ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ESTUDIO Y DESARROLLO DE UNA METODOLOGÍA PARA LA IMPLEMENTACIÓN DE UN MODELO DE GESTIÓN Y ADMINISTRACIÓN DE RED PARA LA UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO (UTEQ)

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN

OLGA ALEXANDRA ROSERO VLASOVA

(olga_vlassova@hotmail.com)

DIEGO ALEJANDRO PROAÑO SARASTI

(diegol2_ok@hotmail.com)

DIRECTOR: MSc XAVIER CALDERON
(xavieralex_calderon@hotmail.com)

Quito, Julio de 2009

DECLARACIÓN

Nosotros, Olga Alexandra Rosero Vlasova y Diego Alejandro Proaño Sarasti, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Olga Alexandra Rosero Vlasova Diego Alejandro Proaño Sarasti

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por la Señorita Olga Alexandra Rosero Vlasova y el Señor Diego Alejandro Proaño Sarasti, bajo mi supervisión

MSc Xavier Calderón
DIRECTOR DEL PROYECTO

AGRADECIMIENTO

Nuestro especial agradecimiento al Ingeniero Xavier Calderón por su acertada labor en la dirección de este proyecto, así como por su constante apoyo y preocupación.

A los ingenieros y personal administrativo de la Universidad Técnica Estatal de Quevedo por brindarnos todas las facilidades y por toda la ayuda prestada para culminar con éxito este proyecto.

A todas aquellas personas que de una u otra forma colaboraron durante el desarrollo de este trabajo.

Olga Alexandra Rosero Vlasova
Diego Alejandro Proaño Sarasti

DEDICATORIA

Este trabajo lo dedico sobre todo a mi mamá que es la persona más importante en mi vida, y a Andrés por haberme brindado el apoyo en todo momento y ayudarme a alcanzar mis metas.

También a mis amigas de toda la vida Graciela, Lency y Gisella, por sus consejos y cariño.

Olga Rosero

DEDICATORIA

Este proyecto lo dedico a Dios por haberme brindado la fuerza necesaria para culminarlos.

A mi mamá por ser mi guía, mi ejemplo, quien ha sido la persona más importante y a la cual le debo haber alcanzado todos mis anhelos.

A mis abuelitos por ser mis segundos padres y poder dedicarles este triunfo con todo mi corazón.

A mi tío Santiago, Darío y Oswaldo, quienes desde pequeño han sido mis padres, mis tutores, mis hermanos y mis amigos, les debo mucho.

A Gabriela, que en los momentos difíciles ha sido mi apoyo, mi sostén y quien a pesar del tiempo me ha colaborado con sus palabras y su amor.

A Olga, por ser mi compañera de proyectos desde primer semestre y quien me ayudó en todo y sobre todo a terminar el presente proyecto.

A mis amigos que de alguna manera siempre estuvieron apoyándome.

Diego Alejandro

PRESENTACIÓN

Para la presentación del presente proyecto se debe tomar en cuenta los antecedentes de los últimos años con respecto al desarrollo de la tecnología. La misma que a tenido un crecimiento que pocos hubieran podido predecir, y donde la comunicación ya no ve un problema en la distancia, idioma o situación social.

Las redes de datos, han ido incrementando su alcance, complejidad y servicios prestados a los usuarios, requiriendo de que las personas a cargo tengan un elevado control de la calidad, ofertando niveles de servicios altos, una gran disponibilidad y una regulación del ancho de banda capaz de garantizar que los elementos mencionados anteriormente, sean cumplidos conforme lo ofrecido en los contratos.

La gestión de una red es un factor muy importante para realizar un exitoso manejo operativo de la red. Las instituciones cada vez son más dependientes de los servicios de las redes, es así que si los servicios se encuentran ejecutándose correctamente, es sinónimo de que la institución y sus usuarios trabajan de manera adecuada.

La red de una institución con un correcto desempeño, asegura que sus servicios serán iniciados de forma rápida y que estos se mantendrán ejecutándose sin interrupción. Además, la gestión de red permite mantener los costos de red y costos operacionales bajo control. Permite que los equipos de red sean utilizados de manera eficaz y sean instalados donde más se los necesite, es decir sin desperdiciar los recursos informáticos.

Por otro lado si no se realiza una buena gestión de red, esto puede traer como consecuencias el deterioro o la interrupción de los servicios, mala utilización de las inversiones hechas en la red e incluso perjudicar a la reputación de la institución. Es así que podemos ver, que una acertada gestión de la red es crítico para una institución, como la que se menciona en el presente proyecto, la Universidad Técnica Estatal de Quevedo (UTEQ).

Para tener el control de las redes y lograr los resultados deseados se han venido experimentando a lo largo de los años varios métodos de Gestión de las Redes de la Información. Muchos de los cuales se han convertido en estándares y hoy en día son un pilar importante dentro la organización de una empresa o institución para mantener los niveles de calidad de servicios acordados.

Sin embargo, a pesar de toda la importancia que involucra la gestión de red, es sin duda uno de los tópicos menos entendidos en el gran mundo de las redes. Por lo cual muchos administradores de red, piensan de manera equivocada que la gestión es lo más fácil dentro de la implementación de una red, dejándose cegar por la tecnología de red en sí. Y al final dejan el aspecto de la gestión de la red en un segundo plano. Es por este motivo que el presente proyecto realiza el análisis de los modelos de gestión más difundidos actualmente y propone una metodología para la implementación de un modelo para gestionar la red de una institución universitaria como la UTEQ.

Con la propuesta del modelo de gestión se busca satisfacer la necesidad de la Universidad para controlar los recursos y servicios de sus redes de datos y así lograr maximizar su eficiencia y productividad.

RESUMEN

En el capítulo I se realiza un marco teórico completo, donde se presenta entre otras cosas una reseña histórica de la gestión de redes y conceptos generales para entender de que se trata cuando se habla sobre gestionar una red de comunicaciones. Luego, se sigue con la explicación sobre los diversos Modelos de Gestión y Administración de Redes más difundidos que existen en la actualidad, dentro de los que se menciona a los modelos ISO/OSI, TMN, e-TOM y el modelo de Internet o SNMP. Se señalan sus características principales y las diferentes arquitecturas de las que se conforman cada uno de ellos. Para concluir con este capítulo I, se presentan unas comparaciones entre los modelos de gestión y sus ventajas y desventajas, respectivamente.

En el capítulo II, se procede al análisis de la situación actual de la red. Se empieza con una breve reseña sobre la institución y su situación organizacional. Luego, se procede a identificar la topología de la red que existe actualmente en la universidad, así como los equipos utilizados en ella. Se describe la infraestructura del Backbone de la red y se realiza un análisis detallado de las subredes cableadas con los que se cuenta. Se realiza la descripción sobre los equipos físicos y lógicos de la red. Dentro de la gestión, se indica la manera como se administra actualmente la red, mostrando sus debilidades, amenazas y riesgos. Además se especifican cada uno de los servicios que ofrece actualmente la universidad a sus usuarios.

Este capítulo II finaliza con las conclusiones encontradas a través de los datos recogidos, es decir, con la información recabada se elabora un diagnóstico y se presentan los requerimientos de la red universitaria. Todo esto parta utilizarlo como punto de partida para la selección de un modelo de gestión acorde a la UTEQ (Universidad Técnica Estatal de Quevedo).

En el capítulo III, de las conclusiones de requerimientos realizadas en el capítulo anterior, se procede a plantearse los objetivos para la implementación de un modelo de gestión en la universidad. Y luego se sigue con la elección del modelo

de gestión de red para el cual se desarrollará la metodología de implementación. Siendo éste el punto principal en el desarrollo del presente capítulo.

En este capítulo III también se sugieren herramientas de software de monitoreo y equipos de hardware adicionales necesarias para la implementación del modelo de gestión. Además, se topan temas relacionados a calidad de servicio, recuperación ante desastres y fallas técnicas; y se establece las pautas de cómo el sistema se sobrepondrá a ellos. Además, se proponen políticas de seguridad, así como los equipos para brindar mayor confiabilidad a los usuarios de la red.

Como parte final del capítulo III se trata sobre las repercusiones a futuro del modelo de gestión estandarizado que se propone para ser desarrollado en la UTEQ, es decir, cómo éste modelo garantizará la escalabilidad tanto del modelo de gestión, como del hardware y software de la red para que éstos sigan cumpliendo con los estándares solicitados por la universidad bajo sus requerimientos tecnológicos y organizacionales. Como parte final en este capítulo se plantea el plan de migración a seguir en caso de implementarse el presente proyecto.

En el capítulo IV se realiza un análisis de costos de la posible implementación del modelo de gestión, tomando en cuenta hardware y software que la universidad debería adquirir para llevarlo a cabo.

En el último capítulo, el capítulo V se elabora las conclusiones y recomendaciones obtenidas con el desarrollo del presente proyecto.

Al final del proyecto se presentan los Anexos que contemplan y profundizan la información presentada en cada uno de los capítulos.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

CAPÍTULO I

CAPÍTULO II

CAPÍTULO III

ÍNDICE DE TABLAS

CAPÍTULO I

CAPÍTULO II

CAPÍTULO III

CAPÍTULO IV

ANEXOS

CAPÍTULO I
MARCO TEÓRICO: MODELOS DE GESTIÓN Y ADMINISTRACIÓN DE RED

1.1 INTRODUCCIÓN

El crecimiento de las redes y su complejidad, cada vez vuelve más necesaria la introducción de nuevas formas de trabajo que permitan al administrador de la red, tener un seguimiento completo sobre todos los recursos *IT (Information Technology)*. Es de ésta necesidad que nace el desarrollo de los modelos de gestión, para brindar a las empresas sistemas estándares que les permitan llevar un control sobre sus recursos informáticos y mejorar sus servicios a los usuarios.

1.1.1 RESEÑA SOBRE LA EVOLUCIÒN DE LA GESTIÒN DE REDES [11]

La gestión de las redes surgió con la aparición de las mismas, y por la necesidad de poder controlar los recursos que la componen. Y a medida que las redes han ido cambiando, también ha evolucionado la forma en que las redes son gestionadas o controladas. En la evolución que ha seguido la gestión de redes podemos mencionar tres etapas:

1.1.1.1 Gestión Autónoma [11]

Las primeras redes eran pequeñas y comprendían pocos nodos y cada uno de ellos poseía su propio sistema de gestión local. Las decisiones que afectaban a más de un nodo, implicaban la comunicación con cada uno de los administradores de los mismos.

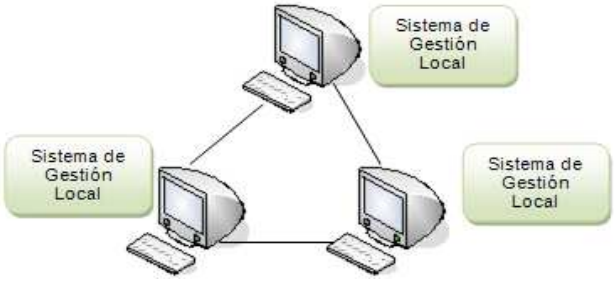


Figura 1.1 Gestión Autónoma [11]

1.1.1.2 Gestión Homogénea [11]

Con el pasar de los años las redes aumentaron su tamaño y eran redes propietarias, es decir, utilizaban componentes de un mismo fabricante, el mismo que aportaba su sistema de gestión, que en la mayoría de los casos, estaba centralizado en único nodo.

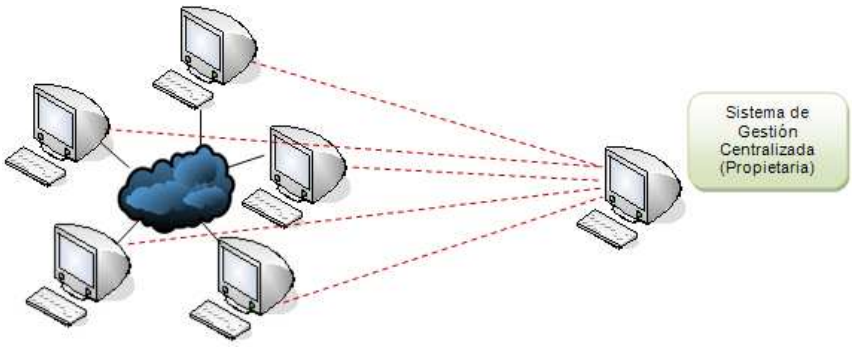


Figura 1.2 Gestión Homogénea [11]

1.1.1.3 Gestión Heterogénea [11]

Las redes cada vez crecían más, hasta ser compuestas por diferentes tecnologías que utilizaban recursos de variados fabricantes. Todo esto llevo a la necesidad de tener un sistema donde coexistan sistemas de gestión de diferente naturaleza.

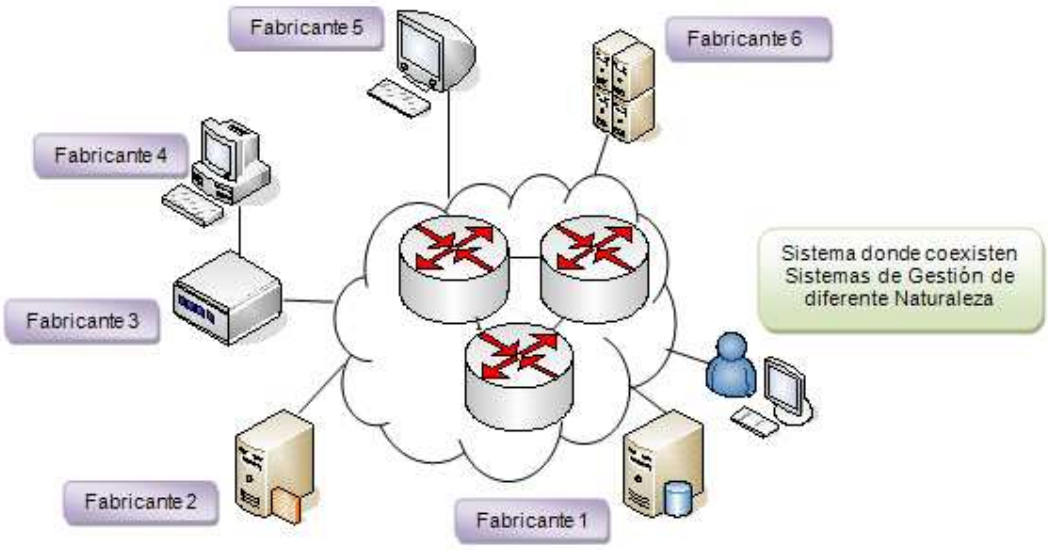


Figura 1.3 Gestión Heterogénea

Actualmente, la evolución de las redes continúa y esto ha llevado a la aparición de un nuevo tipo de gestión, la gestión integrada. La gestión integrada, busca superar problemas que presentaba la gestión heterogénea. Dentro de los que se puede menciona, la incompatibilidad que se daba entre datos de gestión, procedimientos y protocolos de comunicación con funcionalidad similar, así como la duplicidad e inconsistencias de la información almacenada en las bases de datos.

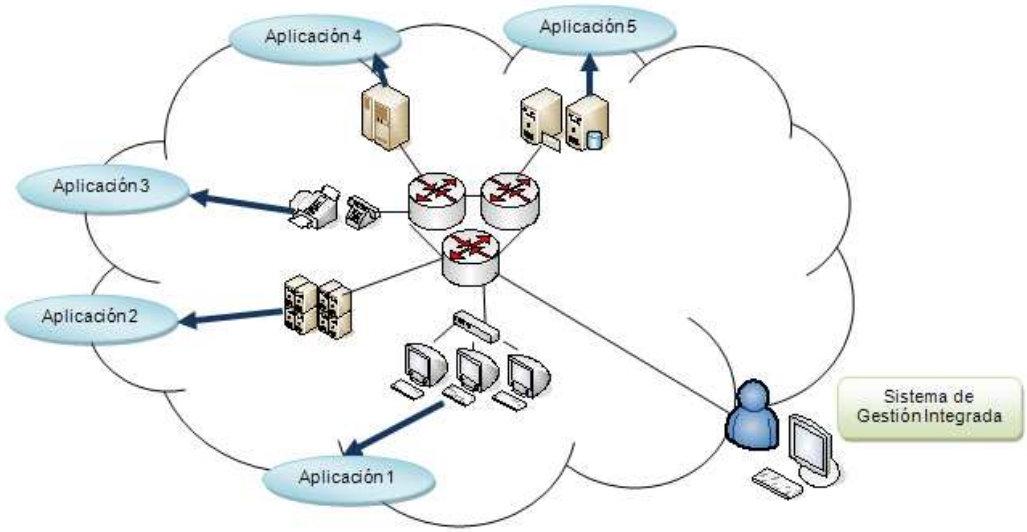


Figura 1.4 Gestión Integrada

1.2 CONCEPTOS GENERALES

1.2.1 DEFINICIÒN Y DIFERENCIAS ENTRE GESTIÓN Y ADMINISTRACIÓN DE RED [14]

En el campo tecnológico se habla de “gestión” en relación a su equivalente en el idioma inglés: *“management”*. Sin embargo, el concepto *management* abarca un área muy extensa en el área tecnológica.

