

**DISEÑO DE UNA GUÍA METODOLÓGICA PARA LA EVALUACIÓN Y
PRUEBAS DE RENDIMIENTO DE REDES LAN MEDIANTE LA UTILIZACIÓN
DE SOFTWARE GNU**

ELISA VERÓNICA ROMERO CRUZ

**UNIVERSIDAD AUTÓNOMA DE BUCARAMANGA
FACULTAD DE INGENIERÍA DE SISTEMAS
TELECOMUNICACIONES Y TECNOLOGÍAS WEB
BUCARAMANGA**

2010

**DISEÑO DE UNA GUÍA METODOLÓGICA PARA LA EVALUACIÓN Y
PRUEBAS DE RENDIMIENTO DE REDES LAN MEDIANTE LA UTILIZACIÓN
DE SOFTWARE GNU**

ELISA VERÓNICA ROMERO CRUZ

Trabajo de grado presentado para optar el título de Ingeniero de Sistemas

**Director:
Ing. Karol Dalila Reyes**

**UNIVERSIDAD AUTÓNOMA DE BUCARAMANGA
FACULTAD DE INGENIERÍA DE SISTEMAS
TELECOMUNICACIONES Y TECNOLOG
BUCARAMANGA**

2010

Nota de Aceptación

Firma Director

Firma del Jurado

Firma del Jurado

Bucaramanga 23 de Noviembre de 2009₃

AGRADECIMIENTOS

El autor expresa su agradecimiento a:

Dios por darme sabiduría y fortaleza en cada una de las dificultades que se me presentaron en la realización de este proyecto, Gracias Señor por iluminarme y darme las oportunidades para seguir adelante. TE AMO.

A mi madre NURIS, por apoyarme y esperar el momento preciso para darle este orgullo. A Mantilla por conseguir los recursos necesarios para continuar con mi carrera. A Juan David y Rafael por darme esos momentos de alegría y relax que necesitaba.

Un agradecimiento especial, a mi directora Karol, por todo el apoyo, el seguimiento, interés y confianza que depositó en mí para guiarme en la realización de mi proyecto, por el tiempo que me dedicó sabiendo que tenía muchas cosas que hacer. Gracias Karol.

Y a todas las personas que contribuyeron en mi formación personal, que me acompañaron y estuvieron apoyándome en los momentos más difíciles de mi vida.

Gracias a Todos.

CONTENIDO

	pág.
INTRODUCCIÓN	18
1 OBJETIVOS	20
1.1 OBJETIVO GENERAL	20
1.2 OBJETIVOS ESPECÍFICOS	20
2 MARCO TEÓRICO	22
2.1 ¿QUÉ ES UNA RED DE ÁREA LOCAL?	22
2.2 TOPOLOGÍA DE REDES DE ÁREA LOCAL	23
2.3 TRANSFERENCIA DE INFORMACIÓN	24
2.3.1 Redes Conmutadas	24
2.3.1.1 Conmutación de Circuitos	24
2.3.1.2 Conmutación de paquetes	25
2.3.1.3 Conmutación de mensajes	25

2.3.2	Redes de Difusión (Multipunto)	25
2.4	ARQUITECTURAS DE REDES	25
2.4.1	El modelo OSI	26
2.4.2	El modelo TCP/IP	27
2.5	PERTURBACIONES EN LA TRANSMISIÓN	28
2.5.1	Atenuación	28
2.5.2	Distorsión de retardo	29
2.5.3	Ruido	29
2.5.4	Capacidad del canal	29
2.6	PROTOCOLO DE RED	30
2.6.1	SNMP: <i>Simple Network Management Protocol</i>	30
2.7	PROTOCOLOS DE RED EN EL MODELO TCP/IP	32
2.7.1	Capa de Red	33
2.7.1.1	<i>Protocolo IP</i>	33
2.7.1.2	<i>Protocolo ARP</i>	34

2.7.1.3	Protocolo DHCP	35
2.7.2	CAPA DE TRANSPORTE	35
2.7.2.1	<i>Protocolo TCP</i>	35
2.7.2.2	Protocolo UDP	36
2.7.2.3	Protocolo SCTP	36
2.7.3	CAPA DE APLICACIÓN	37
2.7.3.1	Telnet	37
2.7.3.2	<i>Protocolo FTP</i>	37
2.7.3.3	Protocolo SMTP	38
2.7.3.4	Protocolo DNS	38
2.7.3.5	Protocolo HTTP	40
2.8	LA ADMINISTRACIÓN DE REDES, ENFOQUE PARA LA EVALUACIÓN Y PRUEBAS DE REDES LAN	40
2.8.1	Documentación de Red	41
2.8.2	Distribuciones MDF e IDF	41
2.8.3	Registros de Mantenimiento	41

2.8.4	Rendimiento de la red	41
2.8.5	Control de red	42
2.8.6	Control de tráfico	42
2.8.7	Solución de problemas de red	42
2.9	DESARROLLO DE LA GUÍA	43
2.9.1	MRTG	46
2.9.1.1	Funcionamiento de MRTG	47
3	CASO DE ESTUDIO Y DE APLICACIÓN DE LA METODOLOGÍA DE LA GUÍA: COLEGIO NUEVO CAMBRIDGE	49
3.1	DOCUMENTACIÓN Y ESTABLECIMIENTO DE LA LÍNEA BASE	49
3.1.1	Capa de acceso	49
3.1.1.1	Esquema de la Red	49
3.1.1.2	Topología de la Red	50
3.1.1.3	Distribución de la Red – Mapa de Centros de Cableado y Ubicación de Equipos	50
3.1.1.4	Equipos Activos	56

3.1.2	Capa Interred	60
3.1.2.1	Asignación y Recopilación de Direcciones IP	60
3.1.2.2	Ancho de Banda	60
3.2	MONITOREO	61
3.2.1	Capa de Interred, Transporte y Aplicación	61
3.2.1.1	Configuración de MRTG y SNMP	61
4	CONCLUSIONES	69
	BIBLIOGRAFÍA	71
	ANEXOS	73

LISTA DE TABLAS

	pág.
Tabla 1. Capas del Modelo OSI y sus funciones	26
Tabla 2. Capas del Modelo TCP/IP y sus funciones	28
Tabla 3. Metodología de la Guía	44
Tabla 4. Equipos Activos	56
Tabla 5. Características del Servidor Principal y School Pack	57
Tabla 6. Distribución del Ancho de Banda Colegio Nuevo Cambridge	60

LISTA DE FIGURAS

	pág.
Figura 1. Esquema de una Red de Área Local	23
Figura 2. Topologías Lógicas en Redes LAN	23
Figura 3. Arquitectura de Administración de SNMP	31
Figura 4. Protocolos en el modelo TCP/IP	33
Figura 5. Diagrama de Procesos para Corrección de Errores	48
Figura 6. Distribución topológica de la Red del Colegio Nuevo Cambridge	50
Figura 7. Distribución de Centros de Cableado y Equipos. Piso 1	52
Figura 8. Distribución de Centros de Cableado y Equipos. Piso 2	53
Figura 9. Distribución de Centros de Cableado y Equipos. Piso 3	54
Figura 10. Distribución de Centros de Cableado y Equipos. Piso 4	55
Figura 11. Distribución de Equipos Activos	59
Figura 12. Ejecución de SNMP	64

Figura 13. Configuración de la Comunidad en el Switch DELL 66

Figura 14. Configuración de envío de la lectura de SNMP al Servidor 67

LISTA DE ANEXOS

	pág.
Anexo A. Registro de Operaciones Diarias	74
Anexo B. Hoja de vida Equipos De Cómputo y/o Comunicación	75
Anexo C. Registro de direcciones IP y MAC	76
Anexo D. Encuesta realizada a administradores	77
Anexo E. Tabulación y Gráficos de Resultados encuesta	79

GLOSARIO

ANCHO DE BANDA: aplicado a un medio de transmisión, se refiere a su capacidad de transmisión de la información.

ARP (*Address Resolution Protocol o Protocolo de Resolución de Direcciones*): es un protocolo incluido en la arquitectura TCP/IP que permite averiguar la dirección MAC de un equipo a través de su dirección.

ARQUITECTURA DE RED: especifica la topología, el método de acceso al medio y los protocolos de comunicaciones de la red.

CONTROL DE FLUJO: método asociado con el propósito de impedir saturación de un equipo receptor de datos. Hay que tener en cuenta que la recepción de la información necesita tiempo de proceso y que el destinatario utiliza una memoria limitada para almacenar temporalmente los mensajes entrantes. Si esa memoria se llena, el receptor puede perder los siguientes mensajes que llegan.

DATAGRAMA: método de transmisión derivado de la conmutación de paquetes donde cada paquete se envía de forma independiente. No se establece ninguna reserva de ninguna trayectoria (por donde circularán los paquetes).

DIRECCIÓN: este término aplicado a las redes de comunicaciones se utiliza generalmente para identificar de forma unívoca a los usuarios o equipos conectados a ella.

DNS (*Domain Name System o Sistema de Nombres de Dominio*): se trata de un protocolo TCP/IP que permite utilizar direcciones de dominio (formada por cadena de caracteres) que están asociadas con direcciones IP. De esta forma, los

usuarios pueden trabajar con direcciones de dominio que son más sencillas de recordar y utilizar que las direcciones IP.

FTP (File Transfer Protocol o Protocolo de Transmision de Archivos): servicio que permite la transferencia de archivos entre un equipo cliente y un servidor.

HTTP (Hyper Transfer Protocol o Protocolo de Transferencia de Hipertexto): es el protocolo utilizado por los equipos clientes para obtener páginas de hipertexto desde los servidores.

HUB (Concentrador): es el dispositivo multipuerto encargado de interconectar los distintos equipos que forman la red. Puede ser activo o pasivo y simple o dual.

IP (Internet Protocol o Protocolo de Interred): es el protocolo más importante que funciona a nivel de red de la arquitectura TCP/IP.

LAN (Local Area Network o Red de Área Local): constituye un grupo de equipos que se encuentran interconectados a una distancia corta. Esta distancia suele reducirse a un interior de un edificio o a edificios colindantes.

MAC (Media Adrress Control o Control de Acceso al Medio): es la técnica que consiste en controlar la utilización de un medio compartido por varios equipos.

MRTG (Multi Router Traffic Grapher) es un programa de Código Abierto que se puede implementar sobre Sistemas Operativos UNIX (más común) y Windows para realizar graficas del tráfico por medio del protocolo SNMP.

PAR TRENZADO: cable formado por dos hilos de cobre revestidos por un aislante que van entrelazados de forma helicoidal para aumentar su inmunidad al ruido.

PROTOCOLO: conjuntos de normas que definen cómo debe realizarse un servicio de una determinada red de comunicación.

RARP (*Reverse Address Resolution Protocol o Protocolo de Resolución de Direcciones Inverso*): este protocolo se encarga de obtener la dirección IP de un equipo del que se conoce su dirección MAC.

ROUTER: dispositivo de interconexión de redes que funciona a nivel de red de la arquitectura y que decide cuál es el mejor camino para el envío de los paquetes.

SMTP (*Simple Mail Transfer Protocol o Protocolo Simple de Transferencia de Correo*): protocolo de gestión de correo electrónico utilizado en Internet.

SNMP (*Simple Network Management Protocol o Protocolo Simple de Administración de Red*): protocolo que permite monitorizar el estado de las estaciones y dispositivos de la red.

TCP (*Transmission Control Protocol o Protocolo de Control de la Transmisión*): este protocolo está definido en el nivel de transporte de la arquitectura TCP/IP y se encarga fundamentalmente de controlar los errores que no detectan los protocolos a niveles inferiores.

TCP/IP: arquitectura de comunicaciones que emplea la red Internet. Los protocolos más importantes que incluye son TCP (a nivel de transporte) e IP (a nivel de red).

TELNET (*Telematics Network o Red Telemática*): servicio definido en el nivel de aplicación del TCP/IP que se utiliza para iniciar sesiones de terminal remoto en equipos servidores.

TOPOLOGÍA: forma en la que se encuentran interconectados los

diferentes equipos en la red. La *topología física* se refiere a la definición anterior, mientras que la *topología lógica* se refiere a cómo se distribuye la información enviada por la red.

UDP (*User Datagram Protocol* o *Protocolo de Datagramas de Usuario*): protocolo definido a nivel de transporte de TCP/IP que, al contrario de TCP, es no orientado a la conexión y no realiza control de errores.

Hoy en día es necesario que la información y servicios de red en una empresa sean entregados a sus usuarios de manera ágil y rápida. Para tal rendimiento es necesario el trabajo de un administrador, trabajo que se elabora con la supervisión diaria del desempeño de la red y la solución de problemas que se presenten en la transmisión.

En este documento se presenta la reseña del diseño de una Guía Metodológica que sirve de refuerzo para un administrador de red a la hora de realizar un trabajo de diseño lógico y físico en la evaluación y realización de pruebas de una red de datos.

La Guía está estructurada en **3 fases** importantes: La recopilación de conceptos básicos, los métodos para la elaboración de pruebas de rendimiento de la red y un caso de estudio con la aplicación de los métodos recomendados.

Línea de Investigación: Las Redes de computadoras como eje principal en la comunicación, lo que nos lleva al Diseño, implementación, gestión y mantenimiento de ellas, otorgando soluciones informáticas.

Palabras Claves: Redes de Área Local, Evaluación, Pruebas, Métodos, Administración de Redes.

Este proyecto tiene como objetivo principal crear una guía de apoyo para los administradores de red, un material que los ayudará en los procesos de evaluación y realización de pruebas de rendimiento de redes a partir de las mejores prácticas y el recorrido ascendente de las capas del modelo TCP/IP. Adicionalmente, se recomienda el uso de herramientas de software libre como Multi Router Traffic Grapher: MRTG.

La Guía está estructurada de manera que se logre una implementación fácil y practica de los constantes seguimientos que se deben llevar a cabo para el mejoramiento del rendimiento de una red, y desde ese punto el administrador pueda dar soluciones a fallas considerando experiencias y parámetros usados con mayor frecuencia.

La Guía consta de tres fases importantes, la primera consta de conceptos sobre redes LAN y su estructura básica.

La segunda fase consiste en las tareas que se deben tener en cuenta para llevar a cabo una buena evaluación y realización de pruebas de rendimiento de una red.

Por último, la fase de caso de estudio, el cual se basa en la realización de pruebas de rendimiento en la red del Colegio Nuevo Cambridge a partir de los pasos planteados en La Guía.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Desarrollar una Guía metodológica que proporcione una secuencia de pasos de análisis, diagnóstico y evaluación de redes de datos, que permita a los administradores realizar consideraciones a nivel físico y lógico en la solución de problemas, o el planteamiento del crecimiento y desarrollo de la misma.

