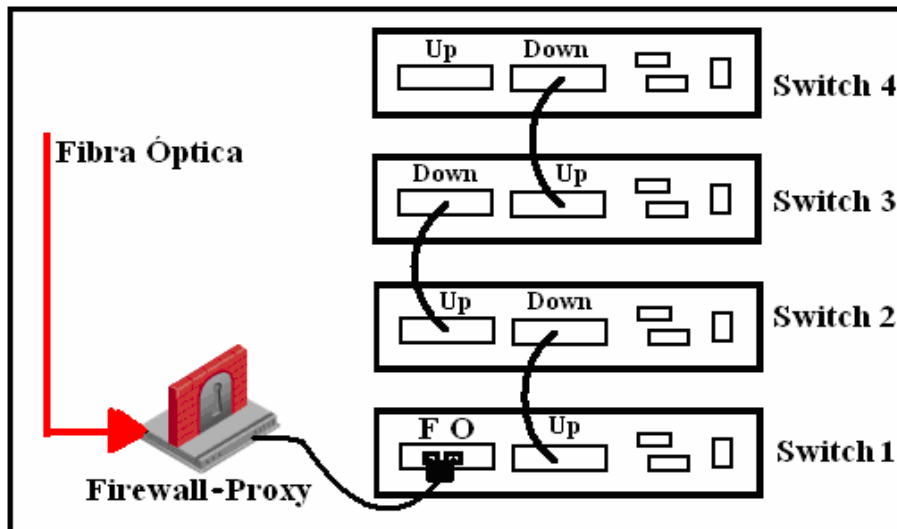


Figura 13.18 Interconexión del Firewall con el apilado

La última recomendación en cuanto a la configuración de la conexión de los equipos de interconexión sería para la red inalámbrica del CAE504. Debido a que la red inalámbrica del CAE504 tiene una afluencia reducida de usuarios en comparación con la red alámbrica del mismo centro. Se recomienda conectar en cascada el *Router* RTM, en el primer puerto del apilado de los 96 puertos disponibles, cada *Access Point* irá conectado a uno de los puertos del *Router*.

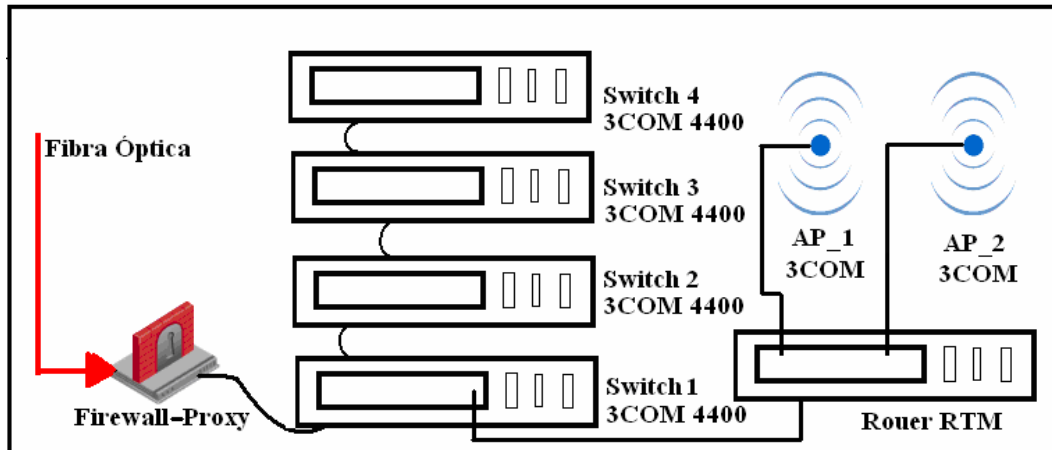


Figura 13.19 Configuración final del CAE504

De tal forma que la configuración de la conexión de los equipos de interconexión quedaría como lo muestra la figura 13.19.

En la figura 13.19 se puede apreciar la conexión de los *Access Point* conectados al *Router* MTR, y éste a su vez conectado al primer puerto de los 96 puertos del apilado. Esto implica que el *Router* estará en contienda con los equipos conectados al apilado por el ancho de banda. Por otra parte los equipos conectados a los *Access Point* podrán hacer uso del ancho de banda disponible, sin entrar en contienda con los equipos conectados al apilado, siempre y cuando la transferencia de archivos se lleve a cabo de equipo inalámbrico a equipo inalámbrico, pues de otra forma si algún equipo inalámbrico desea transmitir algún archivo a un equipo de la red alámbrica entonces hará uso del *Router*, donde éste entrará en contienda por el ancho de banda dentro del apilado.

### 13.3.3 Direccionamiento IP recomendado

La figura 13.20 muestra las direcciones IP de la red empleadas en el CAE504.

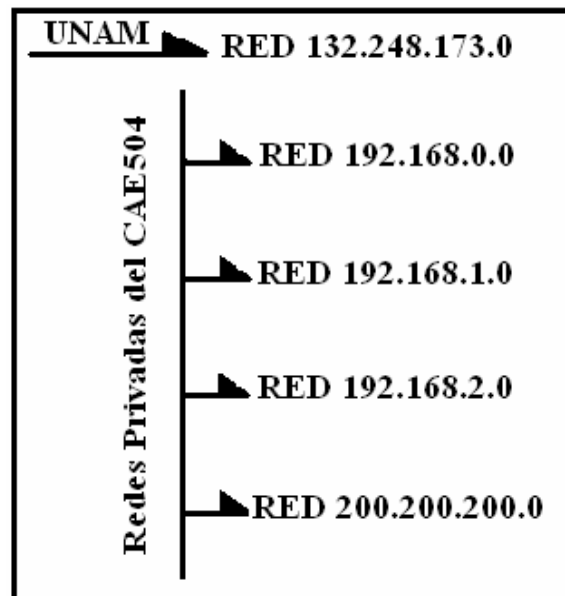


Figura 13.20 Redes del CAE504

El esquema de la figura 13.20 es un subproducto del inventario de direcciones IP, levantado en el capítulo 12. En este esquema se pueden observar las direcciones pertenecientes a las redes privadas del CAE504. Algunas de estas direcciones podrían servir para la nueva configuración propuesta en este trabajo de tesis, sin embargo, se recomienda reducir el número de redes con la finalidad de tener una administración de direcciones IP más ágil y reducida.