Generalmente el término *management* se aplica en el español como “administración”, y teniendo en cuenta este punto de vista se puede decir que

gestión y administración abarcan distintas áreas. Aunque realizando una revisión de ambos conceptos se puede afirmar que las palabras gestión y administración son sinónimos, aunque el segundo concepto sea más general.

1.2.1.1 Administración [16]

Hace referencia al proceso de planear la ejecución de actividades, su realización y finalización de manera eficiente haciendo uso de un conjunto de recursos físicos y humanos. La administración busca el desempeño de cuatro funciones fundamentales como: planeación, organización, dirección y control.

Se puede ver que la administración tiene muchas áreas de desempeño, dejando de lado aspectos que se considerarían netamente “administrativos”.

1.2.1.2 Gestión

Su concepto está muy ligado al proceso administrativo haciendo referencia a los procesos de gerencia de actividades, entre las que incluyen la supervisión y control de su realización. Teniendo como objetivo principal el asegurar las formas de funcionamiento adecuadas para llevar a cabo estas actividades, las cuales a su vez permiten alcanzar los objetivos planteados por otras funciones de la administración.

De manera informal se dice, que la gestión de una red se refiere a todas las actividades asociadas con poner a funcionar una red, incluyendo la tecnología necesaria para soportar esas actividades. Siendo una parte muy significativa el simple hecho de monitorear la red, y saber siempre que es lo que está sucediendo en ella, aunque la gestión comprende otras funciones. [1]

Muchas veces al referirnos a la gestión de red, hablamos sobre la “salud” de la red, es así que podríamos decir que una red es como un paciente que debe ser monitoreado constantemente para saber su desempeño y sus capacidades para brindar un buen servicio. Así también si una red presenta malos funcionamientos estos deben ser identificados por medio de alarmas, para reaccionar lo más rápido y darle solución. [1]

1.2.1.3 Definición Formal de Gestión y Administración de Red [1]

"La gestión de red se refiere a las actividades, métodos, procedimientos y herramientas que pertenezcan a la operación, administración, mantenimiento y aprovisionamiento de los sistemas de red".

Donde:

- *Operación,* tiene que ver con tener la red funcionando sin interrupciones. Esto incluye el monitoreo de la red para establecer los problemas que están presentes lo más rápido posible, idealmente antes de que el usuario se entere de la existencia de dicho problema.
- *Administración,* que involucra el seguimiento de los recursos de la red y como están asignados.
- *Mantenimiento*, que se refiere a las actualizaciones y reparaciones para el correcto desempeño de la red. El mantenimiento también incluye las medidas correctivas y preventivas dentro de la red.
- *Aprovisionamiento,* se refiere a la configuración de los recursos para soportar los servicios que requieran.

Existen definiciones dadas por instituciones de estandarización como la ISO[1], la cual define que: "La gestión de red es un conjunto de facilidades para controlar, coordinar y monitorizar los recursos que soportan las comunicaciones". [14]

En el campo tecnológico, y específicamente en el área de las telecomunicaciones, el concepto que se maneja con fuerza es el de gestión. Esto debido a que las aplicaciones relacionadas en el campo de las comunicaciones generalmente tienen como objetivo asegurar el funcionamiento apropiado de un sistema. Es importante aclarar que los términos gestión y administración de red se utilizarán como sinónimos, para el desarrollo del presente trabajo.

[1] ISO: International Standarization Organization, es el organismo encargado de promover el desarrollo de normas internacionales de fabricación, comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica.[28]

1.2.2 IMPORTANCIA Y BENEFICIOS DE LA GESTIÓN DE UNA RED DE DATOS [1]

Antes, el éxito de la empresa se basaba solamente en la competitividad con respecto a la superioridad tecnológica de sus productos y de la garantía del desempeño de servicios básicos, pero actualmente cada vez depende más de la Calidad del Servicio *(QoS)* que ofrecen, el precio de negociación y el soporte a los clientes. Es aquí, donde tiene su importancia la gestión de la red de una empresa, porque ésta con sus diferentes herramientas le permite a la empresa reducir costos, mejorar la velocidad y la calidad del servicio, y así aumentar los réditos y la competitividad de la misma frente al resto de empresas.

Entre los principales beneficios de la gestión de red están:

1.2.2.1 Costos

La gestión ayuda a bajar costos, porque permite hacer más eficientes las operaciones de la red y permitir que los administradores de la red sean más productivos. En una empresa existe lo que se conoce como Costo Total de la Propiedad (con sus siglas en inglés *TCO*[2]*: Total Cost of Ownership*) que comprende el costo de los equipos y el costo para operar la red. La gestión permite disminuir el *TCO*, y estos costos que se bajan le permiten a la empresa ser más competitiva, desde el punto de vista económico.

1.2.2.2 Calidad

Las aplicaciones de gestión de red ayudan a controlar los factores que determinan la calidad del servicio como son: el ancho de banda realmente disponible y los retardos en la red. Con la gestión de la red se garantiza la confiabilidad y la disponibilidad de los servicios de la red.

1.2.2.3 Réditos

La gestión dentro de una red no sólo mejora la calidad del servicio y disminuye costos. También es importante porque permite a la empresa tener nuevas

[2] TCO: Total Cost of Ownership: es un método de cálculo diseñado para ayudar a los usuarios y a los gestores empresariales a determinar los costes directos e indirectos, así como los beneficios, relacionados con la compra de equipos o programas informáticos.

oportunidades dentro del mercado de las comunicaciones y obtener réditos. Una red correctamente gestionada permite reducir tiempos entre que el servicio sea ordenado y se encuentre corriendo, porque automatiza los pasos que se deben dar para crear el servicio. Todo esto se transforma en obtener réditos más rápido y dar satisfacción a los usuarios.

1.2.3 PRINCIPALES DESAFÍOS DE UN SISTEMA DE GESTIÓN DE RED [1]

A medida que crece el número, la complejidad y heterogeneidad de los recursos de las redes, también crece la importancia de la gestión de las redes y los desafíos que esta debe enfrentar. Cada vez a las redes se les añade más dispositivos de diferentes tipos, de diferentes versiones. Y al mismo tiempo son más los usuarios conectados a la red y usando mayor cantidad de servicios. Todo esto vuelve cada vez más complicado el control y seguimiento de la red.

Entre los principales desafíos que enfrenta la gestión de red están:

- Desafíos Técnicos.
- Desafíos Operativos y Organizacionales.
- Desafíos de Negocios.

1.2.4 ELEMENTOS BÁSICOS DE GESTIÓN Y ADMINISTRACIÓN DE RED [1]

En la gestión de red, se debe empezar considerando que existen elementos en la red que necesitan y deben ser gestionados, luego están los sistemas y aplicaciones que son usados para gestionar la red y donde reside la lógica de la gestión en sí. Todo esto ayuda a los administradores a monitorear y recolectar los datos de la red, luego estos datos serán interpretados y analizados para decidir que comandos serían los adecuados para cambiar el comportamiento de la red y lograr los resultados requeridos.

Para que exista comunicación entre la red que necesita ser gestionada y las aplicaciones de gestión, existe la red de gestión con las aplicaciones de red

específicas para la gestión, sin las cuales sería imposible intercambiar la información y los comandos de gestión.

Además de los elementos técnicos para la gestión de la red, también es necesaria una organización, que al final es la responsable del correcto funcionamiento de la red.

1.2.4.1 Dispositivos de Red *(NE: Network Element)* [1]

También llamados elementos de red, son los dispositivos a ser gestionados. El elemento de red forma parte del proceso de gestión. Para poder ser gestionado este proporciona una interfaz para poder comunicarse con el sistema de gestión. A través de esta interfaz el elemento de red puede recibir peticiones del sistema de gestión y así mismo responder estas solicitudes. El dispositivo de red dentro del proceso de gestión toma el rol de “agente” y es el que soporta a las peticiones del “gestor” de manera proactiva, notificándole si ocurre algún evento inesperado.

1.2.4.1.1 Gestor [9]

El gestor es un elemento de sistema cuya tarea es enviar requerimientos de gestión hacia los agentes para el control, coordinación y monitoreo de la red. En la práctica, el gestor es la aplicación *(software)* que emite las directivas de operaciones de gestión y recibe notificaciones y respuestas. Este se implementa en una estación de gestión *(Workstation)* en la cual se tiene una Base de Información de Gestión (*MIB: Management Information Base)* del dispositivo gestionado y una interfaz de usuario.

1.2.4.1.2 Agente [9]

El agente es un elemento de sistema hacia el cual se dirigen los comandos de gestión para el control, coordinación, y monitoreo de la red. Los agentes ejecutan operaciones sobre los objetos gestionados de acuerdo a los requerimientos del gestor, y retransmiten mensajes emitidos por los objetos gestionados hacia el

gestor (Ver figura 1.5). El agente responde a las directivas enviadas por el gestor accesando a la Base de Información de Gestión *(MIB)* para manipular los objetos involucrados en la operación. El agente se encuentra ubicado en el dispositivo de red gestionado.

La relación entre el gestor y el agente se puede comparar a la que existe dentro de un sistema cliente/servidor. La comunicación entre un gestor y agente se da de forma asimétrica como se puede ver en la figura 1.6.

Figura 1.5 Comunicación Gestor-Agente [1]

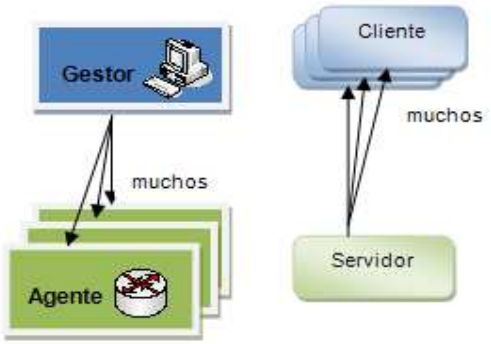


Figura 1.6 Gestor/Agente versus Cliente/Servidor [1]

El agente de gestión es el componente de software que le permite al elemento de red realizar su rol de agente. El elemento de red puede tener varios agentes de gestión (Figura 1.6) a pesar de que desempeñe un solo rol como agente, ya que de esta manera permite a los agentes de gestión poder servir a funciones

diferentes. El agente de gestión se compone de tres partes principales (Figura 1.7) como se explica a continuación:

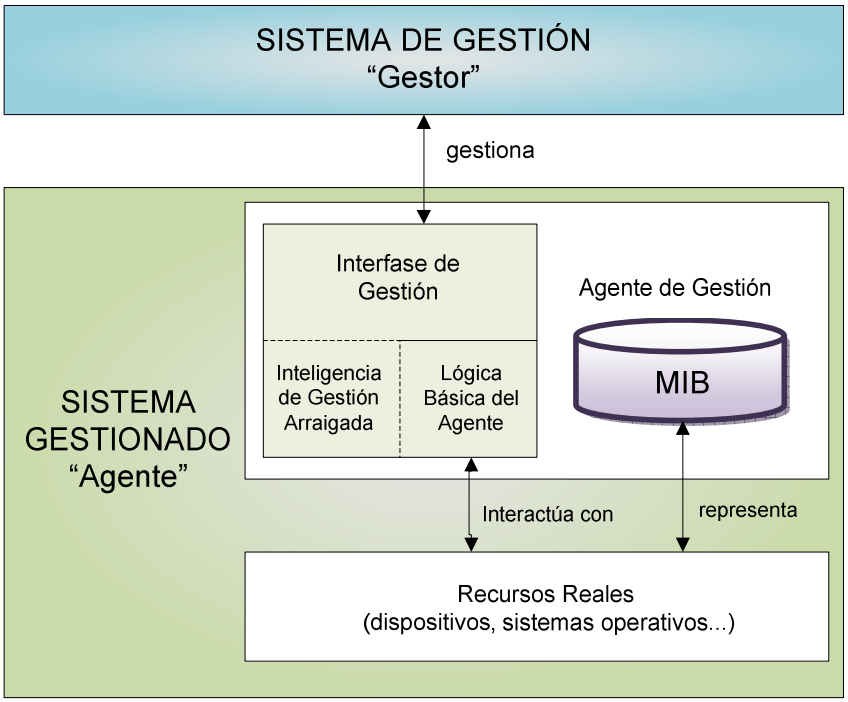


Figura 1.7 Anatomía de un Agente de Gestión [1]

a. La Interfase de Gestión

Es la encargada de manejar las comunicaciones de gestión, la cual soporta los protocolos de gestión para permitir la comunicación entre el agente y la aplicación de gestión.

b. La Base de Gestión de Información (MIB)

Es donde se almacenan datos de manera conceptual, que representan la información desde el punto de vista de gestión. No se debe confundir una MIB con una base de datos real. La *MIB* es la información del dispositivo a la que se accede a través del protocolo de gestión.

c. La lógica básica del Agente

Es la que realiza la traducción entre la operación de la interfase de gestión, la *MIB* y el dispositivo actual gestionado. Además de estas funciones básicas, el agente lógico puede incluir funciones adicionales y realizar un procesamiento requerido por aplicaciones de gestión, a lo que se le denomina *"embedded management intelligence"*.

1.2.4.1.3 Información de Gestión [1]

La información de gestión es proporcionada por el agente de gestión y representa una abstracción de aspectos del mundo real para satisfacer los propósitos de la gestión de una red. La información de gestión no modela con todo detalle los aspectos del mundo real, por eso se dice que es una abstracción.

1.2.4.1.4 Objetos de Gestión (MOs: Management Objects) [1]

Un objeto de gestión se puede definir como una porción de toda la información de gestión, que expone un aspecto específico del mundo real. Hay que saber diferenciar entre una abstracción de gestión del *MO* y lo que representa en base a esto el objeto de gestión. El objeto de gestión que representa al objeto del mundo real, se refiere a un recurso real, el mismo que puede ser abstraído de diferentes formas. Es por eso que muchos objetos de gestión, pueden existir concurrentemente, a pesar de que se refieran a una misma cosa.

1.2.4.1.5 Base de Información de Gestión (MIBs)

Como se mencionó anteriormente, una *MIB* representa el almacenamiento de datos de forma conceptual. Los administradores pueden obtener información de la *MIB* con peticiones direccionadas a través del agente de gestión. Cuando el administrador de la red manipula la información de la *MIB*, las configuraciones actuales del dispositivo en ese momento son modificadas, afectando el comportamiento del dispositivo en el mundo real.

La *MIB* es el conjunto de objetos gestionados *(MO)*, los cuales son las piezas de información de gestión que representan a los recursos, los mismos que permiten algún tipo de gestión en una forma abstracta. La *MIB* se encuentra ubicada en el dispositivo gestionado, y una referencia de ésta es necesaria en el gestor.

La información de una *MIB* está estructurada en forma de árbol de manera jerárquica (Figura 1.8). Cada objeto manejado en un *MIB* tiene un identificador de objeto único e incluye el tipo de objeto (Ej. contador, secuencia o *gauge*), el nivel de acceso (Ej. lectura y escritura), restricciones de tamaño, y la información del rango del objeto.

Los datos de la *MIB* se definen usando la notación formal *ASN.1*, la cual es un estándar para la especificación de los tipos de datos que son intercambiados sobre un protocolo de comunicación.

Las *MIBs* suelen ser modificadas cada cierto tiempo para añadir nuevas funcionalidades, eliminar ambigüedades y arreglar fallos.

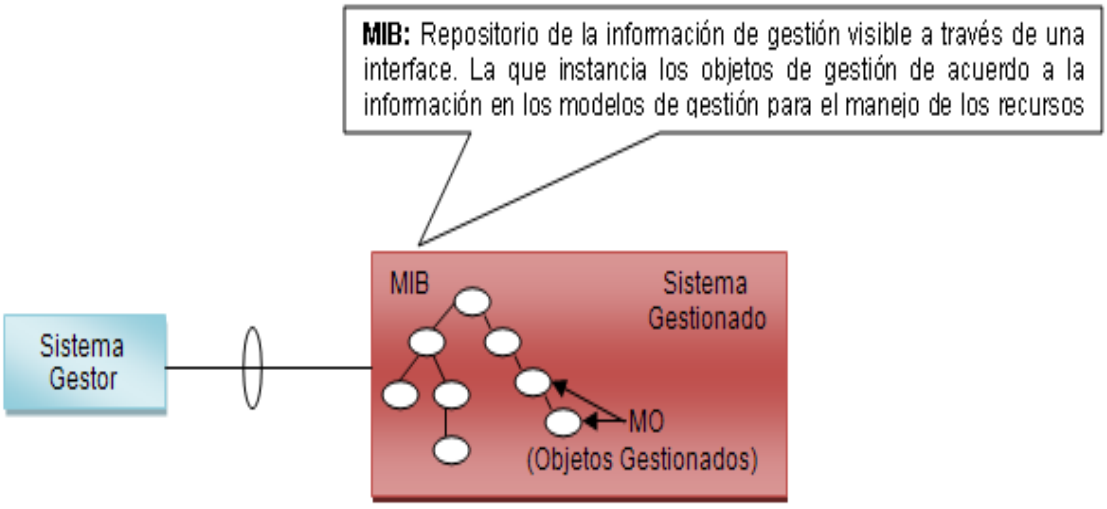


Figura 1.8 Concepto de la Base de Información de Gestión (MIB) [3]

Existe la Base para Gestión de Redes de Internet basadas en *TCP/IP* o comúnmente llamadas *MIB-II*.