1.2 OBJETIVOS ESPECÍFICOS

- Realizar una documentación completa con recomendaciones e información sobre el rendimiento de la red por medio de pruebas de análisis realizadas a redes LAN para dar soporte al administrador de red
- Realizar una investigación de los diferentes tipos de pruebas y evaluaciones que se realizan a una red, con el fin de hacer una selección de las herramientas más útiles que cubran el análisis del diseño lógico y físico de la misma, así como el análisis de tráfico, análisis de ancho de banda, evaluación de cableado y utilidades estadísticas como sniffer, entre o otros.
- Revisar las mejores prácticas utilizadas por los administradores de Red con el fin de analizar diferentes casos de uso y determinar qué procesos son los más usados para analizar las redes de datos y las medidas o decisiones tomadas al final del estudio.

- Desarrollar una Guía metodológica de las mejores prácticas de análisis y acciones que un administrador de red puede seguir para un óptimo planeamiento en el crecimiento y desarrollo de las redes de transmisión de datos

2. MARCO TEÓRICO

2.1 ¿QUÉ ES UNA RED DE ÁREA LOCAL?

“Las **redes de área local**, generalmente llamadas **LAN** (*Local Area Network*), son redes de propiedad privada dentro de un solo edificio o campus hasta unos cuantos kilómetros de extensión. Se usan ampliamente para conectar computadoras y estaciones de trabajo... Las LAN se distinguen de otro tipo de redes por tres características: (1) Su Tamaño, (2) su tecnología de transmisión, y (3) su topología.”¹

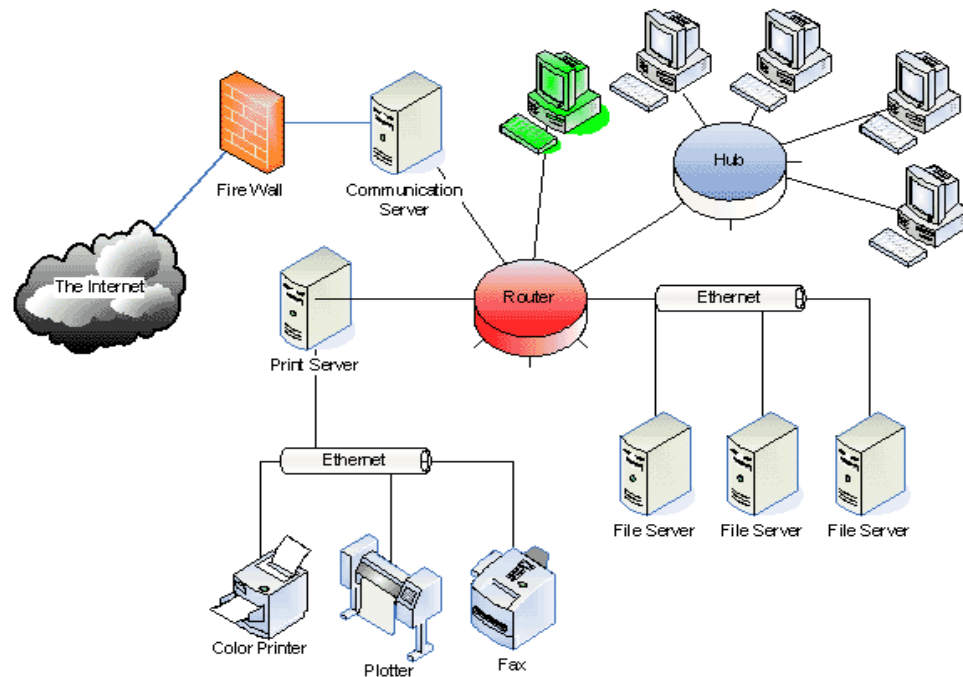
Las LAN están restringidas en tamaño, lo cual significa que el tiempo de transmisión del peor caso está limitado y se conoce de antemano. Conocer este límite hace posible usar ciertos tipos de diseños que de otra manera no serían prácticos, y también simplifica la administración de la red.²

El término red local incluye tanto el hardware como el software necesario para la interconexión de los distintos dispositivos y el tratamiento de la información.

¹ Definición Redes de Area Local. ANDREW S. TANENBAUM. Redes de Área Local, Vrije Universiteit. Amsterdam, The Netherlands. Editorial Pearson. 1997

² Definición Redes de Area Local. ANDREW S. TANENBAUM. Redes de Área Local, Vrije Universiteit. Amsterdam, The Netherlands. Editorial Pearson. 1997

Figura 1. Esquema de una Red de Área Local



Fuente: Autor del proyecto

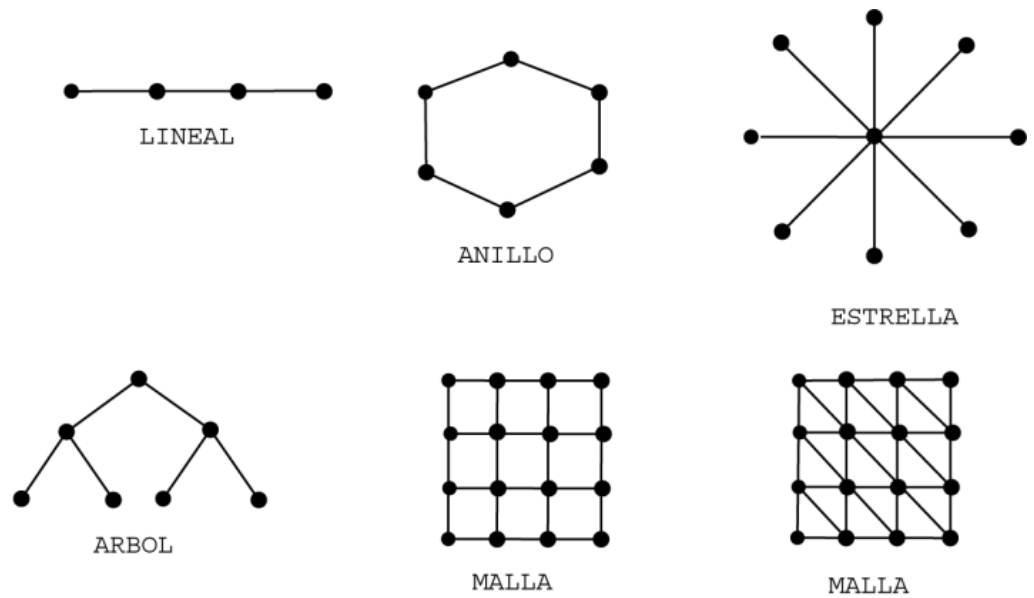
2.2 TOPOLOGÍA DE REDES DE ÁREA LOCAL

En la conexión de computadores se pueden utilizar dos clases de topologías: Lógica y Física.

Topología Lógica: es la manera como están accediendo al medio los equipos y está relacionada con los protocolos. El acceso puede ser Determinístico (por turnos) y No Determinístico (por demanda).

Topología Física: es la manera como están interconectados los equipos de la Red, tales como: Bus o Lineal, Anillo, Estrella, Árbol, Malla, entre otras.

Figura 2. Topologías Lógicas en Redes LAN



Fuente: Autor del proyecto

2.3 TRANSFERENCIA DE INFORMACIÓN

En la transferencia de la información se clasifican teniendo en cuenta la técnica empleada para transferir la información desde el punto de origen al punto de destino, y por lo tanto también depende de la topología que se está empleando en la red.

2.3.1 Redes Conmutadas (punto a punto). Un equipo origen (emisor) selecciona el equipo con el que se quiere conectar (receptor) y la red es la encargada de abrir una vía de conexión entre los dos equipos. Existen tres métodos para la transmisión de información y la habilitación de la conexión:

2.3.1.1 Conmutación de Circuitos: se establece un camino único dedicado. La ruta

que sigue la comunicación se establece durante todo el proceso de comunicación, y una vez terminada la comunicación es necesario liberar la conexión.

2.3.1.2 Conmutación de paquetes: en este caso el mensaje a enviar se divide en fragmentos cada uno de los cuales es enviado a la red y circula por esta hasta llegar a su destino.

2.3.1.3 Conmutación de mensajes: la información que envía el emisor se aloja en un único mensaje con la dirección de destino y se envía al siguiente nodo, éste almacena la información hasta que hay un camino libre, dando lugar, a su vez, al envío al siguiente nodo, y así sucesivamente hasta que el paquete llega a su destino.

2.3.2 Redes de Difusión (Multipunto): Un equipo o nodo envía la información a todos los nodos y el destinatario es el encargado de seleccionar y captar esa información.³

2.4 ARQUITECTURAS DE REDES

En este momento se pasa a brindar una visión general de todos los aspectos que entran en juego en una red cuando se empieza a interactuar en ella, respondiendo preguntas como ¿si se produce una cantidad de errores, cuál se debe empezar a corregir? ¿Hay que compartir un único medio de transmisión? ¿Cómo se

³ Libro Redes de Área Local de Francisco J. Molina

distinguen los diferentes dispositivos en la red? Y para emprender una tarea de administración de red se debe conocer que en las comunicaciones entran dos aspectos fundamentales: el hardware (dispositivos físicos) y el software (programas informáticos dedicados a controlar las comunicaciones).

En las redes de computadores existen dos modelos básicos súper importantes que se emplean como un estándar global, el modelo OSI y el modelo TCP/IP.

2.4.1 El modelo OSI. Este modelo fue propuesta de la organizaron internacional de normas ISO como un avance a la globalización de protocolos, el modelo se ocupa de sistemas abiertos, es decir, sistemas que están preparados para la comunicación con sistemas diferentes.

OSI emplea una arquitectura por niveles con el fin de dividir los problemas de interconexión en partes manejables.

Tabla 1. Capas del Modelo OSI y sus funciones

Capa	Nombre	Funciones	PDU
7	Aplicación	Es el nivel que está en contacto directo con los programas informáticos de las estaciones y contiene los servicios de comunicación más utilizados en las redes	Datos
6	Presentación	Se controla el significado de la información que se transmite, lo que permite la traducción de los datos entre las estaciones; representación de los datos	Datos

Capa	Nombre	Funciones	PDU
5	Sesión	Se establecen sesiones (conexiones) de comunicación entre los dos extremos para el transporte ordinario de datos	Datos
4	Transporte	Es la encargada de tomar los datos procedentes del nivel de sesión y pasarlos a la capa de red, asegurándose de que lleguen correctamente a la capa de sesión del otro	Segmentos
3	Red	Determina la mejor ruta para enviar los datos, mirando el de menor tamaño, mas rápido y menor trafico	Paquetes
2	Enlace de Datos	Detecta y corrige todos los errores que se producen en la transmisión. Al mismo tiempo, se encarga de controlar que un emisor rápido no sature a un receptor lento y se pierdan los datos	Tramas
1	Físico	Es la encargada de la transmisión de dígitos binarios por un canal de comunicación guiado	Bits

Fuente: Autor del proyecto

2.4.2 El modelo TCP/IP. Se suele confundir con un protocolo de comunicación concreto, pero en realidad es una arquitectura de red muy utilizada ya que es la base de comunicación de Internet.

A diferencia del modelo OSI, TCP/IP sólo tiene definida cuatro capas.

Tabla 2. Capas del Modelo TCP/IP y sus funciones

Capa	Nombre	Función
4	Aplicación	Esta capa contiene todos los protocolos de alto nivel que utilizan los programas para comunicarse como TELNET (Terminal Virtual), FTP (Transferencia de Archivos) y HTTP (protocolo que se usa para la navegación de paginas WWW)
3	Transporte	Establece una conversación entre el origen y el destino. Se destacan protocolos como TCP (Protocolo de Control de Transmisión, orientado a conexiones y fiable) y UDP (Protocolo de Data grama de Usuario, sin conexiones y no lleva a cabo control de errores)
2	Interred	Es la más importante de la arquitectura, y su misión consiste en permitir que las estaciones envíen información a la red y lo hagan viajar de forma independiente hasta su destino. En esta capa se encuentra el protocolo IP (Protocolo de Interred, establece el formato de paquetes y direcciones utilizado en esta capa y el tipo de servicio ofrecido)
1	Acceso	No se especifica mucho sobre esta capa, sólo se dice que debe existir algún protocolo que conecte la estación con la Red. Una razón fundamental es que TCP/IP se diseñó para su funcionamiento sobre redes diferentes y por consecuencia esta capa depende de la tecnología utilizada

Fuente: Autor del Proyecto

2.5 PERTURBACIONES EN LA TRANSMISIÓN

2.5.1 Atenuación: la energía de una señal decae con la distancia, por lo tanto hay que asegurarse que llegue con la suficiente energía como para ser captada por la circuitería del receptor y además, el ruido debe ser sensiblemente menos

que la señal original. Para mantener la energía de la señal se utilizan amplificadores o repetidores.

Debido a que la atenuación varía en función de la frecuencia, las señales analógicas llegan distorsionadas, por lo tanto es recomendable utilizar sistemas que le devuelvan a la señal sus características iniciales, usando bobinas que cambian las características eléctricas o amplificando las frecuencias más altas.

2.5.2 Distorsión de retardo: en medios guiados la velocidad de propagación de una señal varía con la frecuencia, es posible que se presente que unas frecuencias lleguen antes que otras dentro de la misma señal. Para atenuar este problema se usan técnicas de ecualización.

2.5.3 Ruido: es toda aquella señal que se inserta entre el emisor y el receptor de una señal dada. Hay diferentes tipos de ruido: el ruido térmico que se produce debido a la agitación térmica de los electrones dentro del conductor; el ruido de intermodulación que se presenta cuando distintas frecuencias comparten el mismo medio de transmisión; diafonía que se produce cuando hay un acoplamiento entre las líneas que transportan las señales; y el ruido impulsivo que se trata de pulsos discontinuos de poca duración y de gran amplitud que afectan la señal

2.5.4 Capacidad del canal: el canal es el elemento que se encarga del transporte de la señal sobre la que viaja la información que intercambia el emisor y el receptor. Se llama capacidad del canal a la velocidad a la que se pueden transmitir los datos de un canal de comunicación de datos. La velocidad de los datos es expresada en bits por segundo.

2.6 PROTOCOLO DE RED

Un protocolo es una descripción formal de un conjunto de reglas y convenciones que gobiernan el modo en que se comunican los dispositivos en una red. Los protocolos determinan el formato, la temporización, la secuenciación y el control de errores en la comunicación de datos. Sin los protocolos, la computadora no puede crear o reconstruir el flujo de bits entrante desde otra computadora a fin de obtener los datos originales.

Los protocolos controlan todos los aspectos de la comunicación de datos. Determinan cómo se construye la red física, cómo se conectan los computadores de red, cómo se formatean los datos para la transmisión y cómo se envían los datos.⁴

2.6.1 SNMP: Simple Network Management Protocol en español, Protocolo Simple de Administración de Redes, es un protocolo que permite a la administración transmitir datos estadísticos por una red a una consola de administración central.⁵

Principio Operativo de SNMP

El sistema de administración de red se basa en dos elementos principales: un supervisor y agentes. El supervisor es la terminal que le permite al administrador de red realizar solicitudes de administración. Los agentes son entidades que se encuentran al nivel de cada interfaz. Ellos conectan a la red los dispositivos administrados y permiten recopilar información sobre los diferentes objetos.