La recomendación de cómo poder llevar a cabo el direccionamiento de las IP, de acuerdo a la nueva configuración de la conexión de los equipos de interconexión que nos dio el apilado mostrado en la figura 13.19, en común acuerdo con el inventario de hardware realizado en el capítulo 12, otorga las bases para hacer la sugestión del direccionamiento IP mostrado en la figura 13.21. El cual ilustra una forma eficiente de llevar a cabo esta tarea.

RED UNAM 132.248.173.0	Distribución	Rango IP	
Firewall RED 192.0.0.0	Sala 1	192.0.0.1 a 192.0.0.12	
	Sala 2	192.0.0.13 a 192.0.0.24	
	Sala 3	192.0.0.25 a 192.0.0.39	
	Sala 4	192.0.0.40 a 192.0.0.55	
	Sala 5	192.0.0.56 a 192.0.0.70	
	Sala de redes	192.0.0.71 a 192.0.0.81	
	Sala de servidores	192.0.0.82 a 192.0.0.88	
	Oficina	192.0.0.89 a 192.0.0.91	
	Coordinación	192.0.0.92 a 192.0.0.94	
	Sala de hardware	192.0.0.95 a 192.0.0.97	
	Sala de telecomunicaciones	Reservadas para uso futuro	
	RED 192.0.1.0	Access Point 1	192.0.1.1 a 192.0.1.250
		Sala de telecomunicaciones	Reservadas para uso futuro
RED 192.0.2.0	Access Point 2	192.0.2.1 a 192.0.2.250	
	Sala de telecomunicaciones	Reservadas para uso futuro	

Figura 13.21 Direccionamiento IP recomendado

Como se puede observar en la figura 13.21, el conjunto de direcciones de red privadas se redujo a sólo 3; mientras que el conjunto actual está formado por 4 direcciones de red (sin considerar las direcciones IP de la red del *backbone* de la UNAM).

También se puede observar en la figura 13.21, que las direcciones IP fueron asignadas de manera consecutiva, sobre el apilado, por otro lado, debido a que el número de puertos (96) es inferior al máximo de direcciones IP asignables (254), las direcciones IP no utilizadas, son guardadas en una bitácora para su uso futuro en la sala de telecomunicaciones, donde estarán a la mano del administrador de red, para la asignación de algún nuevo punto que se requiera en la red.

En cuanto a las redes privadas tenemos el caso de la red 192.0.0.0, La dirección de red es precisamente 192.0.0.0 y la dirección de *broadcast* será 192.0.0.255, de igual forma para la consecuente, la dirección de red será 192.0.1.0 y la dirección de *broadcast* y la última dirección de red sería 192.0.2.0 y su dirección de *broadcast* sería 192.0.2.255.

Para el caso de las direcciones de red de la UNAM, el rango va de la 132.248.173.146 hasta la 132.248.173.181. Debido a que estas direcciones son externas no sufren ninguna modificación.