1.2.4.1.6 Categorización de la Información de Gestión

La información que se mantiene en una *MIB* puede ser diferenciada en algunas categorías de información de gestión. Esto es importante porque las aplicaciones de gestión utilizan cada una de estas categorías con propósitos diferentes. Entre las diferentes categorías se menciona las siguientes:

- Información de Estado.
- Información Histórica.
- Información de Configuración Física.
- Información de Configuración Lógica.

La definición de la *MIB* en sí, necesita ser especificada utilizando un lenguaje de especificación. Entre los principales tenemos:

- *SMIv1 y SMIv2 (Structure of Management Information versiones 1 y 2)*. Es el lenguaje de especificación de *MIB* (DDL: Lenguaje de Definición de Datos), usado de manera conjunta con el protocolo de gestión SNMP.
- *MOF (Manager Object Format)*. Es el lenguaje de especificación utilizado de manera conjunta con la tecnología de gestión llamada *CIM (Common Information Model)*.
- *GDMO (Guidelines for the Definition of Manager Objects)*. Es el lenguaje de especificación utilizado de manera conjunta con el protocolo de gestión *CMIP (Common Management Information Protocol),* aunque actualmente solo se limita al uso comercial.

1.2.4.2 Sistema de Gestión de Red [1]

Así como los agentes de gestión actúan como un Proxy que representan el mundo real con el fin de gestionar los recursos, así mismo, un sistema de gestión actúa como Proxy para la organización de soporte de operaciones. Un sistema de gestión proporciona las herramientas para gestionar la red, estas herramientas

incluyen aplicaciones para monitorear la red, sistemas de aprovisionamiento de servicios, analizadores de tráfico, etc.

Para tener una mejor eficiencia, muchos sistemas de gestión construyen su propia base de datos, en la cual mantienen información temporalmente para evitar tener que regresar al elemento de red repetidamente por la misma información. Esta base de datos interna se la conoce como *MIB* de la caché o *"shadow MIB"* (Ver Figura 1.9).

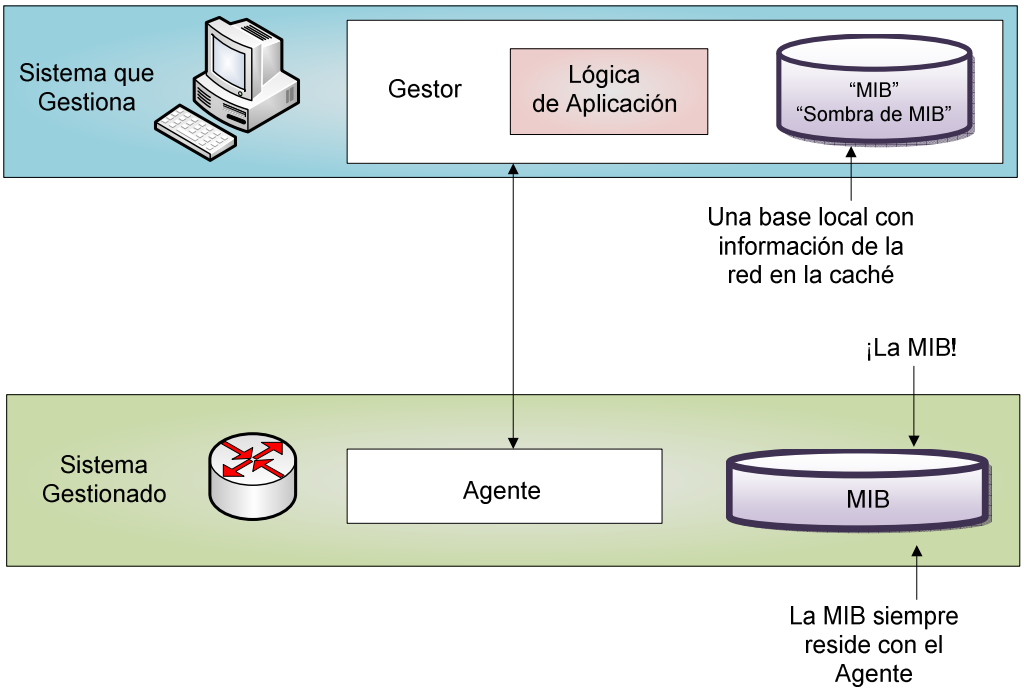


Figura 1.9 Muestra ubicación de la MIB [1]

Un sistema de gestión existe sólo para propósitos de gestión de la red. Es decir, si algo le pasa al sistema de gestión, esto no afecta al funcionamiento de la red en general. Simplemente el administrador no podría monitorear y mantener la red, y la calidad del servicio de la red bajaría, existiría dificultad en ejecutar los servicios y sería difícil agregar nuevos usuarios a la red.

Un sistema de gestión está formado principalmente por: la plataforma de gestión de red y las aplicaciones que la acompañan.

1.2.4.2.1 Plataformas de Gestión de Red

Las restricciones de coste, espacio físico y experticia de los técnicos llevan a la necesidad de buscar una gestión integrada desde un solo sistema, que debería también poder presentar sus interconexiones en un mapa de la red. De estas necesidades se crean las plataformas de gestión de red.

Se puede definir una plataforma de gestión de red como una aplicación de software que proporciona la funcionalidad básica de gestión de red para los diferentes componentes de una red (Ver figura 1.10).

El objetivo de la plataforma es proporcionar una funcionalidad genérica para gestionar los diferentes dispositivos de red.

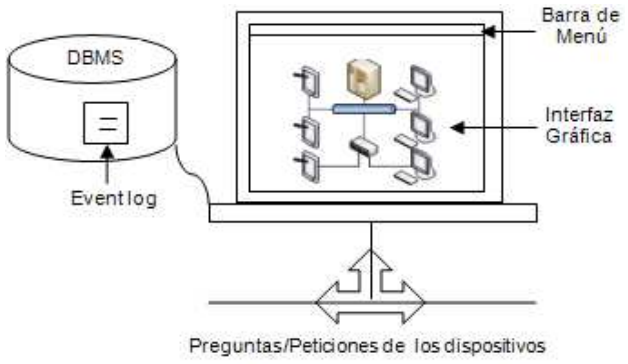


Figura 1.10 Componentes Básicos de una Plataforma de Gestión de Red [2]

Las funcionalidades básicas que debe incluir son:

- Interfaz gráfica de usuario (*GUI*).
- Mapa de la red.
- Sistema gestor de base de datos (*DBMS*).
- Método estándar de consulta de dispositivos (Protocolo).
- Menús del sistema configurables.
- Registro de eventos (*Event Log*).

Características adicionales:

- Herramientas de gráficos.
- Interfaces de programación de aplicaciones (*API*).
- Seguridad del sistema.

1.2.4.2.2 Arquitecturas de Gestión de Red [2]

Una plataforma de red puede usar varias arquitecturas para proporcionar la funcionalidad al sistema. Las arquitecturas de gestión de red más comunes son: Arquitectura Centralizada, Arquitectura Jerárquica y de Arquitectura distribuida.

a. Arquitectura Centralizada [2]

Una arquitectura centralizada se caracteriza por tener la plataforma de gestión de red en un solo sistema de computadora (*NMS: Network Management System*), el que es responsable de todas las tareas de la gestión de red, como por ejemplo:

- Ver las alertas y eventos, lo cual es muy útil para el administrador de la red cuando se trata de localizar daños y hacer la correlación de problemas o fallos de la red.
- Tener un solo sitio para acceder a toda la información y aplicaciones de gestión de la red, lo cual le permite dar a la red mayores niveles de confianza, accesibilidad y seguridad.

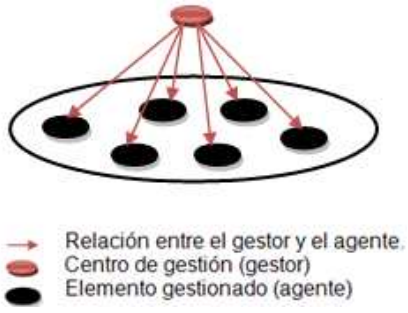


Figura 1.11 Arquitectura de Gestión Centralizada [2]

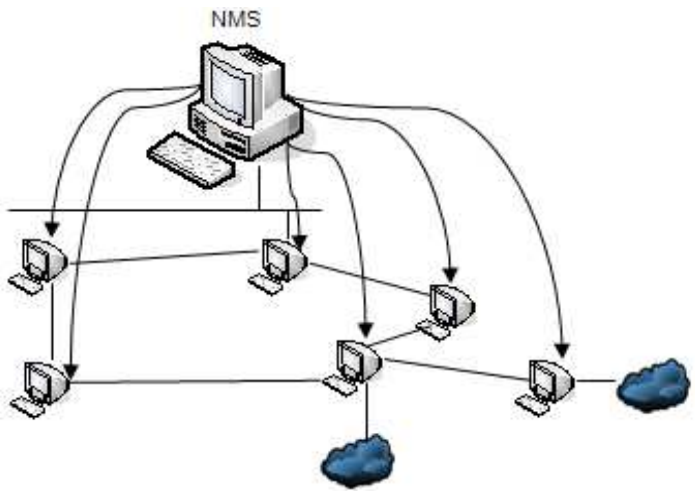


Figura 1.12 NMS responsable único de la gestión de red [2]

Este tipo de arquitectura tiene un sistema que utiliza una única base de datos centralizada.

El sistema central es el punto principal para gestionar la red, sin embargo, este puede permitir el acceso o puede enviar los eventos a otras consolas a través de la red.

a.1 Ventajas de una Arquitectura Centralizada

Una arquitectura centralizada se recomienda, en particular, para redes que requieran un alto grado de fiabilidad. Las principales ventajas son:

- *Recursos centralizados*, debido a que el sistema para la gestión es el centro de la red, puede administrar los recursos que son comunes a todos los usuarios.
- *Seguridad mejorada*, ya que la cantidad de puntos de entrada que permite el acceso a los datos administrados son mínimos.
- *Red escalable*, gracias a esta arquitectura, es posible quitar o agregar usuarios sin afectar el funcionamiento de la red y sin la necesidad de realizar mayores modificaciones.

a.2 Desventajas de una Arquitectura Centralizada

Entre las principales desventajas de una arquitectura centralizada están:

- Una arquitectura centralizada, donde todas las funciones de gestión de red dependen de un solo sistema, tiene la desventaja de no ser tolerante a fallos.
- Es difícil y costoso realizar la gestión por un solo sistema, cuando aumentan los elementos de red y se necesita manejar una mayor carga de información.
- Pero la desventaja más significante dentro de esta arquitectura, es que las peticiones que se envían a los elementos de red se realizan desde un solo sistema, lo cual podría provocar una saturación de tráfico de datos en los enlaces conectados a dicho sistema y de la red en general.

b. Arquitectura Jerárquica [2]

Una arquitectura de gestión de red jerárquica utiliza múltiples sistemas, utilizando uno de ellos para que actúe como un sistema servidor y el resto actuando como clientes. Este sistema se caracteriza porque algunas de las funciones de gestión se encuentran en el servidor, mientras otras son ejecutadas por los clientes.

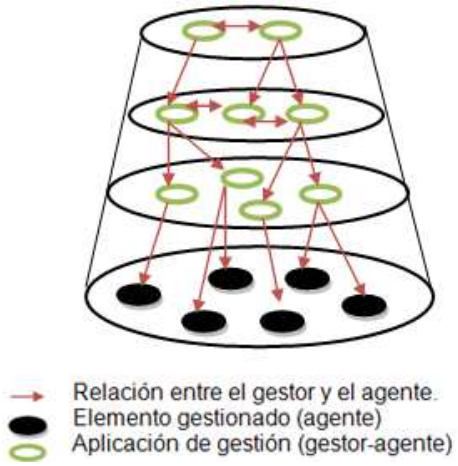


Figura 1.13 Arquitectura Jerárquica de una Plataforma de Gestión de Red [2]

La plataforma de gestión que utiliza esta arquitectura, podría utilizar una base de datos con tecnología cliente/servidor. Es así que debido a la importancia del sistema central, este debe contar con respaldos para redundancia de la información de la red.

b.1 Ventajas de una Arquitectura Jerárquica

Una arquitectura jerárquica presenta las siguientes ventajas:

- No depende de un solo sistema para realizar la gestión de la red.
- Permite la distribución de tareas de gestión de la red, con lo cual supera los problemas de saturación de información que se presentaban en una arquitectura centralizada.
- Los administradores de la red pueden distribuir la monitorización de la red entre los sistemas clientes, ahorrando así recursos de banda ancha.

b.2 Desventajas de una Arquitectura Jerárquica

Una arquitectura jerárquica presenta las siguientes desventajas:

- Al existir múltiples sistemas donde se almacena información sobre la gestión, la reunión de toda la información de la red se vuelve más complicada para el administrador de la red y le exige más tiempo.
- Otra desventaja es que los dispositivos gestionados por cada cliente necesitarían ser lógicamente predeterminados y manualmente configurados, lo cual si no es realizado de manera correcta, podría llevar a un consumo innecesario de ancho de banda, ya que el sistema central y el sistema cliente podrían estar manteniendo información sobre un mismo dispositivo gestionado.

c. Arquitectura Distribuida [2]

Una arquitectura distribuida combina las características de las arquitecturas centralizadas y jerárquicas. Además de tener una plataforma centralizada, utiliza otros múltiples pares de plataformas. Todo esto, con el fin de evitar que toda la información de gestión se concentre en un único sitio. Cada par de plataformas puede tener su propia base de datos para los dispositivos a través de la red, con la cual puede realizar tareas y reportar los resultados al sistema central. Se pretende de esta manera simplificar la gestión de las redes por medio de la automatización, de forma que las decisiones básicas se tomen cerca del origen del problema.

Mediante la gestión distribuida es posible controlar redes de gran extensión de una manera más efectiva, repartiendo entre varias estaciones de gestión las tareas de monitorización, recopilación de información y toma de decisiones.

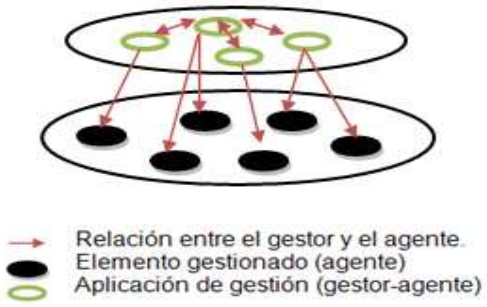


Figura 1.14 Arquitectura Distribuida de una Plataforma de Gestión de Red [2]

c.1 Ventajas de una Arquitectura Distribuida

Una arquitectura distribuida presenta las siguientes ventajas:

- En una arquitectura distribuida se manejan funciones de sondeo para recolectar los datos gestionables de la red, liberando al gestor central de este tipo de tareas y permitiéndole concentrarse en la resolución de eventos más importantes.

- Esta arquitectura tiene una mayor confiabilidad. Al estar distribuida la carga de trabajo en muchas máquinas, la falla de una de ellas no afecta a las demás, y así el sistema sobrevive como un todo.

c.2 Desventajas de una Arquitectura Distribuida

Una arquitectura distribuida presenta las siguientes desventajas:

- El principal problema es el software, el diseño, implementación y uso del software distribuido.
- Otra desventaja es la seguridad de los datos, ya que al ser una arquitectura distribuida existen datos que se comparten.

1.2.4.3 Red de Gestión

Los sistemas de gestión y los elementos gestionados necesitan estar interconectados y comunicados, y es por eso que existe la red de gestión. La red de gestión actualmente no es más que una aplicación distribuida que permite se desarrollen los roles de gestor y agente entre los sistemas y elementos de la red.

La red de gestión puede ser físicamente independiente de la red que maneja el tráfico de los usuarios o clientes de la red, o puede compartir físicamente la misma red.

1.2.4.4 Organización de Soporte para la Gestión

Para una buena gestión además de la tecnología para la gestión, es necesario que exista la organización responsable de realizar la administración de la red. Los aspectos tecnológicos y los organizacionales dentro de la gestión trabajan en conjunto y dependen uno del otro para lograr mejores niveles de rendimiento de la red. Es por eso que muchas veces en las empresas al sistema de gestión se lo conoce como Sistema de Soporte Operacional *(OSS: Operacional Support*

System), es decir, que el sistema de gestión es un factor fundamental dentro del ambiente de soporte operacional de la organización.

El éxito de una empresa se encuentra en su capacidad de optimizar la organización de sus operaciones, y así ser más eficientes para correr la red, ser más rápidos al momento de añadir nuevos servicios, etc.

En una buena estructura organizativa, se tienen claramente definidas las responsabilidades y las tareas de la gestión de la red, como las siguientes:

- *Personal encargado del planeamiento de la red*, que son responsables de analizar la utilización de la red y los patrones de tráfico, y así planificar construcciones de la red y desarrollos de nuevos servicios.
- *Personal encargado de las operaciones de la red*, responsables de que la red se mantenga corriendo sin interrupciones, además de encargarse del monitoreo de la red por si ocurre algún error.
- *Personal encargado de la administración de la red*, los cuales son los únicos de interactuar físicamente con la red, y responsables en desarrollar la red y los servicios en ella. Este personal incluye técnicos que se encargan de cualquier instalación de nuevos equipos en la red, reemplazo de elementos, etc.
- *Personal encargado del manejo de los clientes*, y responsable de interactuar con el usuario. Estas personas se encargan de tomar las órdenes para nuevos servicios y de explicar al usuario sobre las diferentes opciones de soporte para el cliente.