⁴ Protocolos de red. Guía del primer año. CCNA 1 y2. Tercera Edición. Academia de Networking de Cisco System.

⁵ Definición de SNMP, Fuente: <http://es.kioskea.net/contents/internet/snmp.php3>, para información adicional de SNMP, véase: Archivo rfc1157.txt

Los conmutadores, concentradores (hubs), routers y servidores son ejemplos de hardware que contienen objetos administrados. Estos objetos administrados pueden ser información de hardware, parámetros de configuración, estadísticas de rendimiento y demás elementos que estén directamente relacionados con el comportamiento en progreso del hardware en cuestión. Estos elementos se encuentran clasificados en algo similar a una base de datos denominada MIB: Base de datos de información de administración. SNMP permite el diálogo entre el supervisor y los agentes para recolectar los objetos requeridos en la MIB.

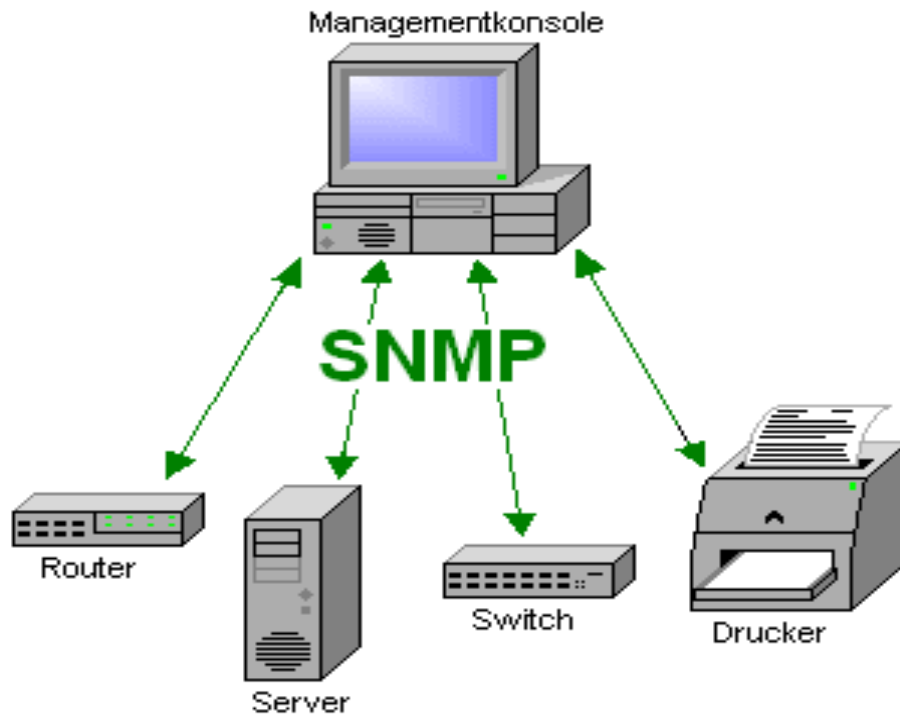
La arquitectura de administración de la red propuesta por el protocolo SNMP se basa en tres elementos principales:

Los **dispositivos administrados** que son los elementos de red (puentes, concentradores, routers o servidores) que contienen "objetos administrados" que pueden ser información de hardware, elementos de configuración o información estadística

Los **agentes**, es decir, una aplicación de administración de red que se encuentra en un periférico y que es responsable de la transmisión de datos de administración local desde el periférico en formato SNMP

El **sistema de administración de red (NMS)**, esto es, un terminal a través del cual los administradores pueden llevar a cabo tareas de administración.

Figura 3. Arquitectura de Administración de SNMP



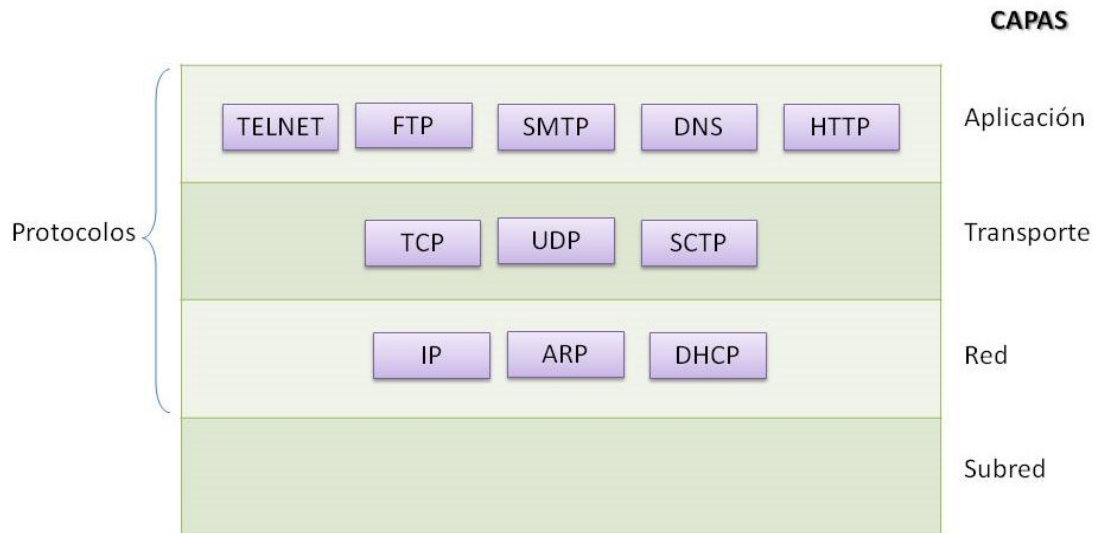
Fuente: Autor del Proyecto

2.7 PROTOCOLOS DE RED EN EL MODELO TCP/IP

TCP/IP es el conjunto de protocolos más utilizado, ya que millones de hosts de todo el mundo y todos los sistemas operativos utilizan este protocolo. TCP/IP es popular porque es flexible, compatible y capaz de funcionar bien en implementaciones de redes pequeñas y grandes. Debido a razones históricas y a la calidad y versatilidad de sus protocolos, TCP/IP es el conjunto estándar de facto de protocolos de Internet.⁶

⁶ Fundamentos de TCP/IP. Guía del primer año. CCNA 1 y 2. Tercera Edición. Academia de Networking de Cisco System

Figura 4. Protocolos en el modelo TCP/IP



Fuente: Tanenbaum, A. S. (1997). *Redes de Computadoras*. Tercera Edición

2.7.1 Capa de Red

2.7.1.1 *Protocolo IP*: el Protocolo de Internet (en inglés *Internet Protocol*) es un protocolo no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados.

Los datos en una red basada en IP son enviados en bloques conocidos como paquetes o datagramas (en el protocolo IP estos términos se suelen usar indistintamente). En particular, en IP no se necesita ninguna configuración antes de que un equipo intente enviar paquetes a otro con el que no se había comunicado antes.

El Protocolo de Internet provee un servicio de datagramas no fiable (también llamado del *mejor esfuerzo* (*best effort*), lo hará lo mejor posible pero garantizando poco). IP no provee ningún mecanismo para determinar si un paquete alcanza

o no su destino y únicamente proporciona seguridad (mediante *checksums* o sumas de comprobación) de sus cabeceras y no de los datos transmitidos. Por ejemplo, al no garantizar nada sobre la recepción del paquete, éste podría llegar dañado, en otro orden con respecto a otros paquetes, duplicado o simplemente no llegar. Si se necesita fiabilidad, ésta es proporcionada por los protocolos de la capa de transporte, como TCP.

2.7.1.2 *Protocolo ARP*: en Ingles, *Address Resolution Protocol* (Protocolo de resolución de direcciones). Es un protocolo de nivel de red responsable de encontrar la dirección hardware (Ethernet MAC) que corresponde a una determinada dirección IP. Para ello se envía un paquete (ARP request) a la dirección de multidifusión de la red (broadcast (MAC = ff ff ff ff ff)) que contiene la dirección IP por la que se pregunta, y se espera a que esa máquina (u otra) responda (ARP reply) con la dirección Ethernet que le corresponde. Cada máquina mantiene una caché con las direcciones traducidas para reducir el retardo y la carga. ARP permite a la dirección de Internet ser independiente de la dirección Ethernet, pero esto solo funciona si todas las máquinas lo soportan.

El **protocolo RARP** realiza la operación inversa. En Ethernet, la capa de enlace trabaja con direcciones físicas. El protocolo ARP se encarga de traducir las direcciones IP a direcciones MAC (direcciones físicas). Para realizar ésta conversión, el nivel de enlace utiliza las tablas ARP, cada interfaz tiene tanto una dirección IP como una dirección física MAC. **ARP** se utiliza en **4 casos** referentes a la comunicación entre 2 hosts:

- Cuando 2 hosts están en la misma red y uno quiere enviar un paquete a otro.
- Cuando 2 host están sobre redes diferentes y deben usar un gateway/router para alcanzar otro host.
- Cuando un router necesita enviar un paquete a un host a través de otro router.
- Cuando un router necesita enviar un paquete a un host de la misma red.

2.7.1.3 Protocolo DHCP: en inglés, *Dynamic Host Configuration Protocol*, es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

2.7.2 Capa de Transporte

2.7.2.1 *Protocolo TCP*: en español Protocolo de Control de Transmisión) es uno de los protocolos fundamentales en Internet.

Muchos programas dentro de una red de datos compuesta por ordenadores pueden usar TCP para crear conexiones entre ellos a través de las cuales enviarse un flujo de datos. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto. TCP da soporte a muchas de las aplicaciones más populares de Internet, incluidas HTTP, SMTP y SSH.

En la pila de protocolos TCP/IP, TCP es la capa intermedia entre el protocolo de Internet (IP) y la aplicación. Habitualmente, las aplicaciones necesitan que la comunicación sea fiable y, dado que la capa IP aporta un servicio de datagramas no fiable (sin confirmación), TCP añade las funciones necesarias para prestar un servicio que permita que la comunicación entre dos sistemas se efectúe: libre de errores, sin pérdidas y con seguridad.

2.7.2.2 Protocolo UDP: en inglés, *User Datagram Protocol*, es un protocolo del nivel de transporte basado en el intercambio de data gramas. Permite el envío de data gramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio data grama incorpora suficiente información de direccionamiento en su cabecera. Tampoco tiene confirmación, ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros; y tampoco se sabe si ha llegado correctamente, ya que no hay confirmación de entrega o de recepción. Su uso principal es para protocolos como DHCP, BOOTP, DNS y demás protocolos en los que el intercambio de paquetes de la conexión/desconexión son mayores, o no son rentables con respecto a la información transmitida, así como para la transmisión de audio y vídeo en tiempo real, donde no es posible realizar retransmisiones por los estrictos requisitos de retardo que se tiene en estos casos.

2.7.2.3 Protocolo SCTP: en inglés, *Stream Control Transmission Protocol*, es un protocolo de comunicación de capa de transporte. SCTP es una alternativa a los protocolos de transporte TCP y UDP pues provee confiabilidad, control de flujo y secuenciación como TCP. Sin embargo, SCTP opcionalmente permite el envío de mensajes fuera de orden y a diferencia de TCP, SCTP es un protocolo orientado al mensaje (similar al envío de data gramas UDP).

Las ventajas de SCTP son:

- Capacidad de Multihoming, en la cual uno (o dos) de los extremos de una asociación (conexión) pueden tener más de una dirección IP. Esto permite reaccionar en forma transparente ante fallas en la red.
- Entrega de los datos en trozos que forman parte de flujos independientes y paralelos —eliminando así el problema de *head of the line blocking* que sufre

TCP—

- Es capaz de seleccionar y monitorizar caminos, seleccionando un camino "primario" y verificando constantemente la conectividad de cada uno de los caminos alternativos.
- Mecanismos de validación y asentimiento como protección ante ataques por inundación, proveyendo notificación de trozos de datos duplicados o perdidos.

2.7.3 Capa de Aplicación

2.7.3.1 Telnet: en inglés *Telematics Networks*, es uno de los protocolos de nivel de aplicación de uso más extendido de TCP/IP y se trata de un protocolo simple de terminal remoto que permite establecer una conexión TCP entre un usuario y un servidor. El usuario realiza pulsaciones sobre el teclado del terminal, que son enviadas al servidor por la red, procesadas por éste; tras lo cual, se realiza el envío de nuevo al usuario del resultado de la ejecución de comandos, que aparece sobre la pantalla del terminal.

Una vez que se ha establecido la conexión Telnet, el usuario ejecutará los comandos y tendrá la sensación de que se encuentra delante del servidor. Por esta razón, los comandos que reconocer el protocolo Telnet son los mismos que se manejan en el sistema operativo del servidor.⁷

2.7.3.2 *Protocolo FTP*: en inglés, *File Transfer Protocol*, es un protocolo de transferencia de archivos entre sistemas conectados a una red TCP basado en la arquitectura cliente-servidor, de manera que desde un equipo cliente nos podemos conectar a un servidor para descargar archivos desde él o para enviarle nuestros

⁷ Telnet. FRANCISO JOSÉ MOLINA ROBLES. REdes de Área Local. Editorial AlfaOmega. MADRID, España

propios archivos independientemente del sistema operativo utilizado en cada equipo.

El Servicio FTP es ofrecido por la capa de Aplicación del modelo de capas de red TCP/IP al usuario, utilizando normalmente el puerto de red 20 y el 21. Un problema básico de FTP es que está pensado para ofrecer la máxima velocidad en la conexión, pero no la máxima seguridad, ya que todo el intercambio de información, desde el login y pass Word del usuario en el servidor hasta la transferencia de cualquier archivo, se realiza en texto plano sin ningún tipo de cifrado, con lo que un posible atacante lo tiene muy fácil para capturar este tráfico, acceder al servidor, o apropiarse de los archivos transferidos.