### 13.4 Comparación de la eficiencia de la configuración actual del CAE504 con la propuesta de tesis

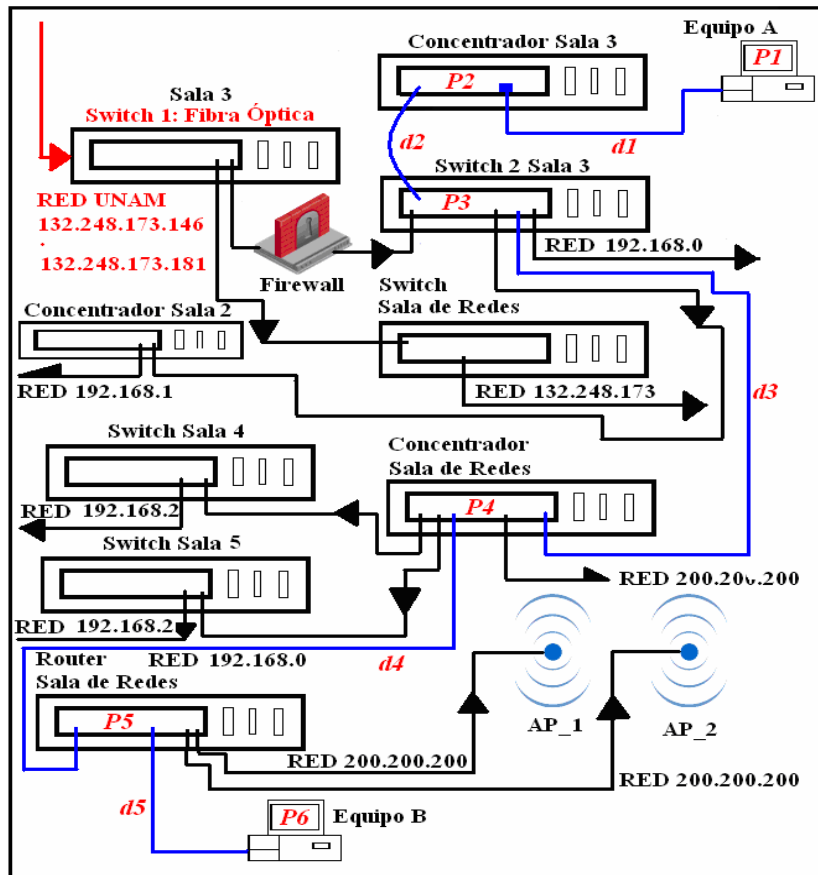


Figura 13.22 Distancias y procesos del paquete en la red actual

Para llevar a cabo la comparación del rendimiento de cada configuración es necesario analizar distancias recorridas por un paquete, así como, el tiempo que tarda cada equipo en procesar a dicho paquete. Por ejemplo. Supóngase que el equipo **A** recibe un comando para transferir un paquete a un equipo **B** como se muestra en la figura 13.22.



Para que el paquete sea enviado a un destino primero debe de someterse a un proceso uno ' $P1$ ' en el equipo fuente, posteriormente recorrerá la distancia uno ' $d1$ ', hasta llegar al proceso dos ' $P2$ ', una vez terminado dicho proceso, tendrá que recorrer la distancia dos ' $d2$ ', hasta llegar al proceso tres ' $P3$ ' y así sucesivamente como lo muestra la figura 13.22. El viaje del paquete termina cuando llega al equipo  $B$  y éste lo procesa.

Como se puede apreciar en la figura 13.22, el paquete fue sometido a seis procesos  $P$  y recorrió cinco distancias  $d$ .

Algo que se debe tener en cuenta es que el ancho de banda varía conforme el paquete cruza por cada cascada y a esto hay que agregar la división del ancho de banda que hacen los concentradores, sin olvidar la contienda que sostienen los *Switches* en cada uno de sus puertos con el poco ancho de banda que les llega por la conexión en cascada.

Para demostrar que la eficiencia mejora de manera considerable con la implantación de la configuración del apilado de *Switches*. Se tomará el ejemplo anterior sobre el apilado de los *Switches* para verificar el rendimiento de dicha configuración, como lo muestra la figura 13.23.

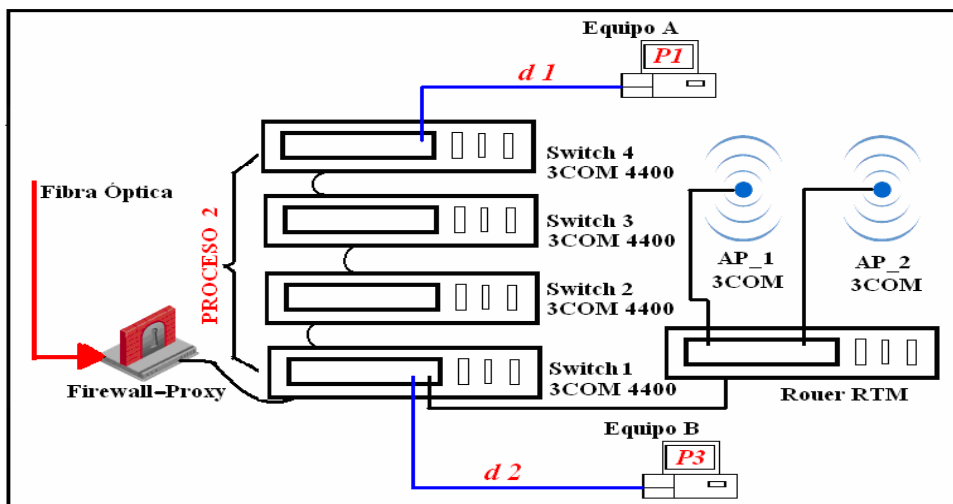


Figura 13.23 Distancias y procesos del paquete en el apilado de la propuesta.

El paquete a enviar comienza su travesía en el equipo  $A$  donde es sometido a un proceso uno ' $P1$ ' y posteriormente recorre una distancia ' $d1$ ' para llegar al apilado de *Switches*, en donde es llevado a cabo un proceso dos, para después ser depositado en un cable donde recorrerá la distancia dos ' $d2$ ' para llegar a su

destino, el equipo **B**, éste lo procesa con un proceso tres '**P3**' poniendo fin, así a la recepción del mensaje.

Adviértase que el apilado de *Switches* asume el comportamiento de un sólo *Switch* y es por esta razón que le procesado en el apilado cuenta como un solo proceso. La división del ancho de banda por parte de concentradores es nula, debido a que se prescindió de ellos. El nivel jerárquico del los *Switches* en el apilado es el mismo y es por esto, que la contienda por el ancho de banda de cada puerto es mucho más equilibrada que en una configuración en cascada y a esto hay que agregarle la ventaja administrativa de una sola dirección IP, para administrar el apilado, en lugar de una dirección IP por *Switch*.

### 13.5 Implantación del agente SNMP y su monitoreo

El apilamiento de los *Switches* los hace funcionar como uno sólo, esto puede traer ciertas ventajas como: La utilización de una sola dirección IP en lugar de cuatro, y el monitoreo de un sólo agente en lugar de cuatro.

Para dar de alta un agente en un *Switch* 3COM serie 4400 se tiene que hacer lo siguiente:

Conectar un extremo del cable MODEM nulo al puerto serial DB-9 del *Switch* y el otro extremo al mismo puerto en una estación de trabajo.

Al ejecutar la acción anterior se requiere establecer una conexión entre el *Switch* y la estación de trabajo.