Además de una correcta estructura organizacional, es necesario considerar varios aspectos adicionales que deben realizarse para que la red corra sin problemas, como los siguientes:

- *Establecer políticas de procesos y operación de la red*, así como la respectiva documentación de los procedimientos operacionales. Ya que esto permite que la gestión de red sea más consistente y eficiente. Y se asegura que las

tareas de gestión si se realicen por las personas responsables de las mismas.

- *Coleccionar las auditorias a la red***.** Es decir, llevar un registro automático de las actividades de las operaciones realizadas en la red, ver quién inició una actividad, en qué momento se realizó la actividad. Todo esto permite reproducir que pasa en la red y recuperarla de alguna situación de fallo producida por algún error humano o técnico.
- *Documentar la red*. Es decir llevar una documentación de toda la red, la cual debe ser exacta y estar actualizada. Esto tiene su importancia para actividades de planificación de la red y para planificar actualizaciones de software.
- *Tener un respaldo confiable y contar con procedimientos de restauración*, lo que permite estar preparados a los administradores de la red en caso de desastre o alguna emergencia.
- *Hacer énfasis en la seguridad***,** teniendo en cuenta que las mayores amenazas para la red a veces se encuentran dentro de la misma empresa y no son solo los hackers los que pueden producir daños.

1.2.4.5 Aplicaciones de Gestión de Red

Las aplicaciones de gestión se crearon para ayudar al administrador de la red a gestionar un conjunto específico de dispositivos o servicios. Las aplicaciones evitan que sus funciones no se solapen con las de las plataformas, al mismo tiempo que busca integrarse a ella a través de la *API* y los menús de interfaces.

Las aplicaciones permiten automatizar la gestión de la red, que van desde las más básicas hasta aquellas con mayor complejidad. Entre las principales herramientas de gestión tenemos:

- Analizadores de Red.
- Gestionadores de Dispositivos *(Craft Terminals).*
- Gestionadores de Elementos.
- Sistemas de Detección de Intrusos.

- Sistemas de Análisis de Desempeño.
- Sistemas de Gestión de Alarmas.
- Sistemas de Inventario.
- Sistemas de Aprovisionamiento de Servicio.

1.2.4.6 Protocolos de Gestión

El protocolo es el conjunto de especificaciones, convenciones y reglas que gobiernan la interacción de procesos y elementos dentro de un sistema de gestión. En la actualidad *SNMP (Simple Network Management Protocol)*, forma parte del modelo de gestión de Internet, y *CMIP (Common Management Information Protocol)* es parte del modelo de gestión OSI; y ambos son los protocolos predominantes.

1.3 PRINCIPALES MODELOS DE GESTIÓN Y ADMINISTRACIÓN DE RED

Las instituciones o empresas siempre tratan de mejorar sus servicios, los cuales dependen de la eficiencia y desempeño de las redes.

Con el gran desarrollo de las redes se llegó a la necesidad de evolucionar hacia los Sistemas de Gestión Integrada, que permitieran realizar el trabajo desde un solo Centro de Gestión, para administrar las redes donde intervienen recursos de diversas tecnologías. Pero para llegar a estos sistemas fue necesaria una estandarización previa de la gestión de red. En la actualidad existen tres modelos fundamentales de gestión de red integrada:

- *Gestión de Red OSI: Open Systems Interconnection (Interconexión de Sistemas Abiertos)*. Definido por *ISO*, con el objetivo de lograr la gestión de los recursos del modelo de referencia *OSI*.
- *Gestión Internet*. Definido por la *Internet Society* para gestionar el modelo de referencia *TCP/IP*.

- *Arquitectura TMN Telecommunications Management Network (Red de Gestión de las Telecomunicaciones)*. Definida por la UIT-T (Unión Internacional de Telecomunicaciones). Es más que un modelo de red, ya que define una estructura de red basada en los modelos antes mencionados.

Otro modelo que será mencionado por ser unos de los últimos estandarizados por la UIT-T, es el Modelo de Gestión de Red de Telecomunicaciones *TOM (Telecom Operations Map)* o *e-TOM (enhanced-Telecom Operations Map).*

Existe diversos modelos de gestión y administración de redes de datos, pero solo los principales en la actualidad, serán estudiados en esta parte del proyecto. Los mismos que se muestran en la siguiente gráfica:

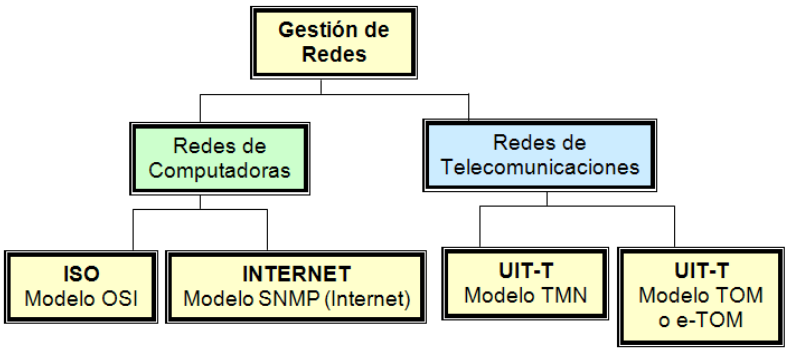


Figura 1.15 División de la Gestión de Redes y los diversos Modelos de Gestión Integrada [9]

1.3.1 MODELO DE GESTIÓN Y ADMINISTRACIÓN DE RED OSI

Este modelo nació de la necesidad de gestionar redes que aplican el modelo OSI, pero su implantación práctica se la debe al modelo *TMN* (modelo que se explica más adelante). Es el estándar que gestiona las 7 capas del modelo *ISO/OSI*. Este modelo de Gestión de Redes *OSI*, está formado a su vez por 4 modelos que se explican a continuación:

- *Modelo Funcional*: *FCAPS*. Se encargado de definir las funciones de gestión que proporcionan una interfaz a la aplicación de gestión.

- *Modelo Organizacional*: Su objetivo es exponer las posibles subdivisiones de la red en dominios de gestión.
- *Modelo de Comunicaciones*: *CMIP*. Se ocupa de detallar el protocolo de gestión y el servicio que proporciona.
- *Modelo de Información*: Define los recursos de red usando una sintaxis abstracta.

1.3.1.1 Modelo Funcional [29]

Este modelo define áreas funcionales o conceptuales, que facilitan entender y diseñar de mejor manera la gestión de una red.

Estas áreas se encuentran definidas en el modelo *FCAPS*. El modelo *FCAPS (Fault, Configuration, Accounting, Performance, Security)* permite una estructura lógica, la cual se encarga de categorizar las funciones de gestión en áreas como: gestión de fallas, gestión de configuración, gestión de contabilidad, gestión de desempeño y gestión de seguridad.

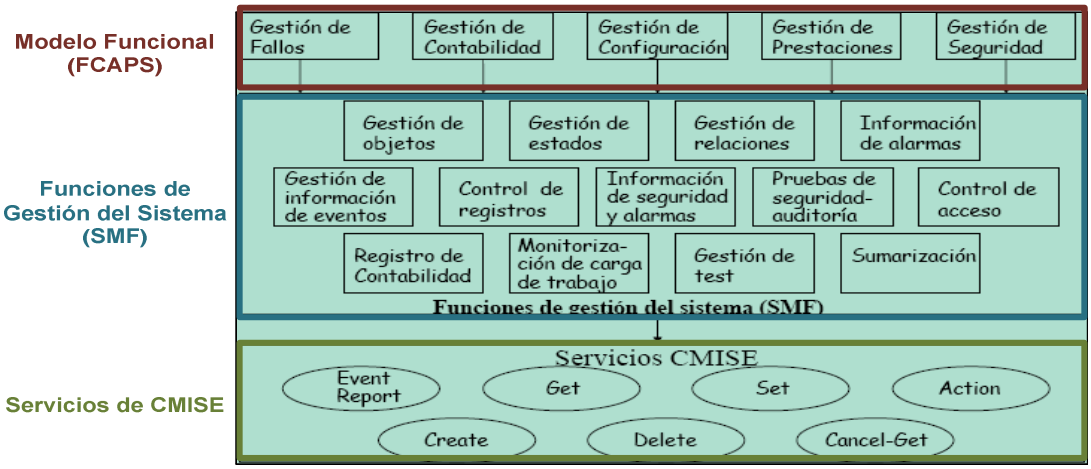


Figura 1.16 Modelo Funcional de OSI y las Funciones de Gestión de Sistemas (*SMF*) [29]

Específicamente en el modelo de gestión y administración *OSI*, las áreas funcionales están constituidas por diversas funciones específicas denominadas *SMF (System Management Funtions)*, las que están encargadas de realizar

procesos de gestión interactuando con los servicios *CMISE (Common Management Information Service Element)* (Ver Figura 1.16).

1.3.1.1.1 Gestión de Fallas

La gestión de fallas (algunas veces también referida como gestión de eventos y errores) es un conjunto de funciones las cuales habilitan la detección, aislamiento, y corrección de operaciones anormales en la red y su ambiente.

Su propósito es detectar y registrar eventos que han ocurrido en diferentes partes de la red, luego establecer la causa de estos eventos con el mayor grado de detalle y seguridad. Todo esto con el objetivo de explorar los errores y ser capaces de repararlos en el tiempo más corto posible.

La gestión de fallas puede ir desde un simple registro de estados de las alarmas originados por los elementos de red y la generación de mensajes de error apropiados a efectos de informar al operador, hasta métodos más sofisticados y efectivos como correlacionar estos eventos individuales y evaluar su correlación por medio de algoritmos apropiados.

Como resultado de aplicar la gestión de evento y error, una gran parte de malfuncionamientos pueden ser descubiertos y eliminados antes que puedan causar problemas detectables por los usuarios.

La gestión de fallas está también relacionada con el mantenimiento de estadísticas. Las estadísticas pueden asistir al administrador en la decisión de si una red cumple con los requerimientos apropiados de confiabilidad, desempeño, etc. o no.

1.3.1.1.2 Gestión de Configuración

La gestión de configuración provee funciones para operar, controlar, identificar, y colectar datos desde ó proveer datos a elementos de red. En la práctica de gestionar redes de telecomunicaciones actuales de banda ancha, la gestión de

configuraciones generalmente incluye dos funciones esenciales lógicamente diferentes. En particular: gestión de configuración estática, y dinámica.

La gestión de *configuración estática* involucra la asignación y desasignación de elementos de red, así como el registro, indicación, muestra y reporte de la topología de la red y listado del equipamiento de red conjuntamente con sus parámetros de sistema, tales como tipo, localización topológica, direcciones físicas y simbólicas, etc. En el caso de redes pequeñas y simples, (en conjunto con el registro de parámetros de equipamiento), la gestión de configuración estática puede también involucrar el control de inventario; sin embargo, en el caso de redes complejas, esta función debería ser manejada separadamente.

La gestión de *configuración dinámica* involucra el establecimiento de las rutas actuales para las interconexiones requeridas por la red. Esto implica la reconfiguración de la red mediante el establecimiento de una posible nueva ruta, si la ruta actual desaparece, o la cancelación de la ruta si llega un requerimiento de cancelación de la misma. En términos de la gestión de configuración dinámica, la presentación de la topología de red tiene que reflejar las rutas y conexiones actuales en la red.

1.3.1.1.3 Gestión de Contabilidad

La gestión de contabilidad (a veces también referida como gestión de tarifación) es un conjunto de funciones que habilita la medición del uso del servicio de red y la determinación del costo de dicho uso. La gestión de contabilidad debería proveer facilidades para colectar registros de contabilidad y establecer parámetros de tarifación para la utilización del servicio.

En el campo de la gestión de contabilidad, se miden el tiempo y otras características del acceso de red de usuario y se calculan los datos necesarios para cobrar sobre la base de varios parámetros (listas de precios, contratos de cliente, tiempo de uso, servicios utilizados, etc).

La información de tarifación y contabilidad es recolectada, clasificada, y registrada. Sobre esta base, se pueden preparar las facturas y ser enviadas a los clientes, se puede calcular el ingreso redituable y se lo puede asentar.

1.3.1.1.4 Gestión de Rendimiento

La gestión de rendimiento (algunas veces también referida como gestión de tráfico) provee funciones para evaluar y reportar sobre el comportamiento del equipamiento de telecomunicaciones y la efectividad de la red y/o elementos de red. Puede involucrar la medición de la intensidad del flujo de datos (tráfico) a lo largo de las diferentes rutas de la red, coleccionando, evaluando y mostrando los datos medidos de esta forma, así como también la determinación de índices de eficiencia y el cálculo del análisis de tendencia. La información colectada y evaluada en este proceso puede ser utilizada también con los datos colectados en la gestión de fallas.

Sobre la base de estos datos, se puede establecer el nivel de carga de tráfico y se puede determinar si una red dada cumple con los requerimientos de rendimiento necesarios. Si ocurre alguna congestión, las rutas de red sobrecargadas pueden ser aliviadas por una reconfiguración de sistema ó por alteración de la estrategia de ruteo actual. La intervención automática en la operación de la red puede ser ejecutada por el Sistema de Gestión de Red. Si se ha observado una carencia permanente de capacidad de red, se debería tomar la decisión para efectuar nuevas inversiones e incrementar la capacidad de red.

1.3.1.1.5 Gestión de Seguridad

La gestión de seguridad involucra el establecimiento de clases de autenticación, el chequeo de autorización de usuarios para acceder a la red, el control de passwords, y la toma de otras posibles medidas para prevenir de cualquier acceso no autorizado a la red. Puede ser una tarea especial la protección de intervenciones no autorizadas a los terminales de gestión, de acuerdo a los requerimientos de seguridad establecidos. Dependiendo de los requerimientos especiales establecidos en acuerdo con el propósito de una red, las funciones

contenidas dentro de la gestión de seguridad pueden variar de aplicación a aplicación.

1.3.1.2 Modelo Organizacional [29]

Este modelo organizacional se encarga de definir los elementos que participan en la administración de la red, sus roles y las reglas de cooperación entre ellos. El modelo de cooperación para el modelo OSI es de Agente-Gestor (Ver Figura 1.17).

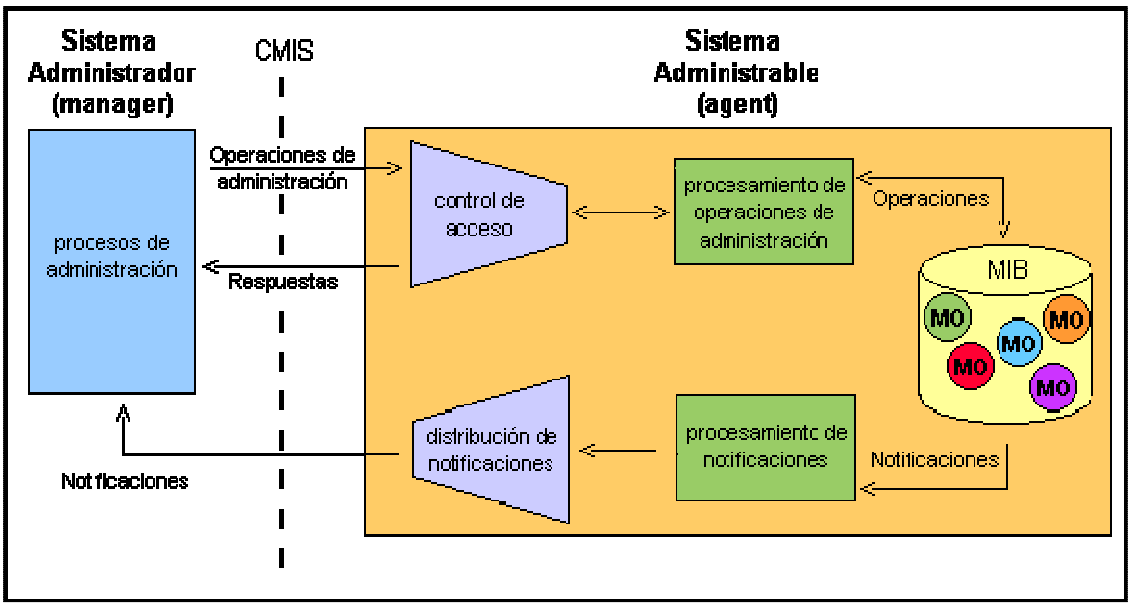


Figura 1.17 Muestra los roles en una administración OSI: un rol de *gestor* y otro de agente [30]

Además, este modelo define los dominios para agrupar los recursos que serán administrados (Ver Figura 1.18). En estos dominios se definen políticas o reglas específicas de administración, las cuales pueden ser por dos motivos principales:

- *Políticas funcionales*. Ejemplo: dominios con una misma política: de seguridad, de contabilidad, etc.)
- *Otras políticas*. Ejemplo: Dominios geográficos, tecnológicos, etc.