2.7.3.3 Protocolo SMTP: (*Simple Mail Transport Protocol o Protocolo Simple de Transporte de Correo*) está definido en el RFC 821 y es un protocolo muy sencillo que se utiliza para transferir mensajes de correo electrónico entre equipos en los que funciona un proceso residente SMTP. Este protocolo no es capaz por sí solo de almacenar el correo enviado a su posterior consulta por los usuarios. En realidad solamente está pensado para que los usuarios reciban el correo cuando se encuentran conectados al servidor (han iniciado una *sesión* en él) y no soporta ningún mecanismo de almacenamiento de correo.⁸

2.7.3.4 Protocolo DNS: (*Domain Name System o Sistema de Nombres de Dominio*) es un protocolo de la capa de aplicación que se encarga de convertir direcciones formadas por cadenas de caracteres ASCII (como, por ejemplo, *www.jccm.es*) en direcciones binarias de transporte. El protocolo DNS se define en los estándares RFC 1034 y 1035. Éste utiliza una base de datos distribuida por la

⁸ SMTP. ANDREW S. TANENDAUM. Redes de Computadoras. Tercera Edición. Editorial Pearson. Vrije Universiteit Amsterdam, The Netherlands. 1997

red en ordenadores llamados *servidores DNS*, que almacenan tablas de correspondencias entre direcciones de nombres de dominio y direcciones IP. Cuando una estación desea establecer una conexión con una dirección DNS, llama a la rutina del sistema o **resolvedor** que primero comprueba si puede obtener la dirección IP a través de una tabla local almacenada de forma temporal de una consulta anterior. Si no la encuentra en esa tabla, envía un mensaje UDP a la dirección del servidor DNS que tenga configurado por defecto (normalmente el más próximo). Este servidor consulta primero en sus registros de recursos de zona la dirección solicitada (en caso de ser un servidor primario o secundario) y devuelve la dirección IP si la encuentra. Si no la encuentra ahí, consultará entonces la tabla local donde están almacenadas temporalmente consultas anteriores. En caso de que tampoco la encuentre ahí, puede consultar otros servidores DNS, operación que se denomina **consulta recursiva**. Finalmente, el resolvedor devuelve la dirección IP solicitada a la estación.⁹

⁹ DNS. ANDREW S. TANENDAUM. Redes de Computadoras. Tercera Edición. Editorial Pearson. Vrije Universiteit Amsterdam, The Netherlands. 1997

2.7.3.5 Protocolo HTTP: El protocolo de transferencia de hipertexto (*HTTP, HyperText Transfer Protocol*) es el protocolo usado en cada transacción de la Web (WWW). HTTP define la sintaxis y la semántica que utilizan los elementos software de la arquitectura Web (clientes, servidores, proxies) para comunicarse. Es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor. Al cliente que efectúa la petición (un navegador o un spider) se lo conoce como "user agent" (agente del usuario). A la información transmitida se la llama recurso y se la identifica mediante un URL. Los recursos pueden ser archivos, el resultado de la ejecución de un programa, una consulta a una base de datos, la traducción automática de un documento, etc.

HTTP es un protocolo sin estado, es decir, que no guarda ninguna información sobre conexiones anteriores. El desarrollo de aplicaciones Web necesita frecuentemente mantener estado. Para esto se usan las cookies, que es información que un servidor puede almacenar en el sistema cliente. Esto le permite a las aplicaciones Web instituir la noción de "sesión", y también permite rastrear usuarios ya que las cookies pueden guardarse en el cliente por tiempo indeterminado.

2.8 LA ADMINISTRACIÓN DE REDES, ENFOQUE PARA LA EVALUACIÓN Y PRUEBAS DE REDES LAN

La administración de redes implica muchas áreas distintas, entre las cuales se incluye la documentación de las redes, el mantenimiento de las redes, la administración del servidor y el mantenimiento del servidor. Cada una de estas labores son importantes como el resto, y no hay que descuidar ninguna de estas. En esta sección se hará una explicación de cada uno de los componentes, y nos enfocaremos en la Documentación y el mantenimiento de las redes, que son los

temas que convergen con la elaboración de la Guía para ayudar al administrador a hacer una tarea completa de realización de pruebas de rendimiento de la red.

2.8.1 Documentación de Red: la documentación representa la memoria del administrador de red. Ante todo incluye el diario técnico y estos componentes: Diagramas de indican el trazado del cableado físico, el tipo de cable, la longitud del cable, el tipo de terminación del cable, la ubicación física de cada patch panel y un esquema de etiquetado para la fácil identificación de cada cable.

2.8.2 Distribuciones MDF e IDF: este documento contiene la distribución física y lógica del armario de distribución principal y de todos los armarios de distribución intermedias de la red. Incluye ka distribución física de los montajes de recintos, el equipo auxiliar y los servidores de utilidad de distribución.

2.8.3 Registros de Mantenimiento: es útil mantener una lista de todas las reparaciones que se hayan hecho en el equipamiento incluido en la red. Esto ayudará a predecir posibles problemas futuros con el hardware y el software existente.

2.8.4 Rendimiento de la red: es una medida de la rapidez y fiabilidad de red. Cada combinación de software y hardware de computadora, de red y de cableado tendrá un rendimiento de red diferente. Esto nos lleva a concluir que para saber si la red no está funcionando bien, tendremos que aplicar una medida con la que comparar el rendimiento. Esta medida se denomina Línea de Base. Un línea de base se establece cuando la red se ha instalado y configurado correctamente.

2.8.5 Control de red: una cuenta de inicio de sesión identifica el usuario de red ante el sistema de red. Esta cuenta, junto con la contraseña del usuario, identifica y da acceso a los recursos del sistema de red. Este ID de cuenta también hace al usuario responsable de sus acciones en la red. Esto se deberá declarar en los documentos de seguridad. El simple hecho de que un usuario de red tenga una cuenta no significa que los recursos de red estén a completa disposición de este usuario. Los derechos de usuario determinan la disponibilidad de los recursos de la red.

2.8.6 Control de tráfico: es el método más sofisticado de control de redes. Busca tráfico de paquetes en la red y genera informes basados en él. Estos programas conocidos como sniffers, no solo detectan los fallos del equipamiento, sino que también determinan si un componente está sobrecargado o pobremente configurado.

2.8.7 Solución de problemas de red: la solución de problemas de red es un proceso sistemático que se aplica con el fin de resolver los problemas de una red. Puede seguir los siguientes pasos:

Paso 1: identifique el problema de la red/usuario

Paso 2: reúna datos acerca del problema de red/usuario

Paso 3: analice los datos para aportar una solución posible al problema

Paso 4: implemente una solución a la red para intentar corregir el sistema

Paso 5: si el problema no se resuelve, deshaga los cambios anteriores y modifique los datos

Paso 6: vuelva al paso 3

En conclusión, la tarea principal de un administrador de red está basada en

consultar el estado de las redes de transmisión de datos en una red específica y desde ahí brindar y aplicar soluciones que mejoren el rendimiento de la misma.

Resumiendo diríamos que aplicaría pasos fundamentales como los siguientes:

- Documentación de la red
- Establecimiento de la Línea Base
- Monitoreo
- Corrección de errores

2.9 DESARROLLO DE LA GUÍA

Con base en el análisis realizado durante el proyecto y la experiencia del Caso Colegio Nuevo Cambridge los pasos propuestos en La Guía para la evaluación, mantenimiento y pruebas de rendimiento de red son:

- Documentación
- Establecimiento de la línea base
- Monitoreo
- Corrección de errores

La Guía plantea la combinación de estos pasos con el recorrido ascendente de las capas del modelo TCP/IP, dado que éste modelo en capas es ideal por su practicidad y fácil acople con las redes existentes en la actualidad.

Esta metodología se plantea en La Guía en la sección METODOLOGÍA PARA LA EVALUACIÓN Y PRUEBAS DE RENDIMIENTO DE REDES DE ÁREA LOCAL. El siguiente cuadro presenta un resumen de las actividades a realizar en cada paso de acuerdo a la capa del modelo TCP/IP:

Tabla 3. Metodología de la Guía

TCP/IP	Documentación → Montaje	Línea Base → Cuando sale en producción	Monitoreo → Periódicamente revisar el comportamiento	Corrección de errores → Eventualmente, cuando se presenta una falla
Acceso	<p>Para la documentación se requiere acceder a los registros como:</p> <ul style="list-style-type: none"> • MAC de las tarjetas y equipos periféricos • Mapa de distribución de la red en el edificio, especificando qué tipos de equipos se encuentran en cada punto • Acudir a la lista o historial de reparaciones y configuraciones que se han hecho en la red 	<p>En este paso tomamos nota y registramos para la documentación de la Red. Antes de todo, revisar la disponibilidad de ambiente o espacio en donde va a ser montada la red</p> <p>Centros de Cableado Distancia entre puntos y longitud de los cables Determinar la topología de la red y el esquema en la interconexión de los equipos Espacio disponible en cada rack</p>	<p>Revisión y mantenimiento periódico de los centros de cableado ITIL → Librería para gestión de tecnologías de información Certificación de puntos</p>	<p>Revisar las terminaciones de los cables, siempre y cuando vayan respetando las normas EIA/TIA-568A (T568A) y la EIA/TIA-568B (T568B) El deterioro o depreciación que puede sufrir una tarjeta interna de los equipos Verificar si hay algún dispositivo quemado o fundido Fallas de conexión Errores en las tablas de conmutación</p>
Internet – interred	<p>Direcciones IP Asignación de IP's (si es dinámica o estática) Procesos de enrutamiento, diseño (selección), configuración, mantenimiento y corrección de errores</p>	<p>Realizar la asignación de dirección IP, sea manual o automática → Registro Establecimiento de la seguridad de acceso a internet Medir el ancho de banda de navegación y distribución del recurso por la asignación de direcciones IP</p>	<p>Revisión periódica de documentos si el direccionamiento es estático Mantenimiento al servidor DHCP si es dinámico Revisión de tablas de enrutamiento, gateways y ACL estándar Hacer seguimiento del control de flujo por medio de herramientas software</p>	<p>El DHCP no entrega dirección Existe un DHCP intruso en la red Fallas de enrutamiento, algunas páginas navegan y otras no</p>
TCP – Transporte	<p>Clasificación de Usuarios Derechos de Usuarios Definición de Contraseñas</p>	<p>Lista de chequeo de los servicios → Plan de pruebas Resultado de las pruebas de</p>	<p>Analizadores de protocolos Configuración de MRTG Configuración y ejecución de</p>	<p>Modificar los modos de operación del tráfico para realizar mejoras en el</p>

TCP/IP	Documentación → Montaje	Línea Base → Cuando sale en producción	Monitoreo → Periódicamente revisar el comportamiento	Corrección de errores → Eventualmente, cuando se presenta una falla
	Soporte y configuración del cortafuegos	uso de los servicios	programas que miden la velocidad de la transmisión de los paquetes y con la frecuencia en que han sido enviados Manejo del protocolo SNMP	rendimiento de la red Servicios permitidos que no funcionan o viceversa Puertos activos con vulnerabilidades → Revisión periódica (escaneos de puertos nmap o vulnerabilidades snort o nessus)
Aplicación	Estadísticas de uso de los sistemas y servicios (buscar sistemas y servicios relevantes para la empresa y analizar sus registros de acceso (logs) Configuración de software especializado en recopilar información y envío de alertas cuando se presenta una falla	Configurar los servicios que estarán disponibles en la red Recopilar la información de los registros (logs) durante un mes para conocer el comportamiento normal		Navegación no funciona y la causa es el Proxy o el servicio web está caído, los servicios fallan por: Llena los discos duros Fallas de memoria o procesamiento Falla de energía y al reiniciar no arrancan La página muestra errores: No ha conexión a las fuentes de datos

Fuente: Autor del Proyecto

En la práctica documentación es importante que se tengan a la mano cada uno de los archivos de información de configuración que se recomiendan, ya que estos son los recursos que posiblemente le ayudarán a responderse preguntas como ¿qué ocasionó la falla en la red? y ¿qué cambios debo implementar para la mejora de la comunicación en la red de datos?

La practica establecimiento de la línea base debe realizarse en la primera ejecución de la red, junto con toda la documentación de configuración inicial, pues este es el punto de medida comparativa en la práctica de monitoreo y corrección de errores.

En la práctica de monitoreo se debe tener en cuenta, las herramientas software que ayudan a establecer la línea base, y nos permiten hacer un seguimiento de la red, y desde ahí poder saber cómo es su desempeño y si se deben hacer mejoras en el equipamiento o los servicios de la red. Para tal hecho se ha recomendado la herramienta Multi Router Traffic Grapher: MRTG.

2.9.1 MRTG: es una herramienta, escrita en C y Perl por Tobias Oetiker y Dave Rand, que se utiliza para supervisar la carga de tráfico de interfaces de red. MRTG genera un informe en formato HTML con gráficas que proveen una representación visual de la evolución del tráfico a lo largo del tiempo.

Para recolectar la información del tráfico del dispositivo (habitualmente routers) la herramienta utiliza el protocolo SNMP (Simple Network Management Protocol). Este protocolo proporciona la información en crudo de la cantidad de bytes que han pasado por ellos distinguiendo entre entrada y salida. Esta cantidad bruta deberá ser tratada adecuadamente para la generación de informes

También permite ejecutar cualquier tipo de aplicación en lugar de consultar un dispositivo SNMP. Esta aplicación proporciona como salida dos valores numéricos que se corresponden a la entrada y salida. Habitualmente suelen utilizarse scripts que monitorizan la máquina local.