Una vez establecida dicha conexión aparecerá una pantalla como la de la figura 13.24.

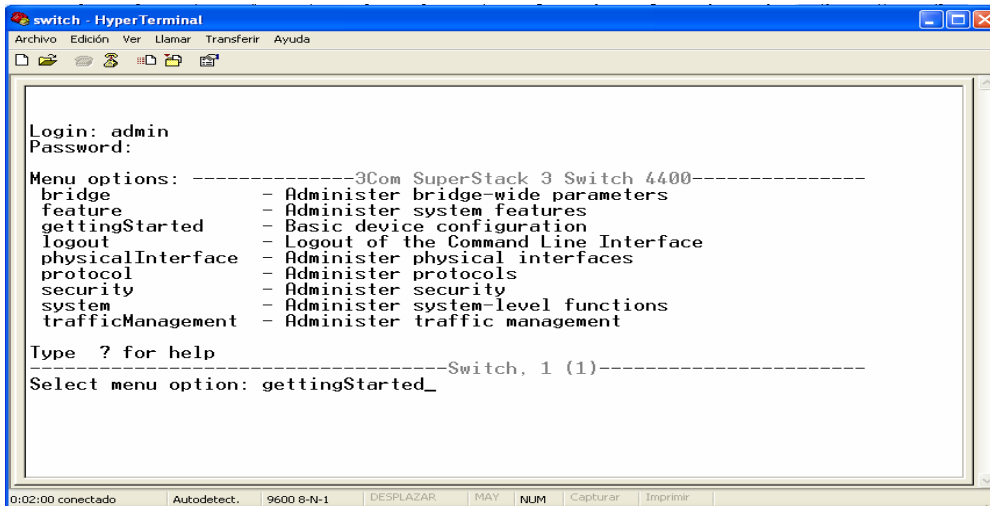
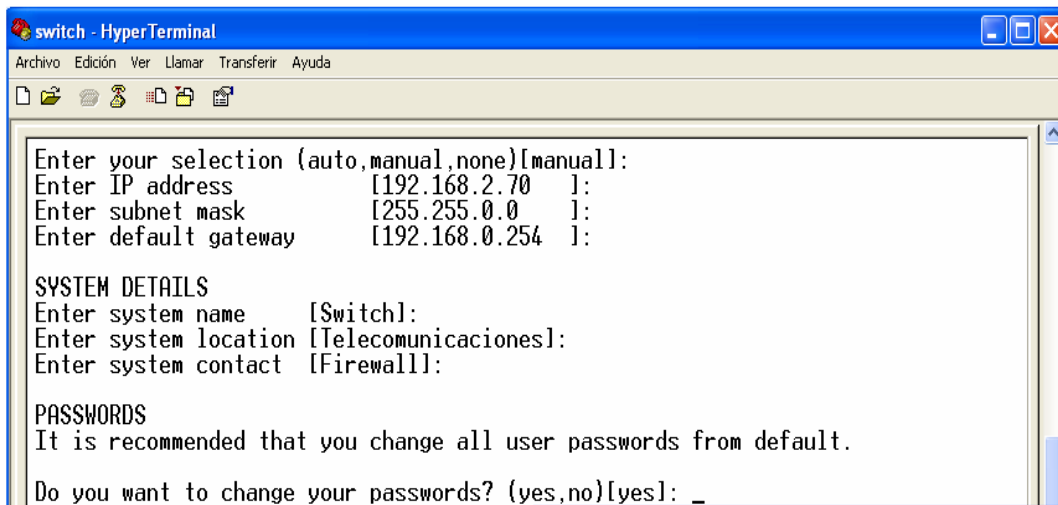


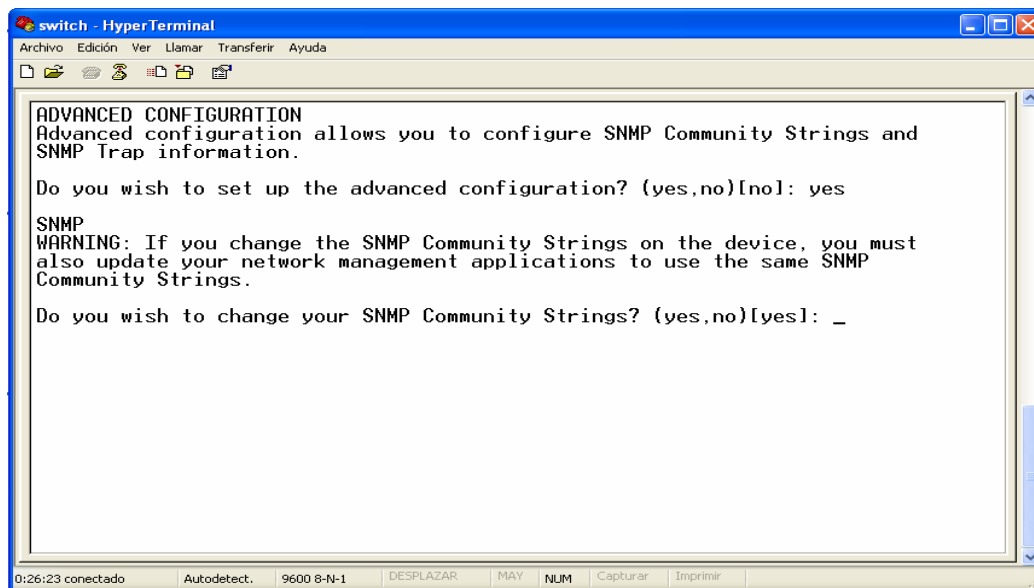
Figura 13.24 Pantalla de menús del Switch 4400 3COM

En esta pantalla se exhibe un menú con diferentes opciones. Se debe de teclear la opción “*gettingStarted*” en el *Prompt*. De este modo aparecerá la pantalla mostrada por la figura 13.25, la cual despliega opciones de configuración para el *Switch*, como: dirección IP, máscara de subred, localización, *gateway*, etc.