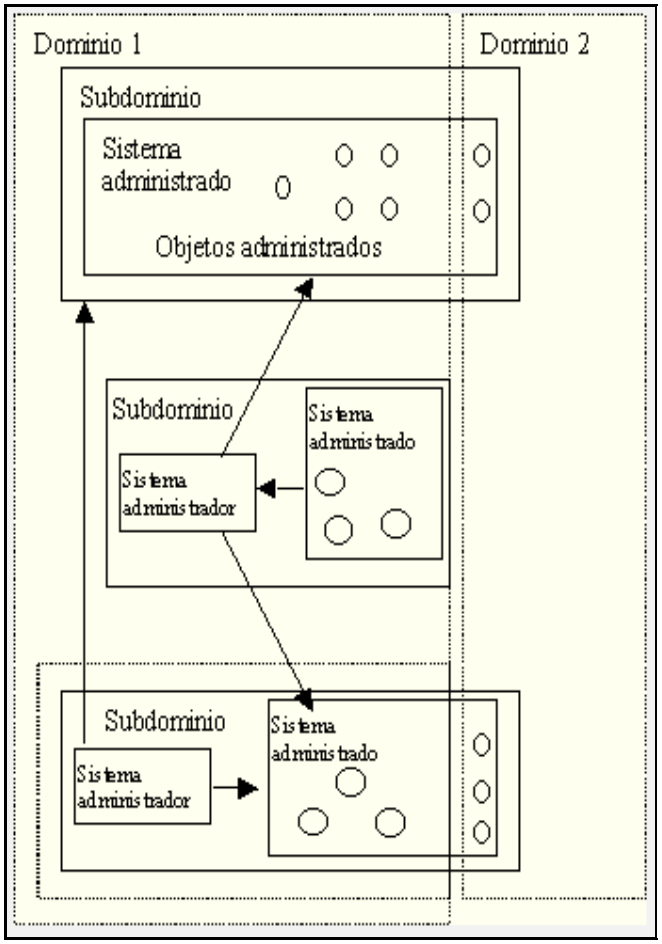


Figura 1.18 La arquitectura de administración OSI distribuida en dominios de administración [31]

Cabe mencionar que dentro de un dominio, se pueden reasignar dinámicamente el papel de gestores y agentes. Los dominios y las políticas son objetos administrables.

1.3.1.3 Modelo de Comunicaciones [32]

Este modelo especifica cómo se lleva a cabo las comunicaciones dentro de la arquitectura OSI. El protocolo utilizado por OSI se denomina *CMIP (Common Management Information Protocol)*, y está definido dentro de la capa de aplicación del modelo OSI, como se muestra en la Figura 1.19.

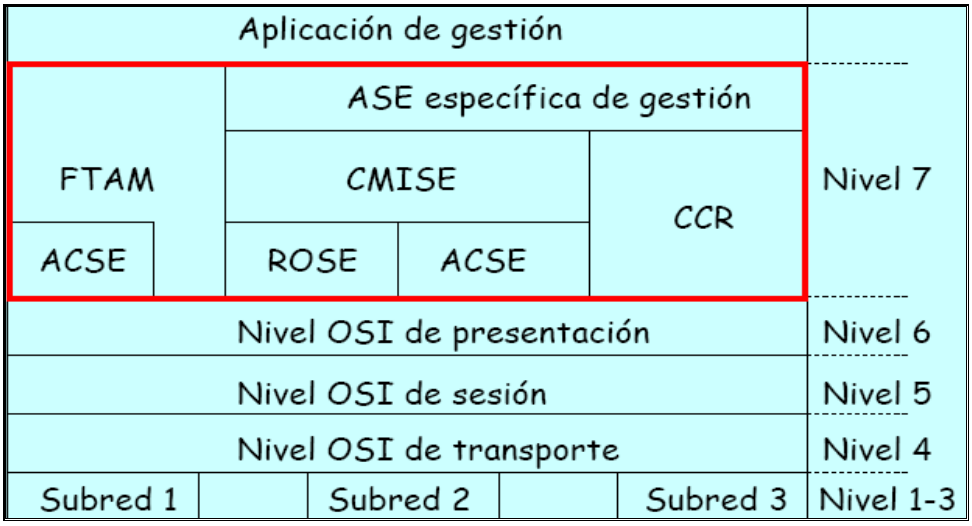


Figura 1.19 Estructura del Modelo de Comunicaciones de OSI [29]

1.3.1.3.1 ASE (Application Service Element) [33]

Se refiere al conjunto de elementos de servicios de aplicación. Una ASE es una parte de una aplicación que se encarga de una tarea en específico.

Existen *ASEs* válidos para varias aplicaciones como las siguientes:

- *ACSE (Association Control Service Element)*. Aplicación para el establecimiento, manejo y liberación ordenada o abrupta de conexiones. Lo utilizan todas las aplicaciones.
- *RTSE (ReliableTransfer Service Element)*. Aplicación que garantiza la fiabilidad en la transferencia de datos, solucionando los problemas que se hayan producido de nivel 4 hacia arriba en el modelo OSI. Se encarga de manejar todas las funciones de nivel 5. Lo utilizan algunas aplicaciones, no todas.
- *ROSE (Remote Operation Service Element)*. Aplicación que facilita el trabajo de petición de operaciones remotas y devolución de los resultados.
- *FTAM. File Transfer, Access and Management.* Aplicación para gestión, acceso y trasferencia de ficheros. Es una norma OSI que juntamente con la transferencia de ficheros ofrece además la posibilidad de acceder a

ficheros ajenos. Fue diseñado para proporcionar un sistema completo de tratamiento de ficheros en un entorno multipropietario.

- *CCR (Commitment, Concurrency and Recovery).* Aplicación para el soporte de las llamadas acciones atómicas (es decir, invisibles). Una acción atómica es aquella que implica a dos o más entidades, que debe desarrollarse sin interferencia de entidades ajenas y, lo más importante, que debe realizarse en su totalidad o no realizarse en absoluto. [34]

1.3.1.3.2 CMISE (Common Management Information Service Element) [32]

La función de intercambio de información entre los gestores y agentes en el sistema de gestión *OSI* se conoce como *CMISE (common management information service element*). *CMISE* se especifica en dos partes:

- *CMIS (common management information service),* que es la interfaz con el usuario, especificando los servicios proporcionados.
- *CMIP (common management information protocol),* que es el protocolo utilizado por el modelo de gestión de sistemas OSI.

a. CMIS (Common Management Information Service)

El CMIS proporciona 7 servicios (Ver Figura 1.20) para realizar operaciones de gestión mediante primitivas de servicio, que son las siguientes:

- *M-EVENT-REPORT*: usado por un agente para notificar la ocurrencia de un evento a un gestor.
- *M-GET*: Usado por un gestor para obtener información de un agente.
- *M-SET*: Usado por un gestor para modificar información de un agente.
- *M-ACTION*: Usado por un gestor para invocar un procedimiento predefinido especificado como parte de un objeto de un agente. La petición indica el tipo de acción y los parámetros de entrada.
- *M-CREATE*: Usado para crear una nueva instancia de una clase de objetos.
- *M-DELETE*: Usado para eliminar uno o más objetos.

- *M-CANCEL-GET*: Usado para finalizar una operación GET larga.

Además para poder realizar operaciones de gestión se necesita establecer asociaciones entre CMISEs. Para ello existen 3 primitivas (Ver Figura 1.20) que proporciona el *ACSE (association-control-service element)* y que pasan de manera transparente el *CMISE*.

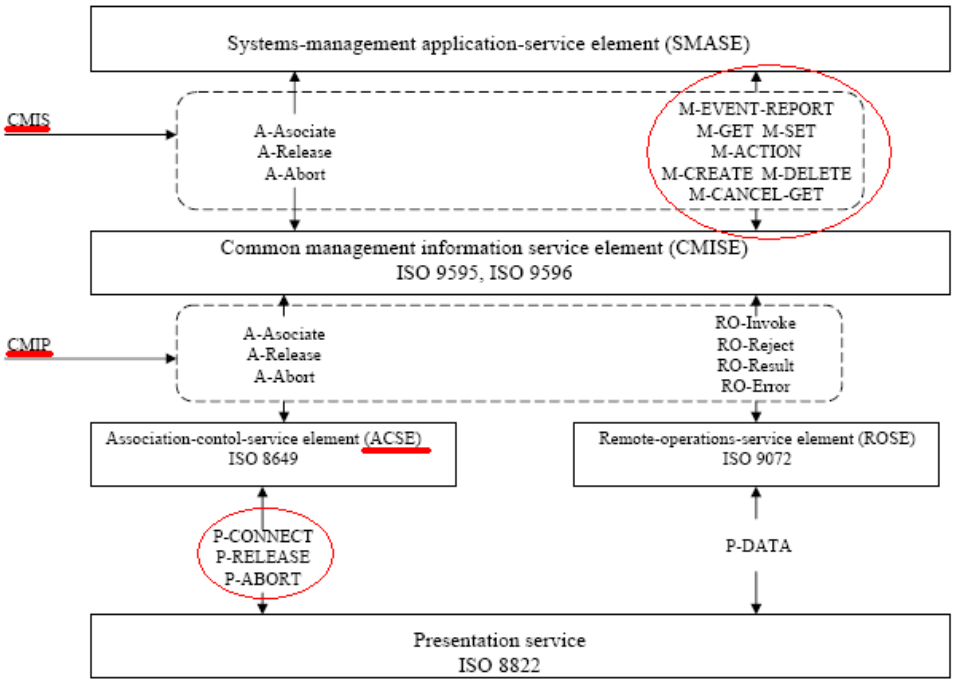


Figura 1.20 Protocolo CMIS/CMIP [32]

Para los servicios de gestión el *CMISE* emplea el *CMIP* para intercambiar *PDUs* (Protocolos de Unidades de Datos), pero para los servicios de asociación no interviene el *CMIP*.

b. CMIP (Common Management Information Protocol)

Entre las características principales de *CMIP* están:

- Sus especificaciones son difíciles de realizar y tediosas de implementar en aplicaciones.

- La comunicación con los agentes está orientada a conexión.
- Su estructura de funcionamiento es distribuida.
- Este protocolo asegura que los mensajes llegan a su destino.

1.3.1.4 Modelo de Información

Este modelo define una estructura (Ver figura 1.21) para la información de gestión que se transmite entre sistemas y su objetivo principal es modelar los aspectos de gestión de los recursos reales de la red gestionada.

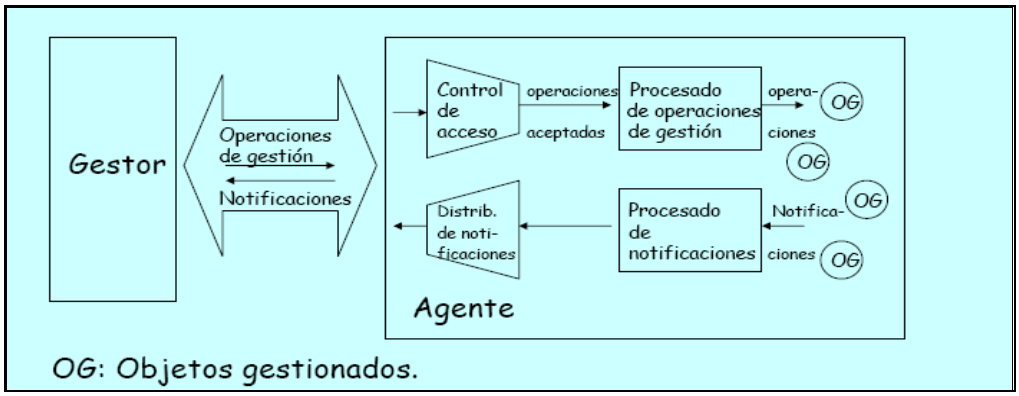


Figura 1.21 Proceso de obtención de la información de gestión de la red [29]

El modelo de información utilizado por el modelo *OSI* hace uso de los principios del diseño orientado a objetos.

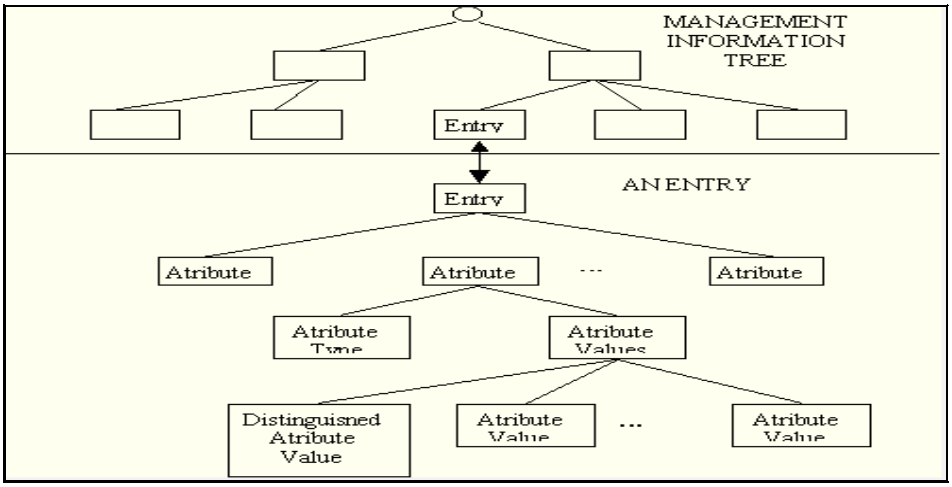


Figura 1.22 Esquema referencial sobre el modelo de información de *OSI* [31]

El modelo de información ofrece un guía para definición de los objetos manejados y sus respectivas interrelaciones, clases, atributos, acciones y nombres (Ver figura 1.22).

1.3.2 MODELO DE GESTIÓN Y ADMNISTRACIÓN TMN (TELECOMMUNICATIONS MANAGEMENT NETWORK)

TMN (TMN: Telecommunications Management Network) es un modelo de gestión estandarizado que permite la construcción de Sistemas de Gestión de Redes formados por un conjunto de funciones de gestión de red que explotan las facilidades de las más actualizadas tecnologías de comunicación.

El modelo *TMN* ha sido adoptado de forma generalizada por los operadores de servicios de telecomunicación como una forma de estructurar lógicamente el soporte de las actividades de su empresa.

Los estándares de gestión de red *TMN* han sido desarrollados con la cooperación de un amplio rango de instituciones de estandarización. Entre las instituciones vinculadas con estas actividades, están:

UIT-T,[3] *ETSI*[4]*, ISO, Network Management Forum, ANSI*[5], etc. Como primer resultado formal en 1988 se publicó la recomendación M.30, la cual fue sustituida por la recomendación M.3010 en el año 1991.

La *UIT-T* define al modelo *TMN* como una red separada de la red de telecomunicación que se conecta con esta última en diferentes puntos para intercambiar información y para controlar las operaciones de la misma. Una *TMN*

[3] UIT-T: Sector de Normalización de las Telecomunicaciones de la UIT (Unión Internacional de Telecomunicaciones) que estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

[4] ETSI: European Telecommunications Standards Institute o Instituto Europeo de Normas de Telecomunicaciones es una organización de estandarización de la industria de las telecomunicaciones, fabricantes de equipos y operadores de redes de Europa

[5] ANSI: American National Standards Institute o 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.

soporta los requisitos de gestión necesarios para planificar, instalar, mantener, operar y administrar redes y servicios de telecomunicación.

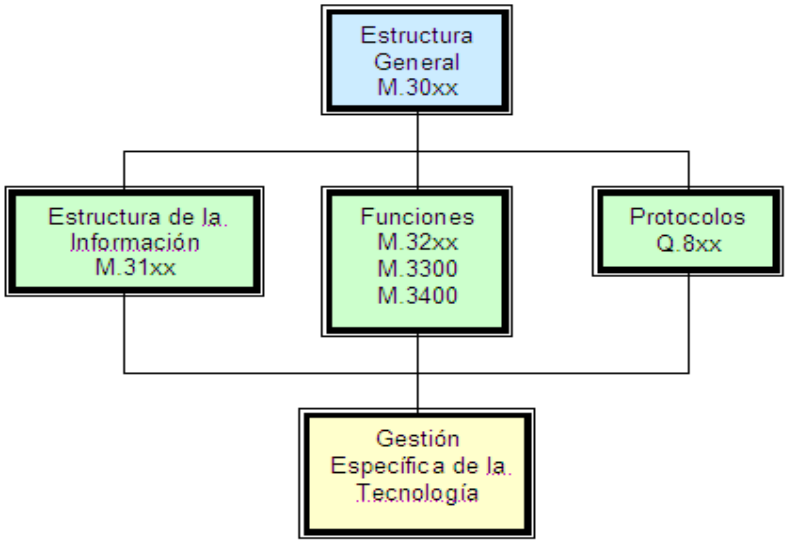


Figura 1.23 Recomendaciones de la UIT-T de las que se compone el Modelo *TMN* [9]

Para el desarrollo del modelo *TMN* se utilizaron varios conceptos del modelo *OSI*, entre los que se encuentran los siguientes:

- Se adoptó el modelo gestor-agente del modelo *OSI*.
- Se siguió el modelo de orientación a objetos de la arquitectura *OSI*.
- Se trabajó conjuntamente en el desarrollo del concepto de dominios de gestión, es decir, particiones administrativas de la red.