Asimismo, proporciona una aplicación cfgmaker que genera la configuración para un router de forma automática utilizando la meta información que proporciona SNMP.¹⁰

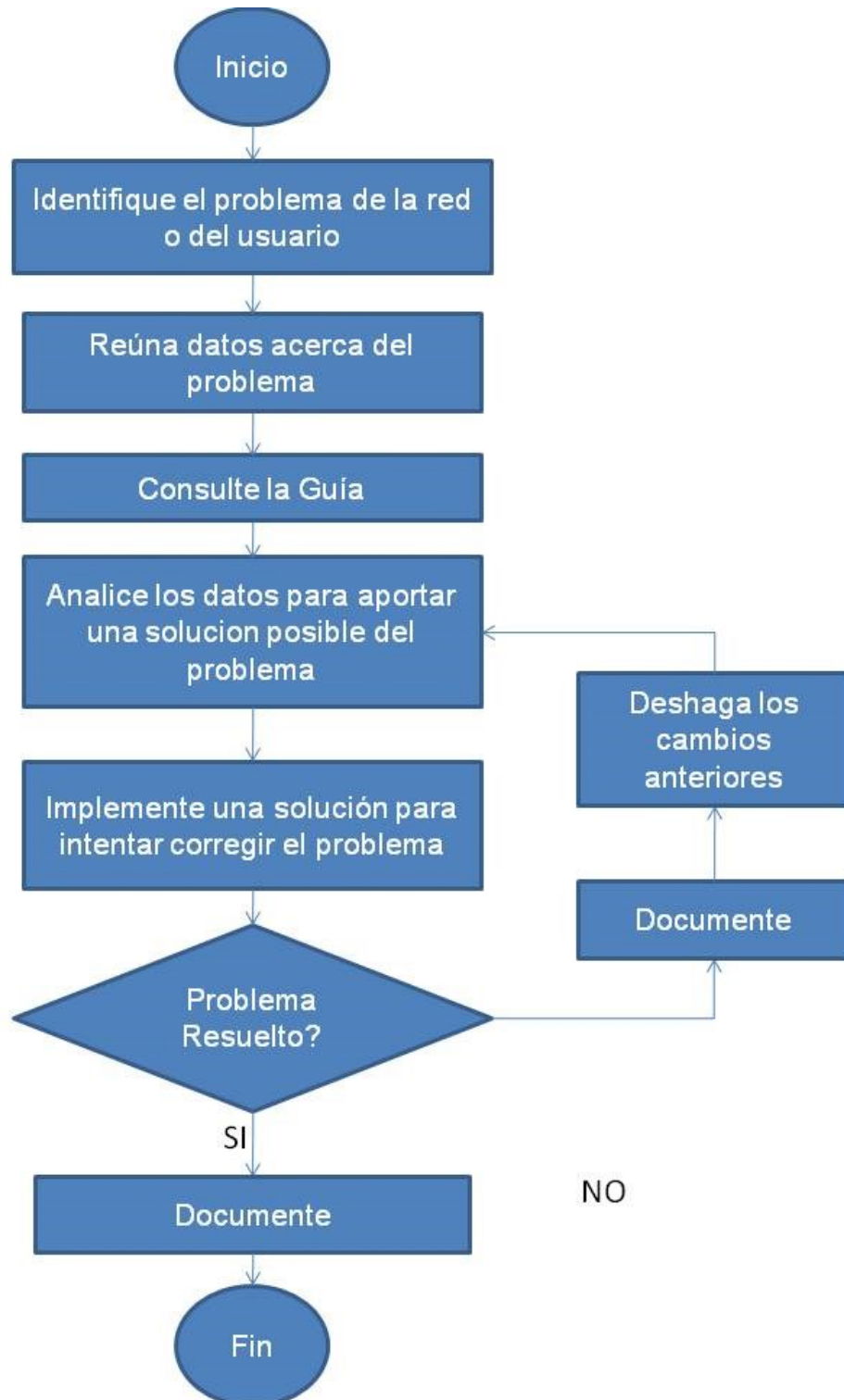
2.9.1.1 Funcionamiento de MRTG: MRTG ejecuta como un demonio o invocado desde las tareas programadas del cron. Por defecto, cada cinco minutos recolecta la información de los dispositivos y ejecuta los scripts que se le indican en la configuración.

En un primer momento, MRGT consultaba la información, la procesaba y generaba el informe y las gráficas. En las últimas versiones, esta información es almacenada en una base de datos gestionada por RRDtool a partir de la cual, y de forma separada, se generan los informes y las gráficas.

En la práctica Corrección de errores se puede resumir en el siguiente diagrama de procesos:

10 Definición de MRTG, Wikipedia, La Enciclopedia Libre. véase <http://es.wikipedia.org/wiki/MRTG>, también puede visitar la página oficial de MRTG: http://www.mrtg.jp/en/es_es/

Figura 5. Diagrama de Procesos para Corrección de Errores



Fuente: Autor del Proyecto

3. CASO DE ESTUDIO Y DE APLICACIÓN DE LA METODOLOGÍA DE LA GUÍA: COLEGIO NUEVO CAMBRIDGE

Los métodos de trabajo planteados en la Guía, son los aplicados al caso de estudio del Colegio Nuevo Cambridge, estos son descritos a continuación:

El Colegio Nuevo Cambridge está ubicado en la Calle 32 No. 22-140 Barrio Cañaveral, en la ciudad de Floridablanca, Santander.

Esta institución se ha caracterizado por su buen desempeño académico y aportes tecnológicos a funcionarios. Desde hace 10 años implementa su sistema de comunicación a partir de equipos tecnológicos y ha evolucionado según la necesidad del cliente. En la actualidad académicamente, utiliza el sistema de información Sophia, herramienta que es 100% Virtual, lo cual requiere de un buen desempeño de la red tanto privada como pública, ya que a partir de ahí los padres de familia hacen seguimiento del avance académico de sus hijos e interactúan con el colegio.

3.1 DOCUMENTACIÓN Y ESTABLECIMIENTO DE LA LÍNEA BASE

3.1.1 Capa de acceso

3.1.1.1 Esquema de la Red. La red de datos del colegio emplea tecnología Ethernet. Las conexiones constan básicamente de: Tarjeta de red con conector de hembra RJ-45, conector RJ-45, cable de par trenzado y concentrador. Adicionalmente, el esquema de comunicación de la red interna es Cliente-Servidor en la cual un PC cualquiera de la red hace la petición y el servidor contesta instantáneamente a la petición, así como la configuración

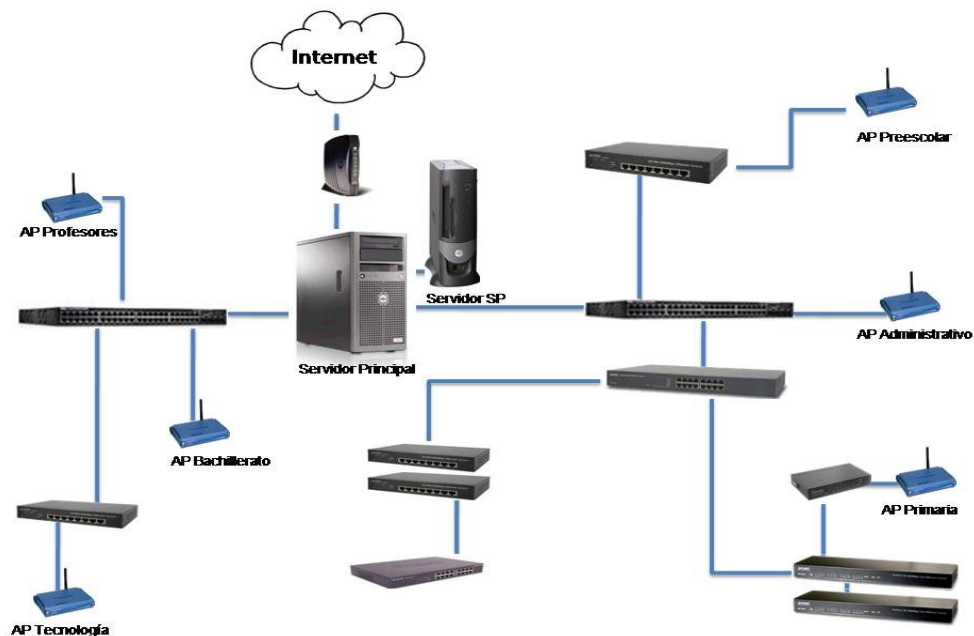
de archivos e impresoras compartidas.

La red tiene una velocidad de transmisión o Ancho de Banda para peticiones Internet de 2000Kbps, servicio que varía según el proveedor. La velocidad interna es la predeterminada 100Mbps, velocidad que varía según las perturbaciones que haya en la red.

3.1.1.2 Topología de la Red. La topología física de la red es Estrella, donde se utiliza un dispositivo como punto de conexión entre Internet y red local. Este dispositivo es el servidor de datos y software de la red. La colisión de datos es casi imposible, ya que cada estación tiene su propio cable, y es fácil ampliar la red.

El estado actual de la topología física de la red del Colegio Nuevo Cambridge, se describe a continuación:

Figura 6. Distribución topológica de la Red del Colegio Nuevo Cambridge



Fuente: Elaborada por el Autor

3.1.1.3 Distribución de la Red – Mapa de Centros de Cableado y Ubicación

de Equipos. La estructura física y distribución de equipos del Colegio Nuevo Cambridge se muestra en el siguiente plano de espacios del colegio.