**Figura 13.25** Opciones de configuración del Switch 3COM 4

Una vez configuradas dichas opciones, aparecerá el *Prompt* para la configuración avanzada, así como lo muestra la figura 13.26.



**Figura 13.26** Configuración avanzada para el agente SNMP

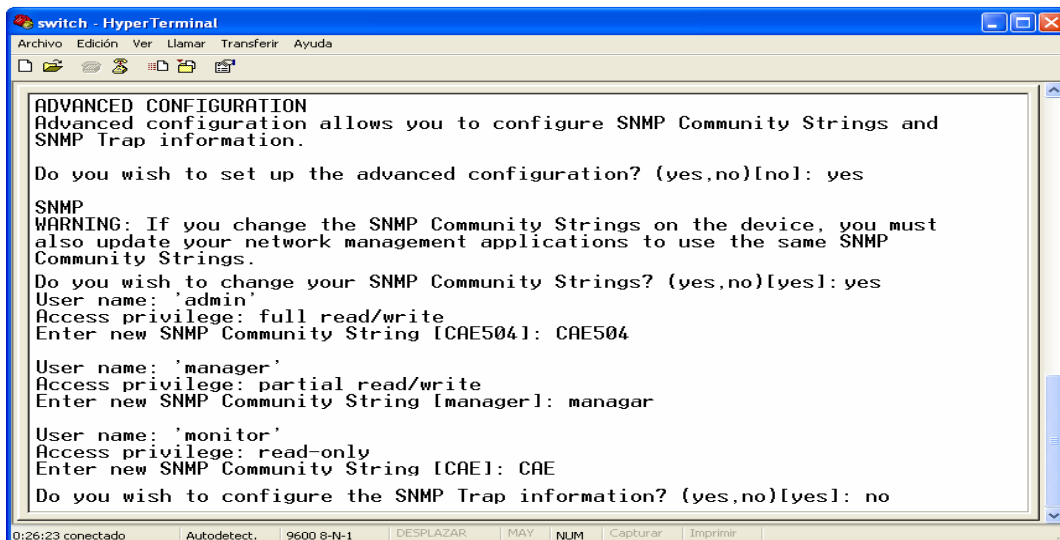


Figura 13.27 Configuraciones de las comunidades SNMP

Una vez que se teclea la palabra “yes” en el *Prompt* aparecerá un letrero de advertencia como se muestra en la figura 13.27. En esta parte se debe introducir el nombre de la comunidad de lectura y escritura de acceso privilegiado y dar entrar, posteriormente se debe introducir el nombre de la comunidad de lectura y escritura en modo administrador o medio de seguridad y dar entrar, por último se debe dar el nombre de la comunidad de sólo lectura y dar entrar.

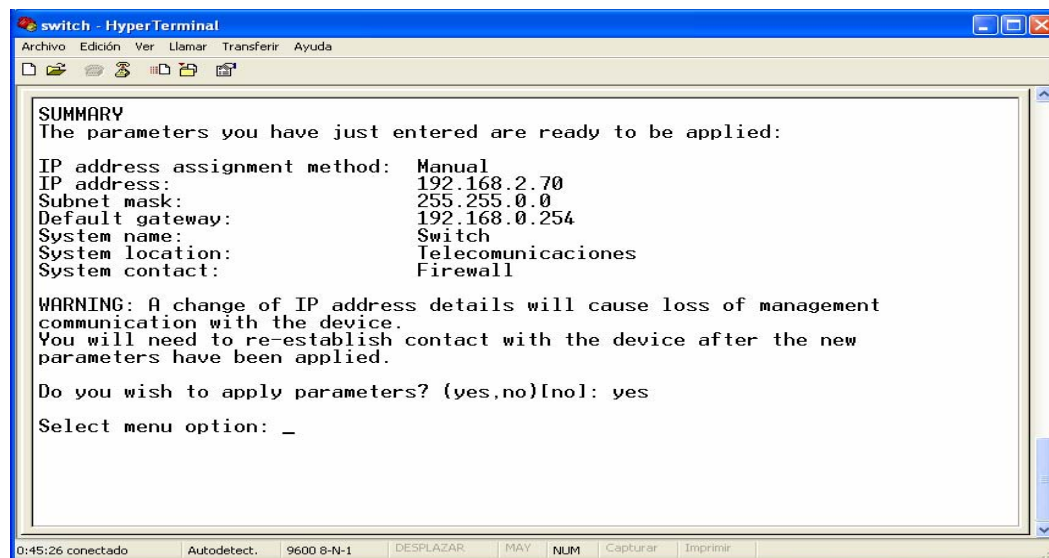
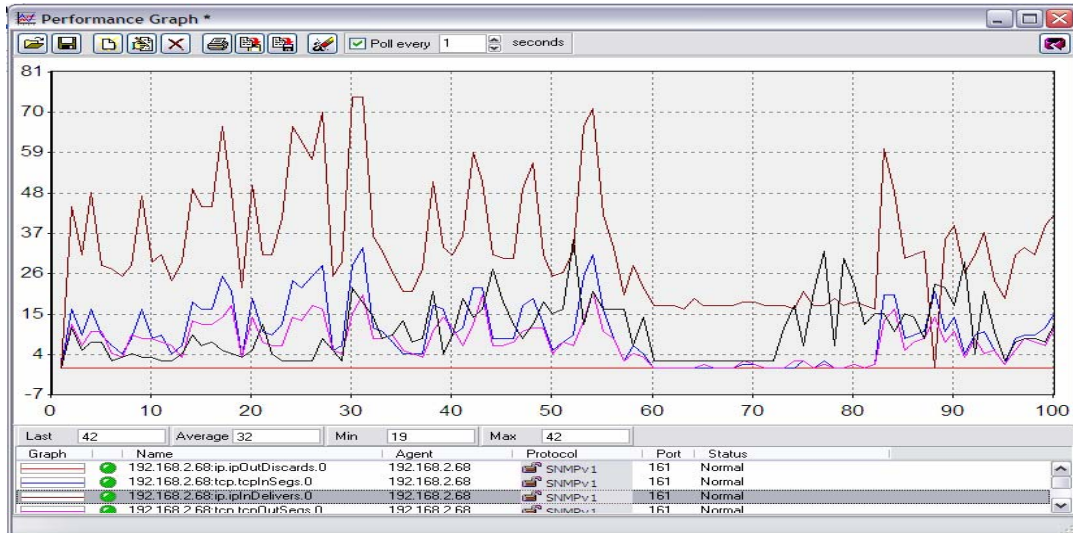