La conexión de los sistemas dentro del modelo *TMN* sigue la definición gestor-agente. Para la comunicación entre el gestor y los agentes se hace uso de entidades denominadas “objetos gestionados”, que no es nada más que una representación lógica de los recursos. El modelo *TMN* se basa en cuatro tipos de arquitecturas:

- *Arquitectura funcional*, que describe la distribución de las funciones dentro de *TMN*, con el objetivo de definir los bloques funcionales a partir de los cuales se construye el modelo de gestión *TMN*.
- *Arquitectura física*, que describe los interfaces y el modo en que los bloques funcionales se implementan en los equipos físicos.
- *Arquitectura lógica*, es aquella que proporciona el marco conceptual, con el propósito de organizar de manera sistémica las diferentes funciones dentro de la *TMN*.
- *Arquitectura de la información*, que sigue los principios de los modelos *OSI* de gestión *CMIS* y *CMIP*.

1.3.2.1 Arquitectura Funcional

La arquitectura funcional *TMN* se define desde el punto de vista de los bloques funcionales, que a su vez proveen las funciones que permiten a la *TMN* realizar la gestión. La arquitectura funcional se basa en tres conceptos fundamentales: el bloque funcional, los puntos de referencia, y los componentes funcionales.

1.3.2.1.1 Bloques Funcionales

Los bloques funcionales representan agrupaciones de funciones generales de la TMN, lo que permite un tratamiento modular de la red y con ello la flexibilidad requerida por ella. Los bloques funcionales del modelo son:

- *Bloque Funcional del Sistema de Operaciones (OSF):* Se encarga de procesar la información asociada a alguna aplicación de gestión con el objetivo de monitorear, coordinar y controlar funciones de telecomunicaciones y las funciones de gestión. Se pueden definir múltiples *OSF* dentro de una única *TMN*.
- *Bloque Funcional de Elemento de Red (NEF)*: Este bloque funcional actúa como agente, susceptible de ser monitoreado y controlado.
- *Bloque Funcional de Mediación (MF)*, este bloque funcional actúa sobre la información que pasa entre un *OSF* y un *NEF (o QAF),* adaptándola,

filtrándola o condensándola, a fin de asegurar que sea conforme a las expectativas de los bloques de función enlazados a la MF.

- *Bloque Funcional de Estación de Trabajo (WSF)*: Este bloque funcional proporciona los mecanismos para el intercambio de información de gestión con el usuario de la *TMN*, e incluye el soporte para la interfaz hombre-máquina. Sin embargo, no se considera que estos aspectos formen parte de la *TMN*, por lo que esta parte del WSF aparece representada en el exterior de la frontera de *TMN*. El bloque WSF proporciona los medios para la comunicación entre los bloques funcionales (*OSF, MF, DCF, NEF*) y el usuario.
- *Bloque Funcional de Adaptadores Q (QAF)*: Este bloque funcional se utiliza para conectar a la *TMN* aquellas entidades (hardware y software que reúne, procesa, analiza y presenta la información de red) que no soportan los puntos de referencia estandarizados (más adelante se da el concepto de puntos de referencia) por *TMN*. Esto significa que la información entre un bloque *TMN*-compatible y un bloque de función no-compatible será traducida por el *QAF*, es decir, permite conectar a la *TMN* aquellas entidades funcionales no-*TMN* con funcionalidades análogas a los bloques funcionales *NEF* y *OSF*, realizando la conversión entre un punto de referencia no-*TMN* y un punto de referencia *TMN*.

Los requerimientos de comunicación de estos bloques funcionales son satisfechos por la Función de Comunicación de Datos (*DCF*), aunque esta no sea considerada un bloque funcional en sí, sin embargo, tiene vital importancia para la *TMN*, para transportar, de manera pasiva, la información de gestión intercambiada entre los bloques funcionales. La DCF es la encargada de proveer las funciones de las tres primeras capas del modelo de referencia OSI.

1.3.2.1.2 Puntos de Referencia

Los puntos de referencia son conceptos abstractos que representan fronteras teóricas entre los elementos físicos de una red *TMN*. Los puntos de referencia separan dos bloques funcionales que intercambian información. Los puntos de referencia se representan con letras minúsculas. Las mayúsculas simbolizan las

interfases (corresponden a la arquitectura física) correspondientes a cada punto de referencia.

Se definen tres clases de puntos de referencia estandarizados en *TMN*

- *Puntos de referencia q*: Estos puntos conectan los bloques funcionales NEF-MF, MF-MF, MF-OSF, OSF-OSF, directamente o a través del DCF (Función de Comunicación de Datos).

  El intercambio de datos a través del punto de referencia q se realiza utilizando interfases Q. Existen 2 tipos de interfaces Q en el modelo *TMN*:

  - Q3: es la interfase para trabajar con los protocolos del modelo de referencia OSI de 7 capas.
  - QX: es la interfase para trabajar con las tres capas más bajas del modelo de referencia OSI.

- *Puntos de referencia f*: Estos puntos conectan los bloques funcionales OSF-WSF, MF-WSF, NEF, DCF al WSF. La interfase F permite el intercambio de datos a través de un punto de referencia f, y se usa en casos en que la WSF no está conectada directamente al OSF, sino a través de la DCN.

- *Puntos de referencia x*: Se encuentran ubicados para conectar bloques de función *OSFs* de dos *TMN*s o bloques *OSF* (*TMN*) – *OSF* (no *TMN*). Puede ser encontrado entre las *DCNs* de dos *TMN*s, ó entre una *TMN* y otro sistema gestionado que no cumple los estándares *TMN.* Además, el interface X permite el intercambio de datos entre dos sistemas de gestión de red.

La recomendación M.3010 también define dos puntos de referencia adicionales, ubicados fuera del área de los elementos estándares de *TMN*. Estos puntos de referencia no-*TMN* son los siguientes:

- *Puntos de referencia g*: Son los puntos entre el WSF y el usuario (el humano).
- *Puntos de referencia m*: Son los puntos de referencia ubicados entre la QAF y un elemento/bloque no-*TMN*.

DESCRIPCIÓN DE LOS BLOQUES FUNCIONALES		DESCRIPCIÓN DE LOS PUNTOS DE REFERENCIA	
OSF	Función de Sistema de Operaciones	**q_3**	Entre OSF y MF, QAF o NEF
MF	Función de Mediación	**q_x**	Entre MF y QAF o NEF
QAF	Función de Adaptador Q	**f**	Para conectar una WSF
WSF	Función de Estación de Trabajo	**x**	Entre dos OSF de dos *TMN*
NEF	Función de Elemento de Red	**g**	Entre la WSF y el usuario
		m	Entre la QAF y entidades no *TMN*

Tabla1.1 Relación entre Bloques Funcionales y Puntos de Referencia [15]

	NEF	**OSF**	**MF**	**QAF(q_3)**	**QAF(q_x)**	**WSF**	**no-TMN**
NEF		q_3	q_x				
OSF	q_3	x^*, q_3	q_3	q_3		F	
MF	q_x	q_3	q_x		q_x	F	
QAF(q_3)		q_3					M
QAF(q_x)			q_x				M
WSF		f	f				G^{**}
no-TMN				m	m	g^{**}	

***El punto de referencia X solo aplica cuando cada OSF está en una *TMN* diferente.

**El punto de referencia g se sitúa entre el WSF y el usuario, quedando fuera del estándar.

Tabla 1.2 Se especifican los puntos de referencia posibles entre los distintos bloques funcionales [35]

La figura 1.24 presenta la arquitectura funcional de la *TMN*, con los bloques funcionales y los puntos de referencia asociados:

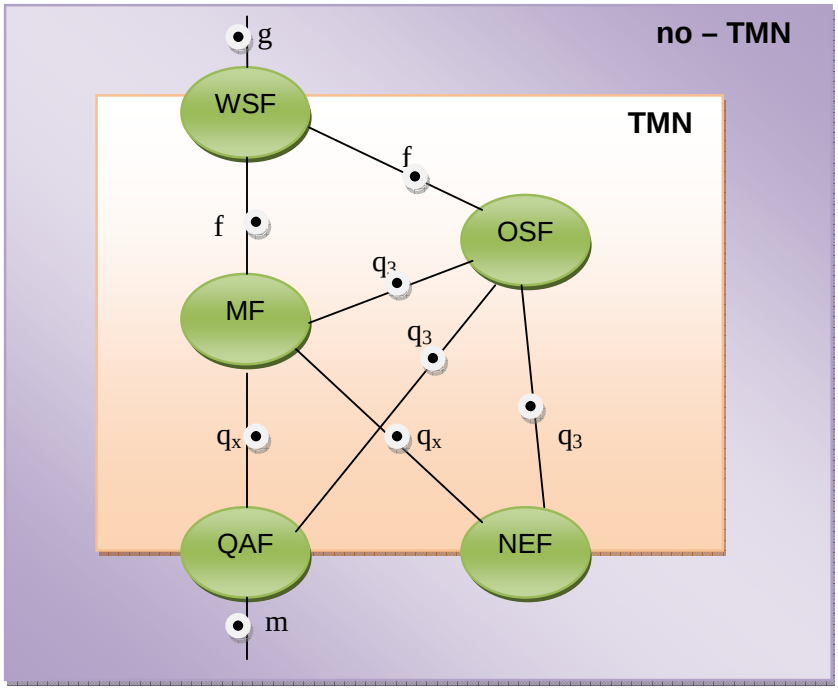


Figura 1.24 Arquitectura funcional de *TMN* [15]

1.3.2.2 Arquitectura Física

La arquitectura física de la *TMN* se encarga de definir cómo se implementan los bloques funcionales mediante equipamiento físico y los puntos de referencia en interfaces.

1.3.2.2.1 Bloques Constructivos

En la arquitectura física se definen los siguientes bloques constructivos:

- Sistema de operaciones (SO).
- Estación de Trabajo (ET).
- Elemento de red (ER).
- Dispositivo de mediación (DM).

- Adaptador Q (AQ).
- Red de comunicación de datos (RCD).

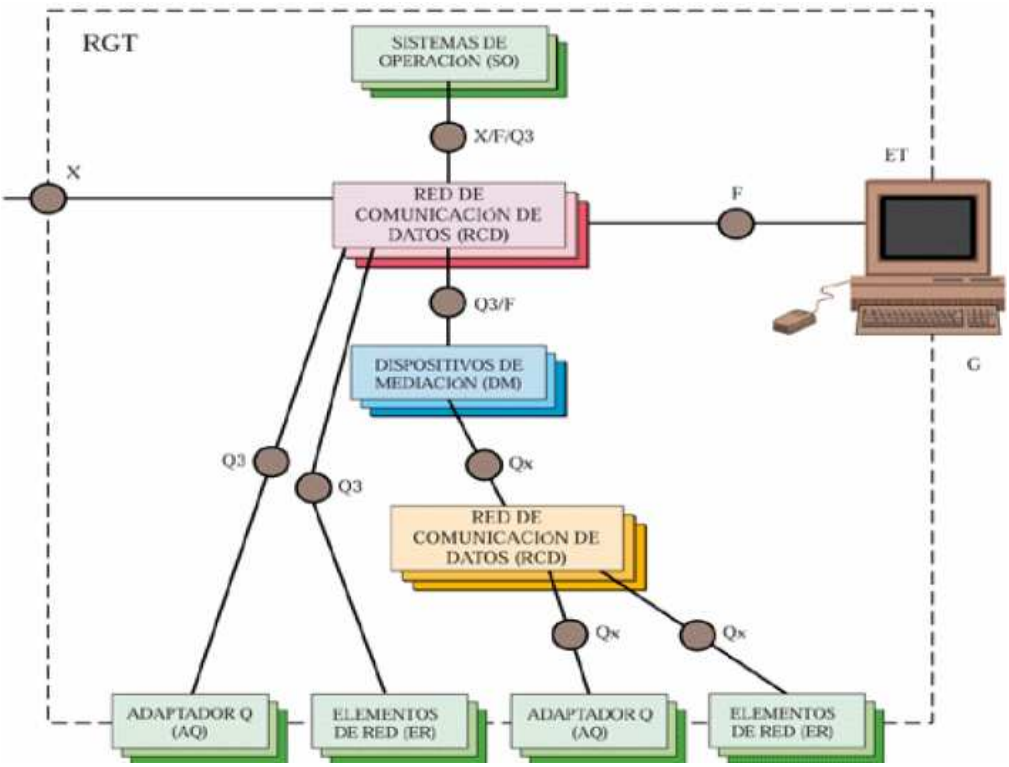


Figura 1.25 Arquitectura Física de la Gestión de red *TMN* [19]

Cada uno de estos bloques puede implementar uno o más bloques funcionales (excepto el RCD que se encarga de realizar el intercambio de información entre bloques), pero siempre hay un bloque funcional que ha de contener obligatoriamente y que determina su denominación.

- *Sistema de Operación (SO)*, se encarga de ejecutar las funciones del sistema de operación. El SO interactúa con los Elementos de Red (ER) para recolectar la información necesaria para las funciones de supervisión (canalización, filtrado de alarmas y monitorización), operación (configuraciones de red, restauración en caso de fallo, etc.), y administración (medidas de tráfico, facturación, estadísticas, etc.) de la red.

Más de un sistema de operación puede participar en los procesos de gestión. Y, por el principio de división de tareas pueden todos estos SOs estar comunicados a través de la red de comunicación de datos (RCD).

- *Estación de Trabajo (ET)*. Soportan la interacción entre los Sistemas de Operación y el Personal encargado de la gestión de red. Generalmente las ET son computadoras equipadas con capacidades gráficas, a través de las cuales, los operadores pueden comunicarse con la red *TMN*.

- *Elementos de Red (ER)*. Los ER son dispositivos de telecomunicaciones gestionables, ubicados en los nodos de la red a ser gestionada. Los elementos de red a través de la interfase estándar pueden transferir mensajes hacia la estación de operación para informarle del estado actual de los elementos, y recibir comandos de control desde ella.

- *Dispositivo de Mediación (DM)*. Los dispositivos de mediación (DM) ejecutan funciones de mediación, como convertir los protocolos e información para la comunicación entre los Sistemas de Operación (SO) y los Elementos de Red (ER) o Adaptadores-Q (AQ). Además, también adaptan la información transferida entre un SO ó la RCD y aquellos elementos *TMN*-compatibles ubicados en la red.

- *Adaptadores-Q (AQ)*. Los Adaptadores-Q proveen interfases-*TMN* para Elementos de Red (ER) que no soportan tales interfases.

- *La red de comunicación de datos (RCD)*. La RCD es una red que ejecuta la función de comunicación de datos (DCF), y se encarga de transmitir los mensajes para ejecutar funciones de gestión entre un SO y ER. La RCD es una red que puede ser implementada de manera separada de la red de telecomunicaciones gestionada y dar la ventaja que los problemas en la red a gestionar no afectarán a la funcionalidad del sistema de gestión, sin embargo, se presenta la necesidad de una inversión más alta, mayores

costes de mantenimiento y un sistema global más complejo como desventajas.

1.3.2.2.2 Interfases

Los interfaces son implementaciones de los puntos de referencia, y son comparables a las pilas de protocolos.

Existe una correspondencia uno a uno entre los puntos de referencia y los interfaces, excepto para aquellos que están fuera de la *TMN*, es decir, los puntos de referencia g y m. *TMN* soporta un conjunto de interfaces normalizados, que son los siguientes:

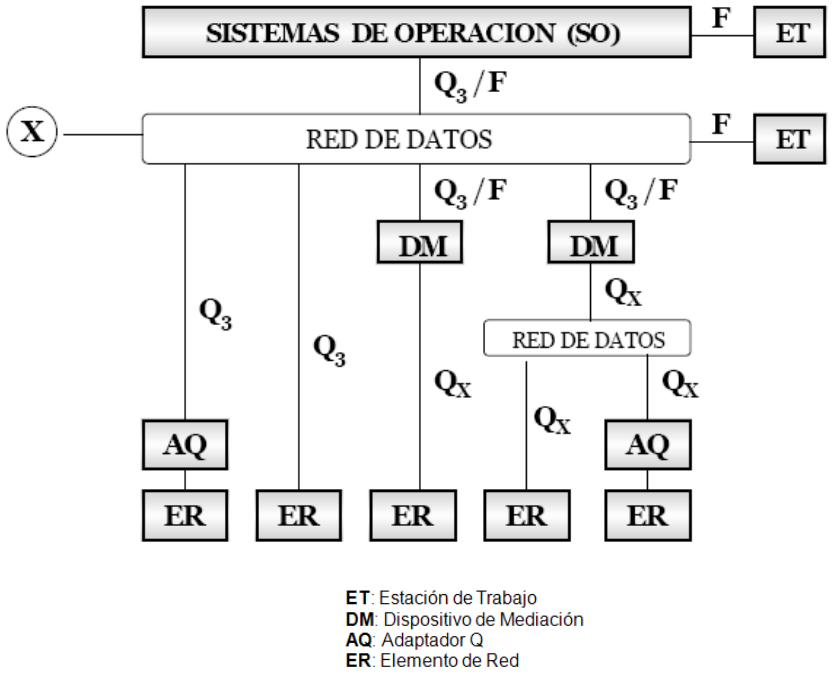


Figura 1.26 Arquitectura Física y Funcional de *TMN* [8]

- *Interfaz Q_3*: Es la interfaz que soporta la comunicación entre los Sistemas de Operación (SO) y los Elementos de Red (ER), directamente o a través de los Dispositivos de Mediación (DM) o Adaptadores-Q (AQ). Es el interfaz más desarrollado de la arquitectura-*TMN*.