Figura 7. Distribución de Centros de Cableado y Equipos. Piso 1

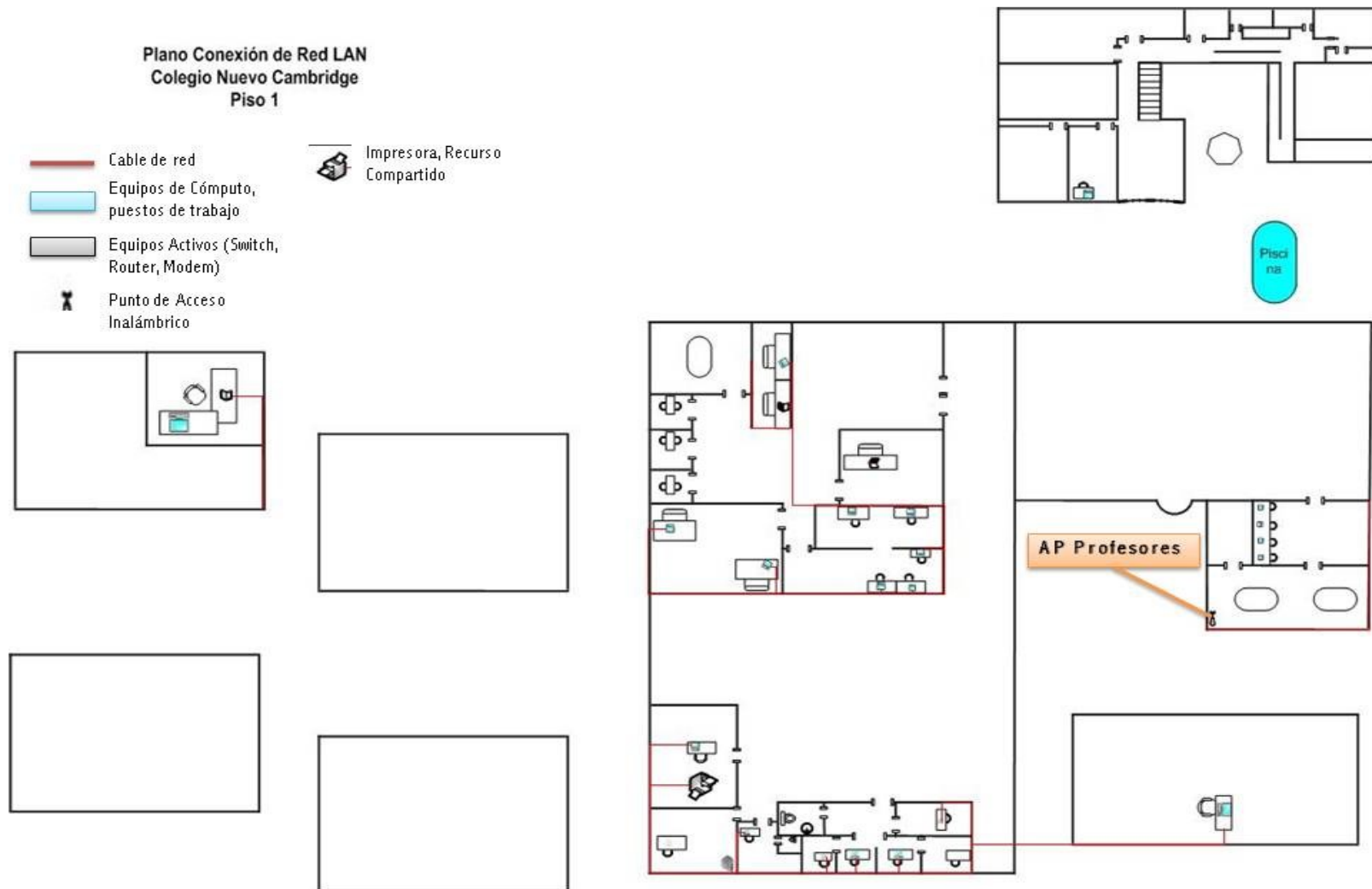


Figura 8. Distribución de Centros de Cableado y Equipos. Piso 2

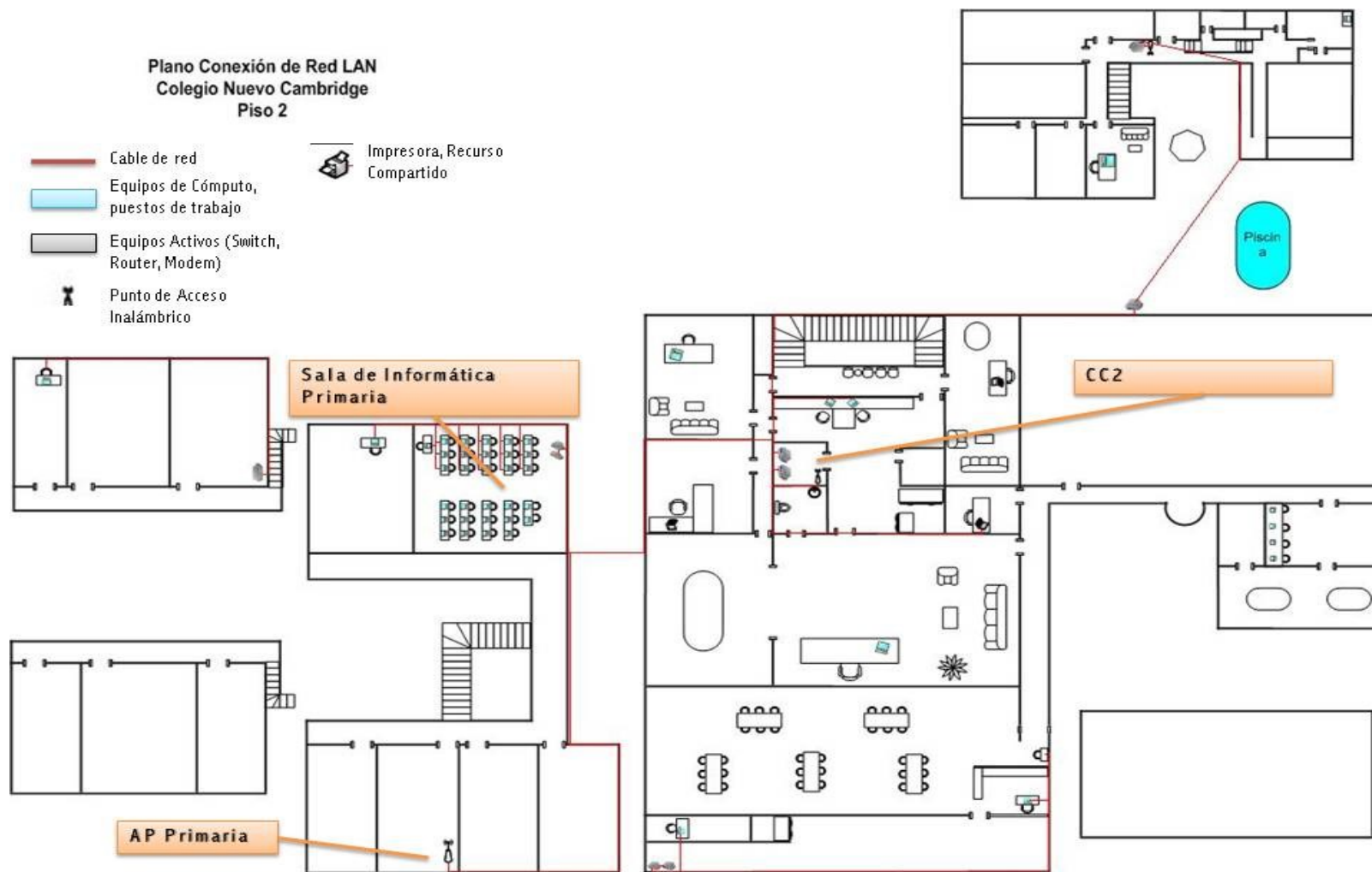


Figura 9. Distribución de Centros de Cableado y Equipos. Piso 3

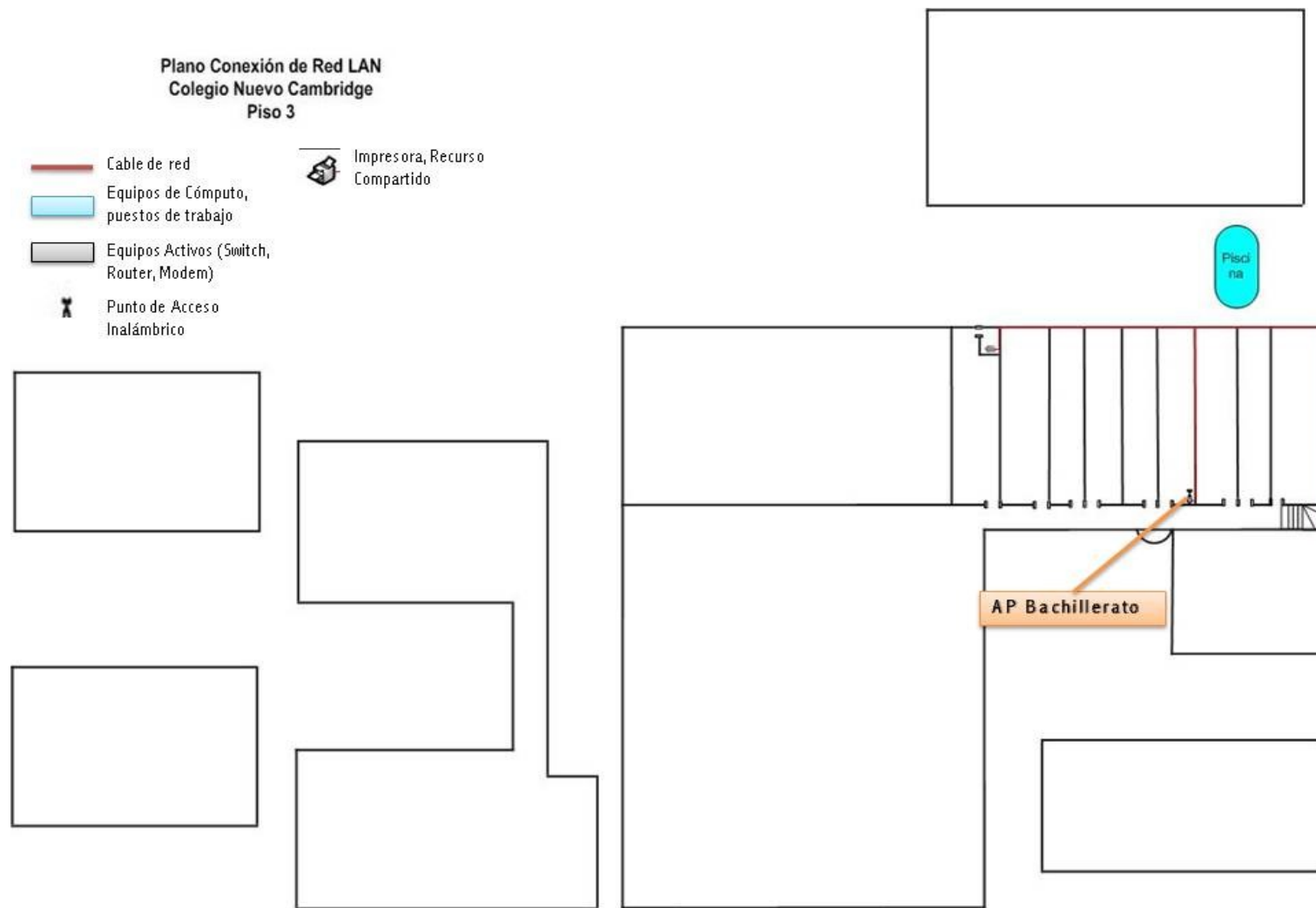
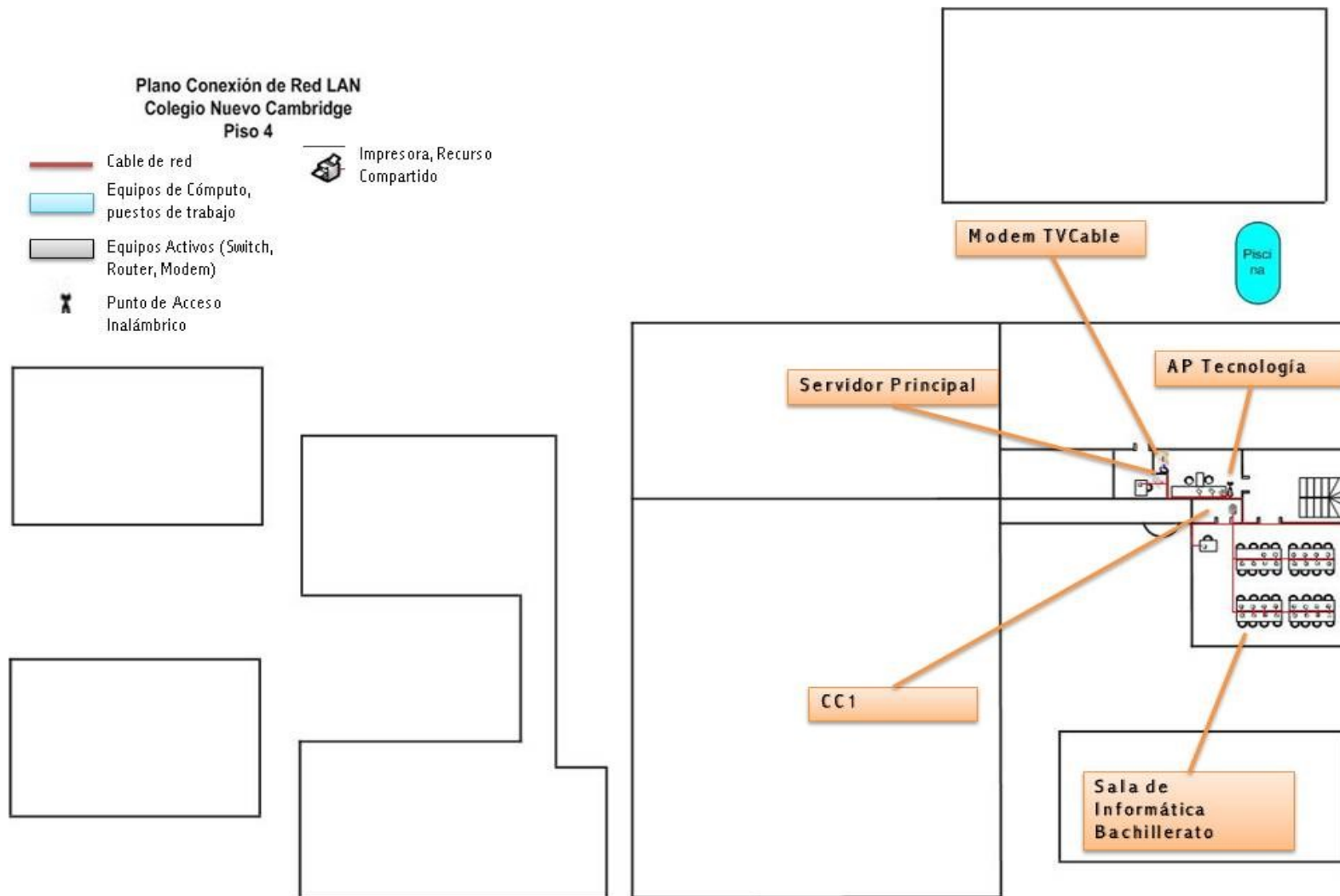


Figura 10. Distribución de Centros de Cableado y Equipos. Piso 4



3.1.1.4 Equipos Activos. En la siguiente tabla se muestra el inventario de equipos activos o de intercomunicación de la red junto con su ubicación, se tiene un total de 20 equipos de los cuales 9 son switches (2 administrables marca Dell), 2 servidores Dell, 3 Hub y 6 Access Point.

Tabla 4. Equipos Activos

Marca	Tipo Equipo	Ubicación	Dirección IP ¹¹
Dell Power Connect 6248	Switch 48	Sala Bachillerato	10.1.1.100
Dell Power Connect 6248	Switch 48	Edificio Administrativo	
Planet FSD-800	Switch 8	Biblioteca	
Planet FSD-800	Switch 8	Biblioteca	
Soho Connect by Planet	Hub 8	Área Tecnología	
LG LS3116A	Switch 16	Cuarto Servicio Piso 3	
LG LS3116A	Switch 16	Fonoaudiología	
Soho Connect by Planet	Hub 8	Primaria Bloque 2	
Planet	Hub 32	Sala Primaria	
Planet FNSW-1601	Switch 16	Sala Primaria	
QPcom QP308R	Switch 8	Preescolar Piso 1	
Planet	Switch 32	Edificio Administrativo	
TRENDNet	AP	Bachillerato piso3	10.1.1.90
TRENDNet	AP	Edificio	10.1.1.80

¹¹ La lista de direcciones IP no es real, ha sido modificada para seguridad del Colegio

		Administrativo	
TRENDNet	AP	Primaria	10.1.1.110
TRENDNet	AP	Preescolar	10.1.1.112
TRENDNet	AP	Área Tecnología	10.1.1.124
TRENDNet	AP	Sala Profesores	10.1.1.222
DELL Optiplex GX250	PC/SchoolPack	Área de Tecnología	10.1.1.87
DELL PowerEdge 840	PC/Servidor	Área de Tecnología	10.1.1.56

Fuente: Elaborado por el Autor

Las características del servidor principal y SP (School Pack) son las siguientes:

Tabla 5. Características del Servidor Principal y School Pack

	SERVIDOR SP	SERVIDOR PRINCIPAL
Físicas	DELL Optiplex GX250; Procesador Pentium 4 2.40 GHz; Cisco Duro 20 GB, RAM 512 MB	DELL PowerEdge 840 Procesador Xenon, RAM 4GB; Dos Discos duros de 250 GB;
Logicas	School Pack, base de datos Académica hasta Mayo 2008	Servicio Web, Proxy, Restricción de Páginas, Base de Datos Actual – Sophia, Distribución del Ancho de Banda según Jerarquía de IP. IP: 1-240 Max; 240 en adelante: distribuida. Acceso a ficheros compartidos con restricciones según perfil de

		usuario.
--	--	----------

Fuente: Elaborado por el Autor

La distribución de los equipos junto con sus vecinos se puede observar claramente en la siguiente figura:

3.1.2 Capa Interred

3.1.2.1 Asignación y Recopilación de Direcciones IP. Actualmente, hay 150 computadores de escritorio permanentes, y un número aproximado de 50 portátiles que se conectan a la red inalámbrica. La asignación de direcciones IP es estática, la red es Clase C 10.1.1.0, red privada. La dirección pública a internet desde el servidor es 200.114.0.11/24.

Por cuestiones de privacidad, la lista de direcciones IP del Colegio Nuevo Cambridge no se encuentra disponible en este documento. Esto con el fin de respetar las políticas de seguridad de la Institución.

3.1.2.2 Ancho de Banda. El Colegio Nuevo Cambridge tiene un canal de conexión a Internet brindado por el proveedor TV Cable – UNE, con un ancho de banda de 2Mbps. Este ancho de banda es distribuido por el servidor a los equipos activos de la siguiente manera:

Tabla 6. Distribución del Ancho de Banda Colegio Nuevo Cambridge

Rango	Velocidad de Transmisión
10.1.1.1- 10.1.1.199	<300Kbps
10.1.1. 200 - 10.1.1.239	200Kps-600Kbps
10.1.1.240 – 10.1.1.254	500Kbps-1000Kbps

Fuente: Autor de la Guía

3.2 MONITOREO

3.2.1 Capa de Interred, Transporte y Aplicación. Dentro de una red es importante llevar un monitoreo de tráfico, este seguimiento permite ayudar a detectar fallas, así como también medir el uso de la red para poder hacer previsiones y tomar medidas de seguridad y calidad.

3.2.1.1 Configuración de MRTG y SNMP. MRTG – Multi Router Traffic Grapher, es un programa de Código Abierto (disponible en <http://www.mrtg.org/>) que se puede implementar sobre Sistemas Operativos UNIX (más común) y Windows para realizar graficas del tráfico con un tiempo de muestreo de mínimo 5 minutos en el modo normal usando diferentes fuentes de datos, pero generalmente se utiliza el protocolo SNMP.

MRTG se usa para monitorear variada cantidad de parámetros. MRTG también se usa para verificar diferentes parámetros como la carga de CPU, uso de memoria, cantidad de procesos en ejecución, etc. Hasta se llega a monitorear el tráfico generado por los correos del sistema, ¿cuántos son virus?, ¿cuántos spam?, ¿cuántos mails?

En el caso del Colegio Nuevo Cambridge, se usó la herramienta MRTG para una de sus concepciones iniciales, que es el graficar el uso de la red.

El análisis de tráfico se hace en el servidor y el switch ubicado en la sala de bachillerato del Colegio. La configuración de MRTG y SNMP para cada uno se hace de la siguiente manera:

- Configuración en el Servidor

El servidor sirve como recepcionista de la lectura de tráfico de cada una de sus interfaces y del mismo modo de la lectura de tráfico generado por el switch y cada una de sus interfaces.