Figura 13.28 Resumen de la configuración.

Una vez hecho lo anterior se presentará un resumen donde se muestran los cambios hechos en el dispositivo como lo muestra la figura 13.28.

Una vez configurado el agente del dispositivo con sus respectivas comunidades se procede a monitorearlo, para lograr esto, se manda a llamar al agente utilizando para este caso en particular el MG – SOFT , el cual desplegará el árbol del agente de allí según se vio en el capítulo 11, se monitorea dicho dispositivo.



**Figura 13.29 Monitoreo del Agente del Switch**

En este caso en particular la figura 13.26 muestra el tráfico IP entrante y saliente, así como el tráfico TCP entrante y saliente.

Como se ha podido observar, existen dos maneras de llevar a cabo la optimización del CAE504, ¿cual propuesta elegir?, eso dependerá de los objetivos y del análisis del costo-beneficio, así como de los recursos con los que se cuenta.

No obstante, la segunda propuesta es una opción óptima, sin embargo, se requiere de recursos mayores, con respecto a la primera propuesta. Por otro lado se puede ver que los beneficios obtenidos con la primera propuesta, no son muy diferentes con respecto a la segunda propuesta, sin embargo, el costo es muy diferente entre ambas propuestas, siendo la primer propuesta, por mucho, más económica.

### 13.6 Presupuesto requerido para implantar la propuesta 2.

El equipo del que se hará mención en la tabla 13.2, no se encuentra en el inventario de hardware elaborado en el capítulo 11.

Concentrador 1 Sala de Redes					
Cantidad	Descripción	Marca	Modelo	Costo USD c/u	Subtotal USD
1	Rack de acero: altura 2.13 m, largo 0.56 m.	NCS Jaguar	NCS-RL12-45HD	\$ 162.00	\$ 162.00
4	Patch panel 24 puertos, 350 Mhz Categoría 5e	CCMTECH	PAT-5E-24	\$ 56.00	\$ 224.00
4	Bandeja	NCS Jaguar	QES0319-0115	\$ 120.00	\$ 480.00
1	Distribuidor de poder. 10 conectores,	CCMTECH	PD-BRF100-1020	\$ 134.00	\$ 134.00
2	Tarjeta de red con conectores de fibra	OVISLINK	GE-2000NF	\$ 183.00	\$ 366.00
4	Kits de apilamiento:  <b>Cada kit contiene:</b>  - 2 Módulos de apilamiento. - 1 cable de apilamiento	3COM	3C17227	\$ 360.00	\$ 1440.00
1822 m	Rollo de 305 m. de cable UTP Categoría 5e	Oem	AWG24	\$ 223.00	\$ 1338.00
200	RJ – 45 Macho	PCCABLENET	13652	\$ 0.35	\$ 70.00
1	Acoplador multimodo	Lucent Technologies	LN-FALUP-SCSC-SMD	\$ 4.15	\$ 4.15
3	Conectores LC multimodo	Lucent Technologies	FUCULCMMFD	\$ 7.00	\$ 21.00
32 m	Fibra óptica Duplex	Optral	CBLEF-PLSTC-DUPL	\$ 1.65	\$ 53.00
183 m.	Canaleta 2m	IBOCO	CADE2568	\$2.00	\$ 366.00
				<b>Total USD</b>	<b>\$ 4658.15</b>

Tabla 13.2 Presupuesto para la optimización del CAE504

Con el objetivo de optimizar la infraestructura de la red del CAE504, se recomienda la adquisición del equipo mencionado en la tabla 13.2. No obstante, los costos son un aproximado promedio.

## Conclusiones

---

La administración de redes, es sin duda un tema fundamental, cuando se trata de optimizar recursos en una determinada red. Por ello la adopción de esta disciplina por parte del CAE504 será de mucha utilidad. De esta forma al rediseñar la red del CAE504 según las filosofías vistas en este trabajo, traerá beneficios como: la adopción de los estándares del cableado estructurado, optimización del ancho de banda, inventario de hardware, mapa de red, inventario IP, disminuir el número de dispositivos de interconexión, bitácoras de estadísticas, un entidad administradora de red, instalación de agentes SNMP, etc.