- *Interfaz Q_X*: Es una interfaz menos elaborada que el Q_3, ideado para facilitar la interconexión en situaciones donde no parece viable implementar la complejidad del Q_3. Esta interfaz soporta la comunicación entre los Dispositivos de Mediación (DM) y los Elementos de Red (ER), directamente o a través de un Adaptador-Q.

- *Interfaz F*: Es la interfaz que soporta la comunicación entre los Sistemas de Operación (SO) y las Estaciones de Trabajo (ET).

- *Interfaz X*: Es la interfaz que soporta la comunicación ya sea entre distintos Sistemas de Operación (SO) o entre un Sistema de Operación y un Sistema ajeno a la arquitectura-*TMN*.

1.3.2.3 Arquitectura Lógica de Niveles TMN *(LLA: Logical Layered Architecture)*

Este modelo estratifica y jerarquiza los servicios de gestión que soporta, articulándolos en una estructura de cinco niveles (Figura 1.27), los cuales se construyen uno sobre la base del otro. [36]

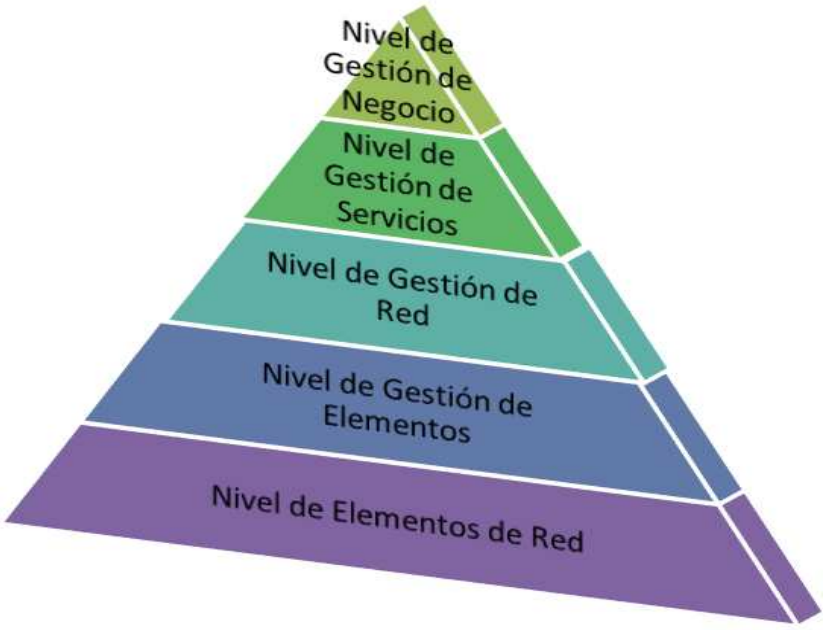


Figura 1.27 Arquitectura Lógica de Niveles *TMN* [1]

Se definen los siguientes niveles:

- Nivel de Elementos de Red.
- Nivel de Gestión de Elementos.
- Nivel de Gestión de Red.
- Nivel de Gestión de Servicios.
- Nivel de Gestión de Negocio.

1.3.2.3.1 Nivel de Elementos de Red

El elemento de red, es el agente de gestión en efecto. Este comprende la funcionalidad de gestión que el elemento de red en sí soporta, independientemente de cualquier sistema de gestión.

El elemento de red es la base de toda la jerarquía de gestión, el resto de capas se construyen sobre ella. Esta capa juega un papel muy importante para la eficacia de un sistema de gestión.

1.3.2.3.2 Nivel de Gestión de Elementos

Este nivel comprende la gestión individual de los dispositivos de la red y que estos se mantengan funcionando correctamente.

En este nivel se encuentran las funciones para ver y cambiar las configuraciones de los elementos, para monitorear los mensajes de alarmas emitidos por los elementos en la red, y para instruir a los elementos de red a correr los *self tests* (auto-diagnósticos).

1.3.2.3.3 Nivel de Gestión de Red

Incluye el control, supervisión, coordinación y configuración de grupos de elementos de red, no solo de elementos individuales como se realizaba en la capa anterior. Con este nivel se asegura la integridad de la red de forma global, ya que es responsable de la cooperación de todos los elementos de red en el sistema gestionado.

1.3.2.3.4 Nivel de Gestión de Servicio

Incluye las funciones que proporcionan un manejo eficiente de las conexiones entre los puntos finales de la red, asegurando un óptimo aprovisionamiento y configuración de los servicios prestados a los usuarios.

1.3.2.3.5 Nivel de Gestión de Negocio

Incluye la completa gestión de la explotación de la red, incluyendo contabilidad, gestión y administración, basándose en las entradas procedentes de los niveles de Gestión de Servicios y de Gestión de Red.

1.3.2.3.6 Modelo TMN redefinido con el modelo FCAPS

Las funciones de gestión de red *TMN* son clasificadas por la recomendación M.3400, en donde se especifica como *TMN* utiliza como parte de su estructura lógica al modelo *FCAPS (Fault, Configuration, Accounting, Performance, Security)* para categorizar las funciones de gestión las áreas de fallos, de configuración, de contabilidad, de desempeño y de seguridad, como ya se explicó previamente con detalle en el modelo OSI.

Cada una de estas áreas funcionales se puede encontrar a su vez en cada una de las capas del modelo lógico jerárquico de la *TMN*, como se muestra en la figura 1.28.

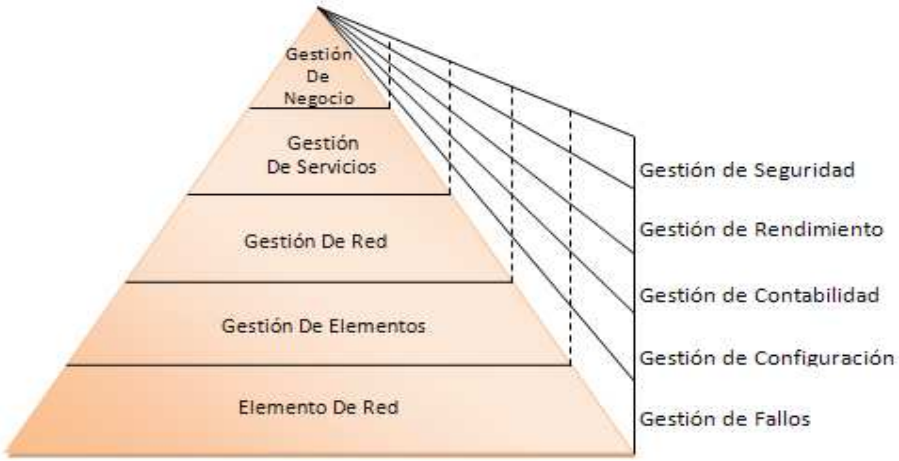


Figura 1.28 Modelo de gestión *TMN* redefinido con el modelo FCAPS [1]

1.3.2.4 Arquitectura de la Información [9]

La gestión de red involucra el intercambio de información entre procesos de gestión, y para esto *TMN* utiliza un modelo de información de gestión que se basa, en su mayor parte, sobre el modelo de gestión de red OSI/CMIP.

La arquitectura de información de *TMN* se basa en modelo orientado a objeto, y utiliza el principio de agente-gestor.

Los conceptos básicos usados en la definición de la arquitectura de información de *TMN* son similares a aquellos aplicados en SNMP y OSI/CMIP: Ello son:

- Objeto Gestionado (*Managed Object: MO*).
- Agente (*Agent*).
- Gestor (*Manager*).
- Base de Información de Gestión (*Management Information Base: MIB*).

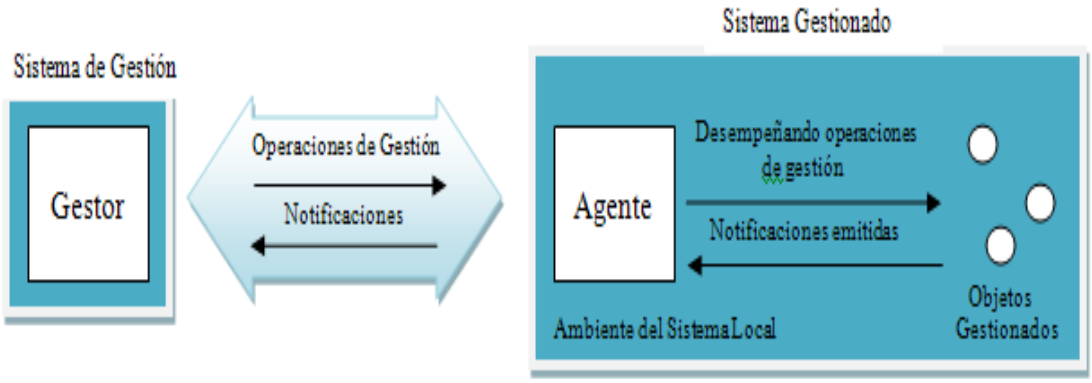


Figura 1.29 Interacción entre el gestor, el agente y los objetos gestionados [37]

La interacción entre un agente, un gestor, y los objetos gestionados de acuerdo a ITU-T M.3010 se muestra en la figura 1.29.

El gestor y el agente se comunican utilizando protocolos “Q” estándares construidos de acuerdo al modelo de comunicación de siete capas de OSI.

Los componentes de un protocolo Q son:

- Interfase de aplicación (estructura comando/respuesta).
- Protocolo de aplicación (la séptima capa del modelo OSI).
- Protocolos de soporte (capas 4-6 del modelo OSI).
- Protocolos de red (capas 1-3 del modelo OSI).

Los elementos esenciales de la interfase de aplicación *TMN* son altamente similares a aquellos mencionados en el modelo de gestión OSI/CMIP mencionados anteriormente.

1.3.3 MODELO DE GESTIÓN DE RED DE TELECOMUNICACIONES TOM (*Telecom Operations Map*) y e-TOM (*enhanced-Telecom Operations Map*) [38] [39]

TOM (*Telecom Operations Map*) o Mapa de Operaciones de Telecomunicaciones, es un modelo de gestión de red desarrollado por la *TeleManagement Forum* (forma parte de la UIT-T) principalmente enfocado a la gestión de servicios empresariales. Este modelo es un marco referencial que posee información fundamental para el mundo de telecomunicaciones y pretende entre otras cosas, estandarizar los conceptos de los procesos, dar estructura coherente a los procesos de una empresa de telecomunicaciones.

El modelo e-TOM o Mapa de Operaciones de Telecomunicaciones Mejorado, es la actual versión de este modelo. En el 2004 el modelo e-TOM fue estandarizado como Recomendación Internacional de la UIT-T M.3050.

El Mapa de Operaciones de Telecomunicaciones mejorado (e-TOM), es parte de la caja de herramientas del NGOSS[6] y brinda un marco referencial de trabajo de procesos empresariales para ser utilizado por los prestadores de servicios y sus proveedores dentro de la industria de las telecomunicaciones.

[6] NGOSS: New Generation Operations Systems and Software o Nueva Generación a los Sistemas de Soporte de Operaciones. NGOSS es un conjunto de modelos y recomendaciones definidos por TeleManagement Forum, convertidos en estándares de facto para el sector de las telecomunicaciones.

e-TOM analiza los procesos empresariales con diverso nivel de detalle de acuerdo a su significación y prioridad para la empresa. El modelo TOM limitaba su alcance a procesos operacionales, en cambio en su nueva versión e-TOM además cubre procesos de gestión empresarial, de mercadeo, retención de clientes, relación con suministradores y socios. [40] El modelo e-TOM se encuentra organizado en tres áreas de procesos (Ver figura 1.30):

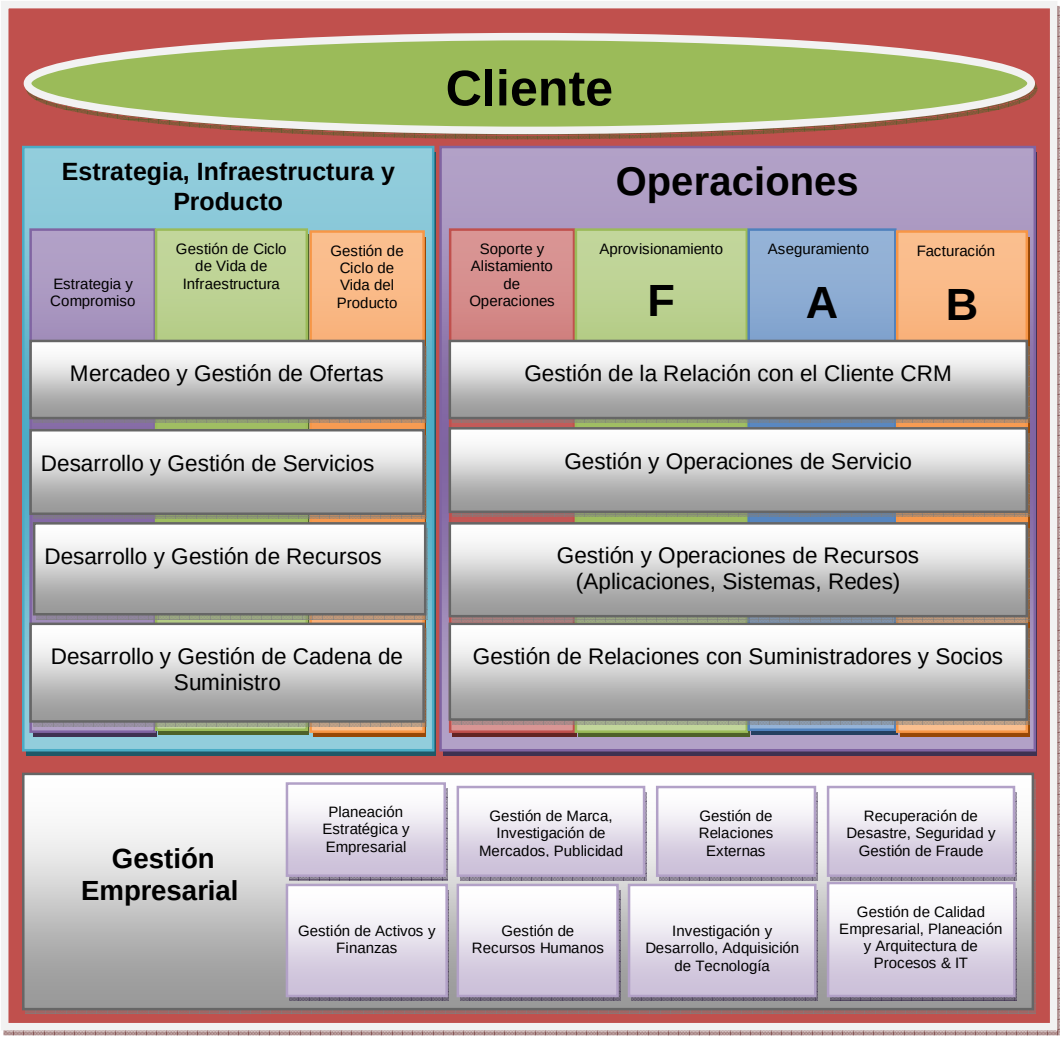


Figura 1.30 Estructura del Modelo e-TOM y sus áreas de procesos [41]

1.3.3.1 Área de Procesos de Estrategia, Infraestructura y Producto [39]

Esta área cubre la planeación y la gestión de los ciclos de vida (definición, planeación, diseño e implementación). El e-TOM agrega esta área al mapa de

procesos, con el propósito de destacar la planeación y desarrollo de los procesos operacionales que están más relacionados con el día a día del negocio.

1.3.3.1.1 Agrupamiento vertical de los Procesos de Estrategia, Infraestructura y Producto [39]

Los Procesos de Estrategia y Compromiso, junto con los dos Agrupamientos de Procesos de Gestión de Ciclos de Vida, son presentados como tres agrupamientos de procesos *end-to-end* verticales.

Los procesos de Estrategia y Compromiso proveen el enfoque dentro de la empresa para la generación de la estrategia de negocio específica y la obtención de capacidades para ésta.

Los procesos de Gestión del Ciclo de Vida de Infraestructura y de Gestión del Ciclo de Vida del Producto dirigen y soportan la provisión de productos a los clientes. Su enfoque es el cumplimiento de las expectativas del cliente, ya sea como ofertas de productos, como la infraestructura que soporta las funciones de operaciones y los productos, o como los proveedores o aliados involucrados en las ofertas de empresa a los clientes.

- *Estrategia y Compromiso.* Este conjunto de procesos encierra todos los niveles de la operación desde el mercado, el cliente y los productos, a través de los servicios y los recursos de los cuales éstos dependen, hasta la vinculación de proveedores y aliados en el cumplimiento de estas necesidades.
- *Gestión del Ciclo de Vida de Infraestructura.* Este conjunto de procesos es responsable de la definición, planeación e implementación de todas las infraestructuras necesarias (aplicaciones, computación y redes), como también todas aquellas otras infraestructuras de soporte y capacidades de negocios (centros de operaciones, arquitecturas, etc.). Esto aplica en conexión con el nivel de recursos o cualquier otro nivel funcional, como por ejemplo, las Unidades de Respuesta de Voz de *CRM (Customer Relationship Management)*, requeridas para proveer productos de Información y Comunicaciones al Cliente y para soportar el negocio. Estos

procesos identifican nuevos requerimientos, nuevas capacidades, y diseñan y desarrollan infraestructura nueva o mejorada para soportar productos. Los procesos de la Gestión del Ciclo de Vida de Infraestructura responden a las necesidades de los procesos de la Gestión del Ciclo de Vida del Producto, ya sea para reducción de costos por unidad, mejoramiento de la calidad de los productos, nuevos productos, etc.