Teniendo en cuenta que el servidor es con sistema operativo Fedora, se inicia sesión de administrador (root), desde la terminal y se ejecuta el comando

```
#yum install mrtg           →instalar MRTG
#yum install snmp           →instalar SNMP
#yum install net-snmp       →instalar SNMP -net
#yum install net-snmp-perl  →instalar SNMP-perl
```

- Configuración de SNMP

El SNMP o Simple Network Management Protocol es un protocolo de red concebido con la idea de poder administrar un servidor, ya sea para cambiar parámetros o emitirle órdenes como para poder obtener datos informativos del servidor como su comportamiento actual, carga y uso de las interfaces de red. Por defecto el SNMP viene desconfigurado, ya que tiene una severa deficiencia por defecto, por lo tanto es recomendable guardar una copia del archivo original de configuración de SNMP, ubicado en el directorio `/etc/snmp/snmpd.conf`

```
# cd /etc/snmp
# cp snmpd.conf snmpd.conf.viejo
```

Ahora, se crea o modifica el archivo `snmp.conf` de la siguiente manera:

```

→Listas de control de acceso (ACL)
## sec.name source community (alias clave de acceso)
com2sec local 127.0.0.1/32 C14v3-d3-Acc3s0
com2sec miredlocal 192.168.1.0/24 C14v3-d3-Acc3s0
com2sec micueva 192.168.1.254 C14v3-d3-Acc3s0

→Se asigna ACL al grupo de lectura escritura
group MyRWGroup v1 local
group MyRWGroup v2c local
group MyRWGroup usm local

→Se asigna ACL al grupo de solo lectura
group MyROGroup v1 miredlocal
group MyROGroup v2c miredlocal
group MyROGroup usm miredlocal

group otrogrupo v1 local
group otrogrupo v2c local
group otrogrupo usm local

→Ramas MIB que se permiten ver
## name incl/excl subtree mask(optional)
view all included .180

→Establece permisos de lectura y escritura
## group context sec.model sec.level prefix read write
notif
access MyROGroup "" any noauth exact all none none
access MyRWGroup "" any noauth exact all all all
access otrogrupo "" any noauth exact all none none

→ Información de Contacto del Sistema
syslocation Administrador
syscontact Administrador (chocolatica@msn.com)

```

Luego, se reinicia el servicio snmp de la siguiente manera

```

#service snmpd stop
#service snmp start

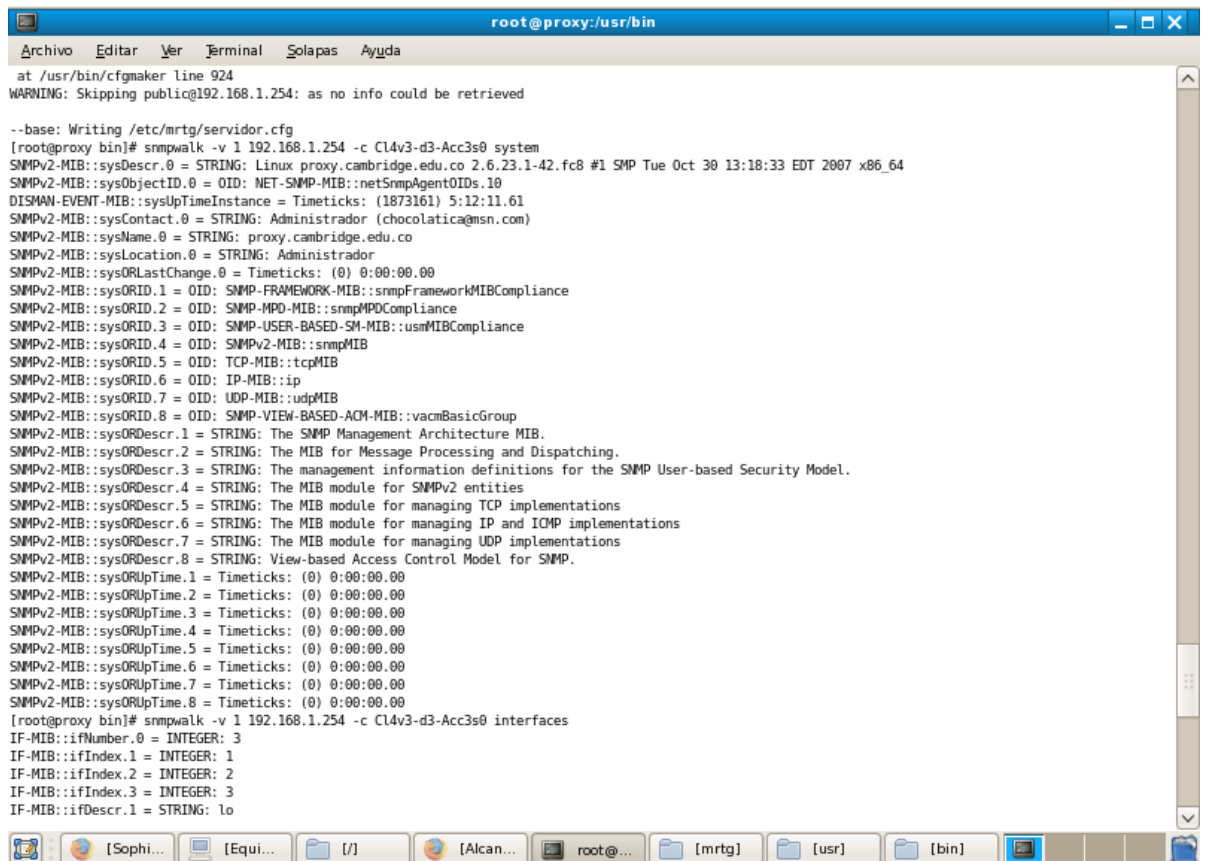
```

Para mirar si la configuración fue correcta, se ejecuta el siguiente comando

```
# snmpwalk -v 192.168.1.254 -c C14v3-d3-Acc3s0 system
```

Donde 192.168.1.254 es la dirección de red del servidor. La siguiente figura muestra la ejecución del comando y cómo responde SNMP ante la petición.

Figura 12. Ejecución de SNMP



```
root@proxy:usr/bin
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
at /usr/bin/cfgmaker line 924
WARNING: Skipping public@192.168.1.254: as no info could be retrieved

--base: Writing /etc/mrtg/servidor.cfg
[root@proxy bin]# snmpwalk -v 1 192.168.1.254 -c C14v3-d3-Acc3s0 system
SNMPv2-MIB::sysDescr.0 = STRING: Linux proxy.cambridge.edu.co 2.6.23.1-42.fc8 #1 SMP Tue Oct 30 13:18:33 EDT 2007 x86_64
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSmpAgentOIDs.10
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (1873161) 5:12:11.61
SNMPv2-MIB::sysContact.0 = STRING: Administrador (chocolatica@msn.com)
SNMPv2-MIB::sysName.0 = STRING: proxy.cambridge.edu.co
SNMPv2-MIB::sysLocation.0 = STRING: Administrador
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORID.1 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance
SNMPv2-MIB::sysORID.2 = OID: SNMP-MPD-MIB::snmpMPCCompliance
SNMPv2-MIB::sysORID.3 = OID: SNMP-USER-BASED-SM-MIB::usnMIBCompliance
SNMPv2-MIB::sysORID.4 = OID: SNMPv2-MIB::snmpMIB
SNMPv2-MIB::sysORID.5 = OID: TCP-MIB::tcpMIB
SNMPv2-MIB::sysORID.6 = OID: IP-MIB::ip
SNMPv2-MIB::sysORID.7 = OID: UDP-MIB::udpMIB
SNMPv2-MIB::sysORID.8 = OID: SNMP-VIEW-BASED-ACM-MIB::vacmBasicGroup
SNMPv2-MIB::sysORDescr.1 = STRING: The SNMP Management Architecture MIB.
SNMPv2-MIB::sysORDescr.2 = STRING: The MIB for Message Processing and Dispatching.
SNMPv2-MIB::sysORDescr.3 = STRING: The management information definitions for the SNMP User-based Security Model.
SNMPv2-MIB::sysORDescr.4 = STRING: The MIB module for SNMPv2 entities
SNMPv2-MIB::sysORDescr.5 = STRING: The MIB module for managing TCP implementations
SNMPv2-MIB::sysORDescr.6 = STRING: The MIB module for managing IP and ICMP implementations
SNMPv2-MIB::sysORDescr.7 = STRING: The MIB module for managing UDP implementations
SNMPv2-MIB::sysORDescr.8 = STRING: View-based Access Control Model for SNMP.
SNMPv2-MIB::sysORUpTime.1 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORUpTime.2 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORUpTime.3 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORUpTime.4 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORUpTime.5 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORUpTime.6 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORUpTime.7 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORUpTime.8 = Timeticks: (0) 0:00:00.00
[root@proxy bin]# snmpwalk -v 1 192.168.1.254 -c C14v3-d3-Acc3s0 interfaces
IF-MIB::ifNumber.0 = INTEGER: 3
IF-MIB::ifIndex.1 = INTEGER: 1
IF-MIB::ifIndex.2 = INTEGER: 2
IF-MIB::ifIndex.3 = INTEGER: 3
IF-MIB::ifDescr.1 = STRING: lo
```

Fuente: Autor de la Guía

La figura anterior también muestra la información de la versión de SNMP que se está usando, en este caso la versión de SNMP es 2 y se concluye que el sistema está listo para empezar a leer el comportamiento de la red.

Después de configurado SNMP se procede a la configuración de MRTG para que muestre de manera amigable lo que está enviando el SNMP.

```
# cfgmaker --global "Workdir: /var/www/html/mrtg/servidor" -  
output /etc/mrtg/servidor.cfg Cl4v3-d3-Acc3s0@192.168.1.254
```

- Configuración de SNMP en el switch DELL ubicado en el salón Bachillerato

Para este proceso es necesario acudir al manual de usuario correspondiente al modelo del equipo (disponible en <http://www.dell.com.co>) y se asigna una contraseña y usuario para configuración.

En esta primera figura se observa la interfaz del sistema de configuración del switch. Para empezar se busca la opción SNMP, y se coloca el nombre de la comunidad de acceso, que debe ser la misma del servidor para que envíe la información al servidor y éste a partir del MRTG la muestre en archivos HTML.

Figura 13. Configuración de la Comunidad en el Switch DELL

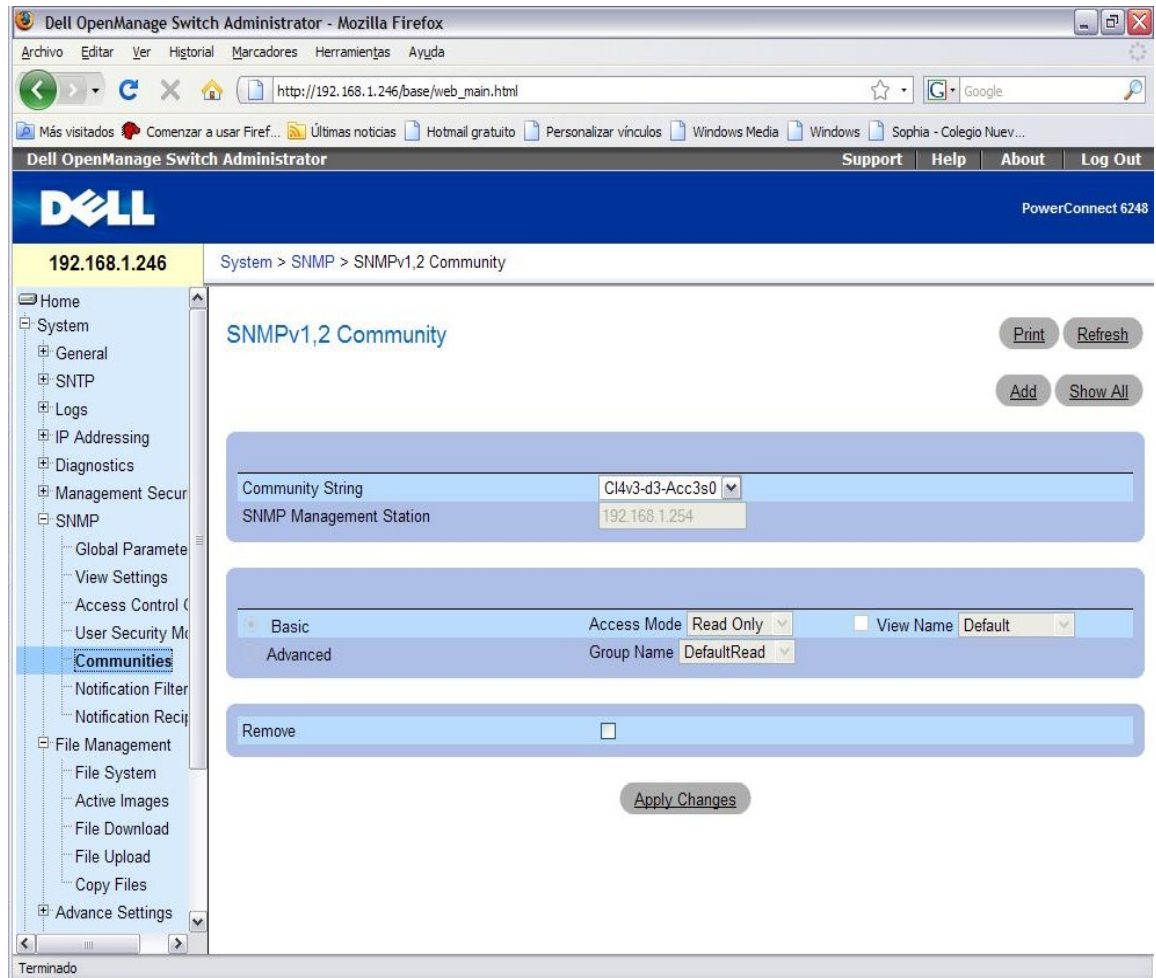
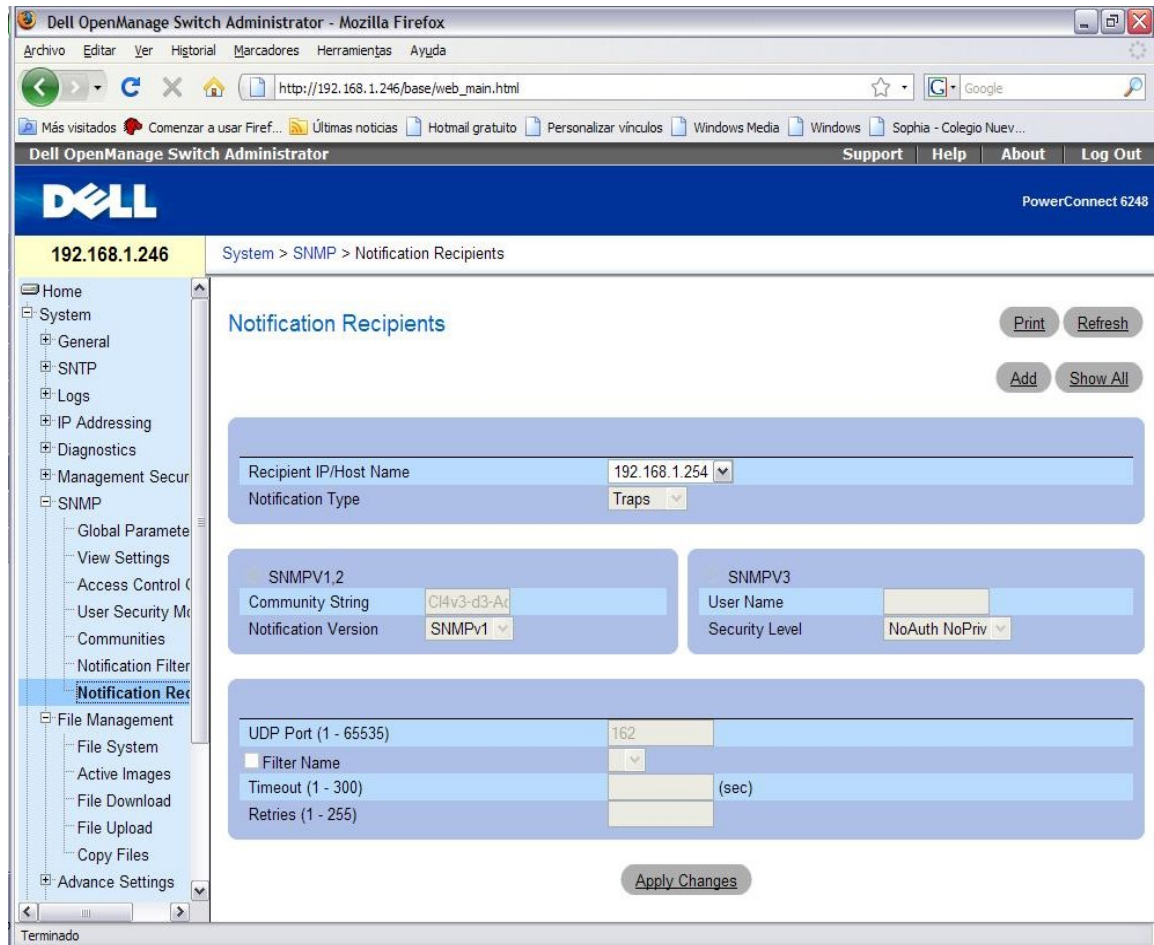