Se debe tomar con mucha atención la parte de análisis debido a que es fundamental ya sea para diseñar, optimizar ó expandir una red en particular ya que esta etapa es crítica a la hora de diseñar una red ó modificar alguna red ya existente.

Se debe de tener en cuenta que el caso del CAE504, es un caso particular, es por ello que quizás no todas las recomendaciones se pueden aplicar. No obstante, dependiendo de la red a analizar, se pueden hacer uso de algunas o quizás de todas las recomendaciones mencionadas en este trabajo, ya que se puede tratar de diseñar una red desde el inicio, se puede tratar de expandir una red en particular u optimizar una red, como fue en este caso en particular.

Para el caso particular del CAE504 no fue necesario modelar la red bajo el estándar *eTOM* debido a que la propuesta de este trabajo muestra los resultados de manera muy clara, no obstante, cuando los resultados no son tan claros o la red diseñada todavía está en papel, es muy recomendable simularla antes de implantarla, de este modo se pueden prevenir ciertos problemas como: cuellos de botella, disminución de ancho de banda, tiempos de respuesta innecesarios, etc.

Para el caso particular del CAE504, propuesta de este trabajo, la optimización, hechó mano del inventario de hardware con la finalidad de llevar a cabo dicha optimización de la manera más económica para la institución para la cual se esta analizando la red en cuestión.

En la optimización de recursos, sólo se utilizan 6 dispositivos de interconexión de los 11 que se tienen funcionando. Con esto no sólo se tiene un ahorro en mantenimiento de dispositivos, sino que también se refleja una disminución en el consumo de energía, púes hay que recordar que los dispositivos de interconexión funcionan las 24 horas del día.

## Conclusiones

---

La nueva organización propuesta en este trabajo traerá un cuarto de telecomunicaciones, donde se centralizará la electrónica de la red, a través de éste, será mucho más sencillo ejercer la administración de la red del CAE504 y tener acceso a los beneficios que esto trae con su implantación.

El nuevo direccionamiento IP permite una mejora en la administración de direcciones IP, y un mejor control sobre éstas. De esta forma se pueden restringir ciertos servicios de Internet a grupos de direcciones IP mientras a otros se les puede dar acceso a estos servicios.

El desarrollar este trabajo fue muy enriquecedor, ya que me permitió ver el universo de las redes desde otra perspectiva, dejándome ver que aún falta mucho por aprender a cerca del tema de redes, antes de considerarme un conocedor del mismo.



## A

### **ACCESS POINT**

Punto de acceso inalámbrico: Es un producto comercial diseñado para actuar como el equivalente inalámbrico de un concertador o switch.

**ANCHO DE BANDA.-** Es el rango de frecuencias en el que se concentra la mayor parte de la potencia de la señal.

### **ANS.1**

Notación de sintaxis abstracta 1: Se trata de un conjunto de producciones que determinaran a las estructuras de datos, tipos y variables de una especificación.

### **ANSI**

Instituto Nacional Estadounidense de Estándares: Es una organización sin ánimo de lucro que supervisa el desarrollo de estándares para productos, servicios, procesos y sistemas en los Estados Unidos.

## B

### **BER**

Reglas de codificación básicas: Es el conjunto de reglas para representar como cadenas de unos y ceros, objetos abstractos del lenguaje ASN.1.

### **BROADCAST**

Señal de difusión: Es un modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

## C

### **CCITT**

Comité Consultivo Internacional Telegráfico y Telefónico: Coordina los estándares para las telecomunicaciones.

**CMIP**

Protocolo de información de administración común: Es el protocolo de comunicación empleado en el modelo de administración de sistemas de sobre el modelo de referencia OSI con sus siete capas.

**CMOT**

Protocolo de información de administración común sobre TCP: Es el protocolo de comunicación empleado en el modelo de administración de sistemas de sobre la torre de protocolos TCP.

**D**

**DHCP**

Protocolo de configuración dinámica para equipos: Es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente

**DoD.-** Departamento de defensa de los Estados Unidos.

**E**

**EIA**

Alianza de industrias electrónicas: Define un sistema genérico de alambrado de telecomunicaciones para edificios que puedan soportar un ambiente de productos y proveedores múltiples.

**eTOM**

enhanced Telecom Operations Map: Las operaciones realizadas bajo esta metodología de las telecomunicaciones son el estándar más ampliamente utilizado y más aceptado para el proceso del negocio en la industria de la telecomunicación

**F**

**FIREWALL**

Es un elemento que se utiliza en redes de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas.

**G**

**GATEWAY**

Puerta de enlace: Es la salida que sirve como enlace entre dos o más redes distintas.

**GDMO**

Clases de Objetos Administrables en el modelo de referencia de administración de sistemas según OSI.

**H**

**HEMS**

High-Level Management System

**I**

**IAB**

Consejo de la Arquitectura de Internet:

**IANA**

Internet Assigned Numbers Authority: Coordina los estándares necesarios para las direcciones en Internet. Es una institución de origen gubernamental.

**IEEE.-**

Instituto de ingenieros de electrónica y electricidad.

**IESG**

Internet Engineering Steering Group

**IETF**

Grupo de trabajo de ingeniería en Internet: Son la técnica de la red. Centrados en el protocolo de Internet el TCP/IP están a las ordenes de ISCO.

**INTRANET**

Se trata de una red privada, la cual no puede ser vista desde Internet.

**IP**

Protocolo de Internet: Se utiliza para llevar a cabo el routeo de paquetes.

**ISOC**

Sociedad de Internet: Es una agrupación sin ánimo de lucro que promulga políticas y promueve la conectividad global en Internet. Este grupo es lo que más cerca queda, a modo de gobierno central, dentro de Internet. Se creó en el 92 y esta completamente abierto a todo aquel que quiera formar parte.

## J

### **JACK RJ-45 HEMBRA**

Conector donde se conecta el RJ – 45 macho.

## L

### **LAN**

Red de área local: Se trata de una red de oficina o de una planta de un edificio.

## M

### **MIB**

Base de información de administración: Se trata de la base de datos que contiene toda la información de un dispositivo a consultar por un agente SNMP.

### **MRTG**

Multi Router Traffic Grapher

### **MO**

Objetos administrados: Abreviatura utilizada para designar a algun objeto administrado dentro de la administración de sistemas según OSI.

### **MODEM**

Dispositivo que permite la transmisión de un flujo de datos digitales a través de una señal analógica.

## N

### **NETWORK MANAGER**

Administrador de redes.

### **NOC**

Centro de operaciones de red: Generalmente es un software que sirve como interfaz entre el administrador y el nodo administrado.

## O

### **O<sub>A</sub>**

Interfaces administradas.

### **OID**

Identificador de objeto: Es un número dado por el conjunto de nodos del árbol derivado por la estructura de información de administración.

**OSI**

Open Systems Interconnection: Es una arquitectura para comunicaciones entre computadoras.

**P**

**PATCH PANEL**

Son estructuras metálicas con placas de circuitos que permiten interconexión entre equipos concentrando un conjunto de cables en un solo dispositivo

**PDU**

Unidad de datos de protocolo: Secuencia de unos y ceros del mensaje SNMP.

**PROMP**

Es la línea donde se escriben los comandos

**PROXY**

Permitir el acceso a Internet a todos los equipos de una organización.

**R**

**RACK**

Armario donde se disponen equipos de interconexión.

**RFC**

Request For Comments: Especifica el método para llevar a cabo una tarea.

**ROUTER**

Dispositivo encaminador de paquetes en la red.

**RTC**

Red de telecomunicaciones.

**S**

**SGMP**

Sistema de Gestión y Monitoreo de Proyectos

**SMI**

Estructura de Información de administración.

**SMF**

Funciones de administración de sistemas

**SNMP**

Protocolo simple de administración de redes.

**SP**

Proveedora de servicios.

**T**

**TIA**

Asociación de industrias de telecomunicaciones.

**TRAP**

Es una señal generada por un agente para reportar ciertas condiciones y cambios de estado a un proceso de administración.

**U**

**UDP**

Protocolo de datagrama de usuario.

## Bibliografía

---

Feit, Sydney. *SNMP: A Guide to Network Management*. McGraw-hill, 1994.

Harneday, Sean J. *Total SNMP: Exploring the Simple Network Management Protocol*. Segunda edición, 1997.

Hein, Mathis, Griffiths, David. *SNMP Version 1 & 2: Simple Network Management Protocol*. International Thompson Computer Press, 1995.

Leinwand, Allan, Fang-Conroy, Karen. *Network Management: A Practical Perspective*. Segunda edición, Addison-Wesley, 1995.

Miller, Mark A. *Managing Internetworks Whit SNMP*. Segunda edición, M&T Books, 1993.

Perkins, David, McGinnis, Evan. *Understanding SNMP MIBs*. Prentice Hall, 1997.

Stalling Williams. *SNMP, SNMPv2, and RMON: Practical Network Management*. Segunda edición, 1996.

Comer, Douglas E. *Interworkings whit TCP/IP – Volume I: Principles, Protocols, and Architecture*. Tercera edición, Prentice-Hall, 1995.

Steedman, Douglas, *Abstract Syntax Notation One (ANS.1) The tutorial and reference, Technology Appraisals, Isleworth*. Middlesex United Kingdom, 1993

## Referencias en Internet

---

### **Modelo Cliente/Servidor**

[www.ucm.es/info/Psyap/taller/aulas98.htm](http://www.ucm.es/info/Psyap/taller/aulas98.htm)

### **Hardware cliente-servidor**

<http://www.fismat.umich.mx/~elizalde/tesis/node19.html>

### **Internet Society**

<http://www.isoc.org>

### **What is an RFC?**

<http://www.RFC.net>

### **MG-SOFT**

<http://www.mibbrowserusermanual.si>

### **MG- SOFT**

<http://www.mg-soft.si>

### **Über ITSMI**

<http://www.itsm.org/>

### **El Modelo de referencia OSI de telecomunicaciones**

[http://www.geocities.com/txmetsb/el\\_modelo\\_de\\_referencia\\_osi.htm](http://www.geocities.com/txmetsb/el_modelo_de_referencia_osi.htm)

### **Saulo.Net**

<http://www.saulo.net/>

### **Redes de computadora**

[www.noc.unam.mx/tech-docs/tmn-unam2.ppt](http://www.noc.unam.mx/tech-docs/tmn-unam2.ppt)

### **Cambridge Consultants - Next-generation telecommunications network**

[www.cambridgeconsultants.com/news\\_pr4.shtml](http://www.cambridgeconsultants.com/news_pr4.shtml)



Alambrado de Edificios:  
ANSI/TIA/EIA-568-A y B

Vías y espacios de telecomunicaciones:  
ANSI/EIA/TIA-569.

Normas para la codificación de colores, etiquetado, y documentación de un sistema de cableado instalado:  
ANSI/TIA/EIA-606.

Requisitos de aterrizado y protección para telecomunicaciones en edificios:  
ANSI/TIA/EIA-607.

Cableado Horizontal:  
ANSI/TIA/EIA TSB-75.

Cableado de Planta Externa  
ANSI/TIA/EIA-758.