Figura 14. Configuración de envío de la lectura de SNMP al Servidor



En el servidor se coloca la configuración correspondiente para la creación de la página HTML a partir de MRTG, de la siguiente forma

```
# cfgmaker --global "Workdir: /var/www/html/mrtg/switch1" -  
output /etc/mrtg/switch1.cfg C14v3-d3-Acc3s0@192.168.1.246
```

Ahora, se procede a enviar la información al archivo `.cfg` para que MRTG actualice las graficas

```
# env LANG=C mrtg /etc/mrtg/servidor.cfg  
# env LANG=C mrtg /etc/mrtg/switch1.cfg
```

Reinicie Apache a fin de cargar la configuración que permitirá acceder hacia los reportes de MRTG a través de éste.

```
# service httpd restart
```

Puede mirar con algún navegador los resultados actuales del monitoreo del servidor en <http://200.114.0.11/mrtg/servidor/servidor.html> ó del switch en <http://200.114.0.11/mrtg/swith1/swith1.html>

4. CONCLUSIONES

- Después de realizar una encuesta, observación y consulta a material bibliográfico e Internet, se dedujo que la documentación, establecimiento de línea base, monitoreo y corrección de errores son las mejores prácticas que debe tener en cuenta un administrador de red para la evaluación y pruebas de rendimiento en redes LAN.
- Con la lectura de las gráficas MRTG en el caso de la red del Colegio, se puede decir que el horario de consumo de la red es de 6am a 7pm, y en este mismo rango se puede observar que entre la 1pm - 2pm y 3pm-7pm el consumo del ancho de banda baja debido a en esas horas sólo trabajan equipos del personal administrativos.
- Seguir la metodología planteada en la Guía en la red del Colegio Nuevo Cambridge, fue mutuamente benéfico porque por una parte permitió organizar la información de la red y entregar una herramienta de monitoreo al Colegio y por otra afinar los pasos planteados en La Guía de manera que se ajustaran a un caso real.
- Para visualizar el consumo de ancho de banda, la Guía hace uso de la herramienta de apoyo MRTG, software que fue configurado y ejecutado en el caso del Colegio Nuevo Cambridge para tomar decisiones con base a los resultados obtenidos. Esta herramienta está disponible para que el administrador del Cambridge pueda hacer programación de mantenimientos en horas de menos consumo, verificar el uso adecuado de los recursos y tener una idea de crecimiento de la red de acuerdo al consumo de tráfico.

- El proveedor de Internet TV Cable/Une le permite al Colegio tener ráfagas de consumo, dejando que la red en instantes pueda tener un tráfico mayor al ancho de banda contratado.

- Es importante resaltar que en la actualidad se cuenta con programas de software libre y propietario que permiten controlar y monitorear servicios adicionales. En este caso se trabajó únicamente con el MRTG, la elección del sistema dependerá de las necesidades específicas de cada empresa.

BIBLIOGRAFÍA

JIM DOHERTY Y NEIL ANDERSON. (2006). *Redes Locales*. España: Ediciones Anaya Multimedia (Grupo Anaya S.A).

MAGEDANZ, T. S. (Dic 1996). *Journal of Networks and Systems Management* (Vol. Volumen 4).

MARECOS, P. D. (Septiembre 2001). CONCEPTOS CLAVES ACERCA DE LA SALUD. *Revista de Posgrado de la Cátedra VIa Medicina N°* 108 , 17 - 19.

OLIFER, N. (2009). *Redes de Computadoras: principio, tecnología y protocolos para el diseño de redes*. Mexico: McGraw-Hill.

ROBLES, F. J. (2004). *Redes de Área Local*. México: Alfaomega Drupo Editor S.A de C.V.

SYSTEMS, A. D. (2004). *Guía del primer año: CCNA 1 y 2* (Vol. Tercera Edición). Madrid: Pearson Educación.

SYSTEMS, A. D. (2002). *Guía del segundo año* (Vol. Segunda Edición). Madrid: Pearson Educación.

TANENBAUM, A. S. (1997). *Redes de Computadoras* (Vol. Tercera Edición). (D. M. Peake, Trans.) Mexico: Pearson.

TOBIAS OETIKER Y DAVE RAND . (n.d.). *MRTG - Multi Router Traffic Grapher*. Retrieved from http://www.mrtg.jp/en/es_es/

WIKIPEDIA. (N.D.). Retrieved from <http://es.wikipedia.org>

ANEXO D

ENCUESTA A ADMINISTRADORES DE RED

Nombre: _____

Cargo: _____

NOTA: Por favor escoger la opción que más se asemeja a su labor como administrador de red. Si el documento es entregado vía e-mail, por favor responder al correo: eromero2@unab.edu.co, y la opción correspondiente en color Rojo.

Gracias.

1.- ¿Con qué periodo realiza una gestión de los elementos (infraestructura y servicios) de una red?

- | | |
|--|---|
| <input type="checkbox"/> Diario | <input type="checkbox"/> Cada 2 a 3 semanas |
| <input type="checkbox"/> Cada 2 a 4 días | <input type="checkbox"/> Mensual |
| <input type="checkbox"/> Semanal3 | <input type="checkbox"/> Semestral o Anual |

2.- ¿Qué herramienta(s) software utiliza para llevar documentación de la distribución física (topología) de su red?

- | | |
|--|--------------------------------------|
| <input type="checkbox"/> Packet Tracer | <input type="checkbox"/> COMNET III™ |
| <input type="checkbox"/> FLAN (F- Links And Nodes) | <input type="checkbox"/> NCTUns |
| <input type="checkbox"/> Kiva | <input type="checkbox"/> Visio |
| <input type="checkbox"/> NS (Network Simulator) | |
| <input type="checkbox"/> Otro. ¿Cuál? _____ | |

3.- ¿Implementa como primer paso, la creación de una línea base (punto de partida) de la red, que le permita deducir efectos en los cambios y posteriores soluciones de la red?

- Si
 No
 No lo conozco

¿Porque?

4.- Seleccione el (los) tipo(s) software para administración de red que manipula para su red: Software De Administración De Soluciones De Red

Administración De Servicios De la Red

Analizador De Protocolos

Analizador De Trafico

Topología De La Red9

Análisis De Ancho De Banda

Analizador De Cables

Otros... ¿Cuales? _____

5.- Maneja algún método sugerido por cisco para la solución de problemas como:

Recorrido niveles del Modelo OSI, del Físico al Aplicación (↑)

Recorrido niveles del Modelo OSI de Aplicación a Físico (↓)

Divide y Vencerás. Dividir niveles del Modelo OSI (↕)

No los Conozco

Aplico un método creado a mi criterio. ¿Cuál? _____

6.- ¿Qué acción(es) realiza frecuentemente como un método de localización del problema, para luego aislarlo y disminuir el rango de posibilidades de deterioro en la red?

Recolección de Síntomas

Acceso al Historial de Reparaciones

Preguntar a usuarios

Aplicar un software de Evaluación de Estado de la Red

Reevaluar cada paso del montaje de la Red (distribución, documentación, etc)

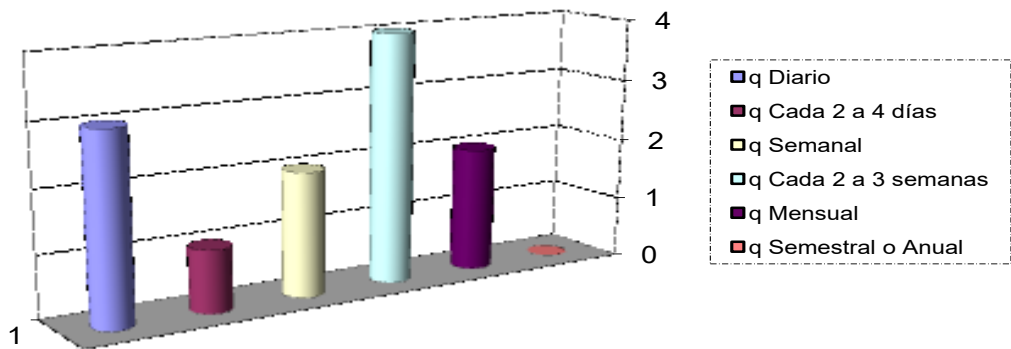
Otro ¿Cuál? _____

*Realizado por:
Verónica Romero Cruz
Estudiante Décimo Semestre
Facultad de Ingeniería de Sistemas
UNAB*

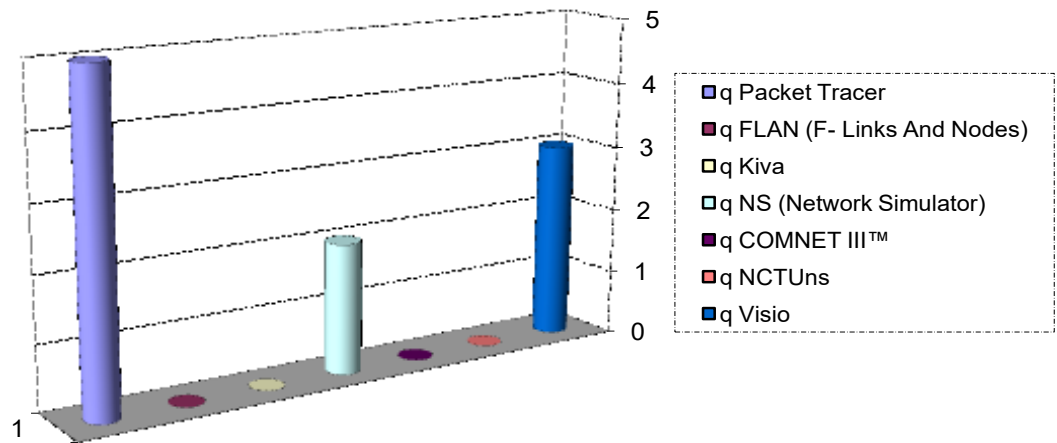
ANEXO E

TABULACIÓN Y REPRESENTACIÓN GRÁFICA DE ENCUESTA REALIZADA A ADMINISTRADORES DE RED

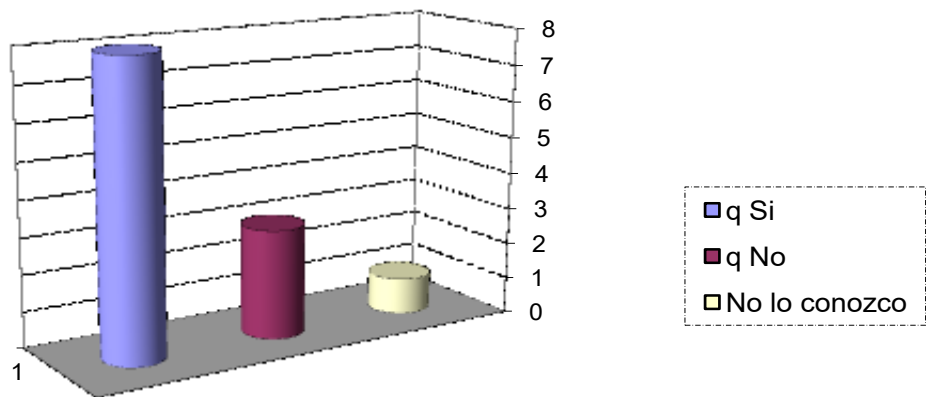
1.- ¿Con qué periodo realiza una gestión de los elementos (infraestructura y servicios) de una red?



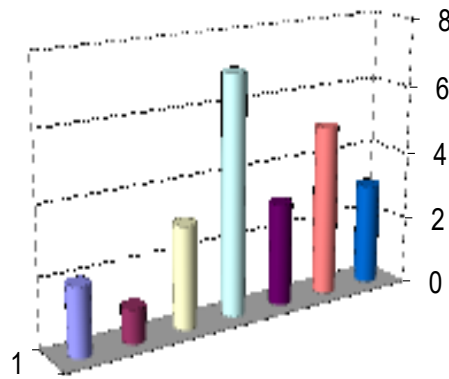
2.- ¿Qué herramienta(s) software utiliza para llevar documentación de la distribución física (topología) de su red?



3.- ¿Implementa como primer paso, la creación de una línea base (punto de partida) de la red, que le permita deducir efectos en los cambios y posteriores soluciones de la red?

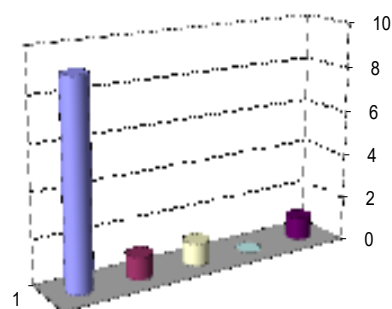


4.- Seleccione el (los) tipo(s) software para administración de red que manipula para su red:



- Software De Administración De Soluciones De Red
- Administración De Servicios De la Red
- Analizador De Protocolos
- Analizador De Trafico
- Topología De La Red
- Análisis De Ancho De Banda
- Analizador De Cables

5.- Maneja algún método sugerido por cisco para la solución de problemas como:



- Recorrido niveles del Modelo OSI, del Físico al Aplicación (↑)
- Recorrido niveles del Modelo OSI de Aplicación a Físico (↓)
- Divide y Vencerás. Dividir niveles del Modelo OSI (↑)
- No los Conozco
- Aplico un método creado a mi criterio.

6.- ¿Qué acción(es) realiza frecuentemente como un método de localización del problema, para luego aislarlo y disminuir el rango de posibilidades de deterioro en la red?