- *Gestión del Ciclo de Vida del Producto.* Este conjunto de procesos es responsable por la definición, la planeación, el diseño y la implementación de todos los productos del portafolio de la empresa. Los procesos de la Gestión del Ciclo de Vida del Producto gestionan productos para márgenes requeridas de ganancias y pérdidas, satisfacción del cliente y compromisos de calidad, como también la entrega de nuevos productos al mercado. Estos procesos de ciclo de vida entienden el mercado a través de todas las áreas funcionales claves, el ambiente del negocio, los requerimientos de los clientes y las ofertas competitivas, con el propósito de diseñar y gestionar productos exitosos en sus mercados específicos. Los procesos de Gestión de Productos y de Desarrollo de Productos son dos tipos de procesos distintos. El Desarrollo de Productos es un proceso predominantemente orientado a proyectos que desarrolla y entrega nuevos productos para los clientes, como también nuevas características y mejoramientos para los productos y servicios existentes.

1.3.3.1.2 Agrupamiento horizontal de los Procesos de Estrategia, Infraestructura y Producto [39]

- *Gestión de Mercadeo y Ofertas.* Estos procesos se enfocan en el conocimiento de la ejecución y el desarrollo del *Core Business* para una Empresa *ICSP (Information and Communications Service Provider).* Incluye funcionalidades necesarias para la definición de estrategias, el desarrollo de nuevos productos, la gestión de los productos existentes y la implementación de estrategias de mercadeo y ofertas, especialmente adecuadas para los productos y servicios de información y comunicaciones.

- *Desarrollo y Gestión de Servicios.* Estos procesos se enfocan en la planeación, el desarrollo y la entrega de servicios al dominio de las Operaciones. Incluye funcionalidades necesarias para la definición de estrategias para la creación y el diseño de servicios, la gestión y el diagnóstico del desempeño de servicios existentes, y el aseguramiento de que las capacidades están dispuestas para satisfacer la demanda futura de servicios.
- *Desarrollo y Gestión de Recursos.* Estos procesos se enfocan en la planeación, el desarrollo y la entrega de los recursos necesarios para soportar los servicios y productos para el dominio de las Operaciones. Incluye funcionalidades necesarias para la definición de estrategias para el desarrollo de la red y otros recursos físicos y no físicos, la introducción de nuevas tecnologías y la interacción con las existentes, la gestión y el diagnóstico del desempeño de los recursos existentes y el aseguramiento de que las capacidades están dispuestas para satisfacer las necesidades futuras de los servicios.
- *Desarrollo y Gestión de la Cadena de Suministro.* El enfoque de estos procesos es el conjunto de interacciones requeridas por la empresa con sus proveedores y aliados, quienes están involucrados en el mantenimiento de la cadena de suministro. La cadena de suministro es una red compleja de relaciones que un proveedor de servicios maneja para proveer y entregar productos.

1.3.3.2 Área de Procesos de Operaciones [39]

Esta área cubre el núcleo de la gestión operacional. El e-TOM recoge los procesos operacionales establecidos por el TOM, los cuales constituyen los flujos de procesos “end-to-end o extremo a extremo”. Estos flujos de procesos son un modelo complementario que se conoce como *FAB (Fulfillmet, Assurance, Billing*) o Aprovisionamiento, Aseguramiento, y Facturación que se agrupan en el área de Operaciones del nuevo mapa.

La visión de e-TOM de las Operaciones también incluye la gestión de ventas y la gestión de las relaciones con el proveedor.

1.3.3.2.1 Agrupamiento vertical de los procesos operacionales [39]

Él área de procesos de Operaciones contiene los agrupamientos verticales de los procesos directos de operaciones de Aprovisionamiento, Aseguramiento y Facturación, junto con el agrupamiento de los procesos de Soporte y Alistamiento de Operaciones. Aquí se ven reflejados los procesos *FAB (Fulfillment, Assurance, Billing)*, que algunas veces son referidos como procesos de Operaciones del Cliente.

- *Aprovisionamiento.* Este proceso es responsable de proveer a los clientes sus productos requeridos de manera oportuna y correcta. Traduce la necesidad de negocio o personal del cliente en una solución, la cual puede ser entregada usando productos específicos del portafolio de la empresa. Este proceso informa a los clientes el estado de su orden de compra, asegura la terminación oportuna, así como también un cliente satisfecho.
- *Aseguramiento.* Este proceso es responsable de la ejecución de las actividades proactivas y reactivas de mantenimiento, para asegurar que los servicios provistos a los clientes estén disponibles continuamente, y para mantener los niveles de *QoS* (Calidad de Servicio). Realiza un monitoreo continuo del estado y del desempeño de los recursos para detectar proactivamente posibles fallas. Recoge datos de desempeño y los analiza para identificar problemas potenciales y resolverlos sin impacto al cliente. Recibe los reportes de problemas desde los clientes, informa a los clientes sobre el estado del problema, y asegura la restauración y reparación, como también la satisfacción del cliente.
- *Facturación.* Este proceso es responsable de la producción oportuna y correcta de facturas, de la provisión de información pre-facturación de uso, y de la facturación a los clientes, del procesamiento de sus pagos, y del recaudo de los mismos. Adicionalmente, maneja las consultas de los clientes sobre facturación, provee el estado de dichas consultas y es responsable de resolver los problemas de facturación para la satisfacción de los clientes de una manera oportuna. Este proceso también soporta el prepago de servicios.

- *Soporte y Alistamiento de Operaciones.* Es responsable de soportar los procesos “FAB”, y de asegurar el alistamiento operacional en las áreas de aprovisionamiento, aseguramiento y facturación. En términos generales, los procesos tienen que ver con las actividades que son de menos “tiempo real” que las de FAB, y las cuales son típicamente menos relacionadas con clientes y servicios individuales y más relacionadas con los grupos de éstos. Ellos reflejan una necesidad en algunas empresas por dividir sus procesos entre el contacto directo con el cliente y las operaciones de tiempo real de FAB y otros procesos de Operaciones que actúan como una “segunda línea” para llevar a cabo las tareas operacionales. No todas las empresas escogen emplear esta división, o colocar la división exactamente en el mismo sitio, de tal manera que es posible que en algunos escenarios los procesos de Soporte y Alistamiento de Operaciones se encuentren inmersos en los procesos FAB.

1.3.3.2.2 Agrupamiento horizontal de los procesos operacionales [39]

En el área de procesos Operacionales del eTOM, hay cuatro agrupamientos de procesos funcionales de Operaciones que soportan los procesos de Aprovisionamiento, Aseguramiento y Facturación, así como también la gestión de las operaciones para soportar los clientes, el servicio, los recursos y las interacciones con el proveedor/aliado.

El TOM original usó los niveles lógicos de Negocios, de Servicios y de Red del TMN para organizar los procesos del núcleo del negocio.

- *Gestión de las Relaciones con el Cliente (CRM).* Comprende el conocimiento fundamental de las necesidades de los clientes e incluye todas las funcionalidades necesarias para la adquisición, ampliación y retención de una relación con un cliente. Trata acerca del servicio y soporte al cliente, ya sea en centros de atención, por teléfono, web o servicio en campo. CRM incluye la recolección de la información de los clientes y su aplicación para personalizar e integrar la entrega de los servicios al cliente, como también para identificar oportunidades para incrementar el valor del cliente para la

empresa. La introducción de CRM es una característica clave del e-TOM sobre TOM.

- *Gestión y Operaciones de Servicios.* Se enfoca en el conocimiento de los servicios (acceso, conectividad, contenido, etc.) e incluye todas las funcionalidades necesarias para la gestión y las operaciones de comunicaciones y los servicios de información requeridos por los clientes, o propuestos por ellos. El enfoque es en la entrega y gestión de los servicios, y no en la gestión de la red y la tecnología de información subyacentes. Algunas de las funciones involucran planeación a corto plazo de las capacidades del servicio, la aplicación de un diseño del servicio a clientes específicos o la gestión de iniciativas de mejoramiento del servicio. Estas funciones están íntimamente conectadas con la experiencia diaria del cliente.
- *Gestión y Operaciones de Recursos.* Este conjunto de procesos mantiene el conocimiento de los recursos (aplicaciones, computación e infraestructura de red) y es responsable de la gestión de todos los recursos (Ej. redes, sistemas de TI, servidores, enrutadores, etc.) utilizados en la entrega y soporte de los servicios requeridos por los clientes, o propuestos por ellos. También incluye todas las funcionalidades responsables de la gestión directa de todos esos recursos utilizados en la empresa. Estos procesos son responsables de asegurar que la infraestructura de red y de tecnologías de información soporte la entrega diaria de los servicios requeridos. La misión de estos procesos es asegurar que la infraestructura funcione sin contratiempos, sea accesible a los servicios y empleados, sea mantenida y responda a las necesidades, directas o indirectas, de los servicios, clientes y empleados.
- *Gestión de las Relaciones con el Proveedor/Aliado.* Soporta los procesos operacionales básicos, los procesos de Aprovisionamiento, Aseguramiento y Facturación de instancias del cliente, y los procesos funcionales de operaciones. Estos procesos se alinean fuertemente con los procesos de Gestión de las Relaciones con el Cliente del proveedor o del aliado. La existencia de estos procesos permite las operaciones *end-to-end* con el cliente o los procesos funcionales con los proveedores o aliados.

1.3.3.3 Área de Procesos de Gestión Empresarial [39]

Esta área cubre la gestión de soporte al negocio. En esta área se concentran los procesos que toda empresa debe tener para su normal funcionamiento. Estos procesos se enfocan en los procesos a nivel de la empresa, metas y objetivos. Estos procesos tienen relación con casi todos los demás procesos en la empresa, ya sean operacionales, de producto o de infraestructura. Dentro de estos procesos, se encuentran los siguientes:

- *Planeación Estratégica y Empresarial.* Se enfoca en los procesos requeridos para desarrollar las estrategias y planes para la empresa, incluyendo la disciplina de planeación estratégica; determinan el negocio y el enfoque de la empresa, incluyendo los mercados que se tienen como objetivo, requerimientos financieros por satisfacer, posibles adquisiciones que mejoren la posición financiera o de mercado de la empresa.
- *Gestión de Marcas, Investigación de Mercados y Publicidad.* Se enfocan en los procesos de Mercadeo Corporativo. Dirigen y soportan los procesos de Mercadeo en las áreas de Estrategia, Infraestructura y Producto, y Operaciones de la empresa. También desarrollan y aseguran el fortalecimiento de la marca o marcas de la empresa. Además, se encargan de la investigación de mercados, diagnóstico de la investigación de mercados, identificación de cambios de mercado, cambios en la satisfacción del cliente, entre otros. También incluyen procesos que desarrollan y ejecutan las estrategias de publicidad en el soporte de toda la empresa, de unidades de negocio y de productos específicos.
- *Gestión de la Calidad Empresarial, Planeación y Arquitectura de Procesos y Tecnología Informática.* Este conjunto de procesos se dedica al desarrollo y mejoramiento las arquitecturas claves de la empresa, así como en la definición de los procesos y políticas de gestión de calidad de la empresa. Los procesos de planeación de la TI (Tecnología Informática) dirigen esta tecnología a través de toda la empresa, provee las guías y políticas de TI, la aprobación de los respectivos presupuestos, etc. Los procesos de desarrollo y gestión de la Tecnología Informática son gestionados en el nivel de procesos de Recursos.

- *Investigación y Desarrollo, Adquisición de Tecnología.* Estos procesos realizan la investigación y el desarrollo de la tecnología dentro de la empresa, y la evaluación de las potenciales adquisiciones de tecnología.
- *Gestión Financiera y de Activos.* Este conjunto de procesos se enfoca en la gestión de las finanzas y los activos de la empresa.
- *Gestión de las Relaciones Externas y con los Accionistas.* Este conjunto de procesos se dedica a la gestión de las relaciones de la empresa con los grupos de interés sobre ella y las entidades externas. Los grupos de interés incluyen accionistas, organizaciones de los empleados, etc. Las entidades externas incluyen reguladores, comunidad local, sindicatos.
- *Gestión de Recursos Humanos.* Este conjunto de procesos provee la infraestructura de recursos humanos para la gente que la empresa usa con el propósito de cumplir sus objetivos.
- *Gestión de Recuperación de Desastres, Seguridad y Fraude.* Este conjunto de procesos se concentra en asegurar que la empresa pueda soportar sus operaciones, procesos, aplicaciones y comunicaciones de misión crítica, de cara a desastres, amenazas de seguridad e intentos de fraude.

1.3.4 MODELO DE GESTIÓN Y ADMINISTRACIÓN DE RED INTERNET O SNMP [42]

El Modelo de Gestión Internet también es conocido como el Modelo *SNMP (Simple Network Management Protocol)*. Es el modelo más usado y difundido a nivel global y su funcionamiento se basa precisamente en el protocolo *SNMP*.

SNMP es un conjunto de especificaciones para gestionar una red de datos. Trabaja a nivel de la capa de aplicación para la administración de los dispositivos de la red. Estas especificaciones contienen el formato de los datos, el manejo del protocolo, y todo lo relacionado al manejo de la información.

1.3.4.1 Arquitectura de Gestión del Modelo de Internet o SNMP

Los elementos básicos (Figura 1.31) de la arquitectura de gestión del modelo de Internet son:

- Estación de Gestión. (Gestor en el modelo OSI).
- Agente.
- MIB (Base de información de Gestión).
- Protocolo de Gestión de Red (*SNMP*).

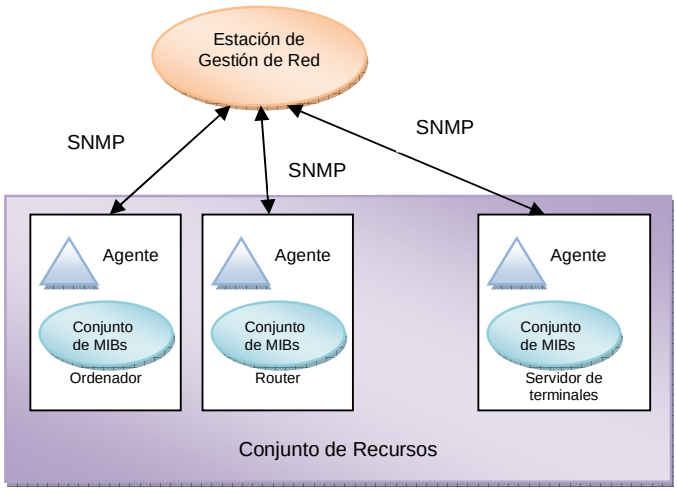


Figura 1.31 Arquitectura del Modelo de Gestión de Red Internet [34]

1.3.4.2 Arquitectura del Protocolo SNMPv1

SNMP (Protocolo Simple de Administración de Red) es parte de la variedad de protocolos que presenta la Arquitectura *TCP/IP*. *SNMP* basa su funcionamiento sobre UDP, es decir, un protocolo no orientado a conexión. Por esta razón, cada intercambio de información entre la estación de gestión y el agente, es una operación diferente.

SNMP consta de 5 mensajes relevantes como se puede ver en la figura 1.32:

- *GetRequest* y *GetNextRequest,* que se utilizan para leer la información de un elemento de la red.
- *SetRequest,* que se utiliza para establecer los cambios pedidos.
- *GetResponse,* que sirve para confirmar o responder a los mensajes anteriormente descritos.

- *Traps,* que se utiliza cuando se genera un evento en los elementos gestionados. Estas traps no necesitan confirmación.

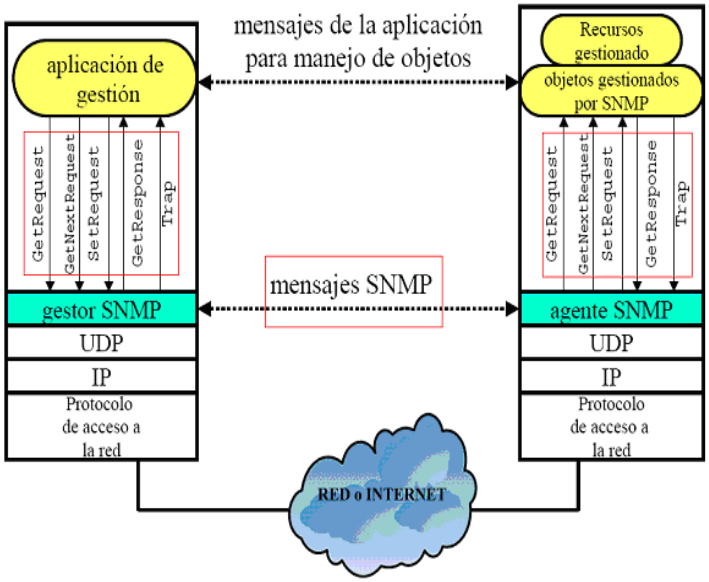


Figura 1.32 Principales mensajes con los que trabaja el protocolo SNMP [32]

La figura 1.32 además muestra como se relaciona la aplicación de gestión con el agente.

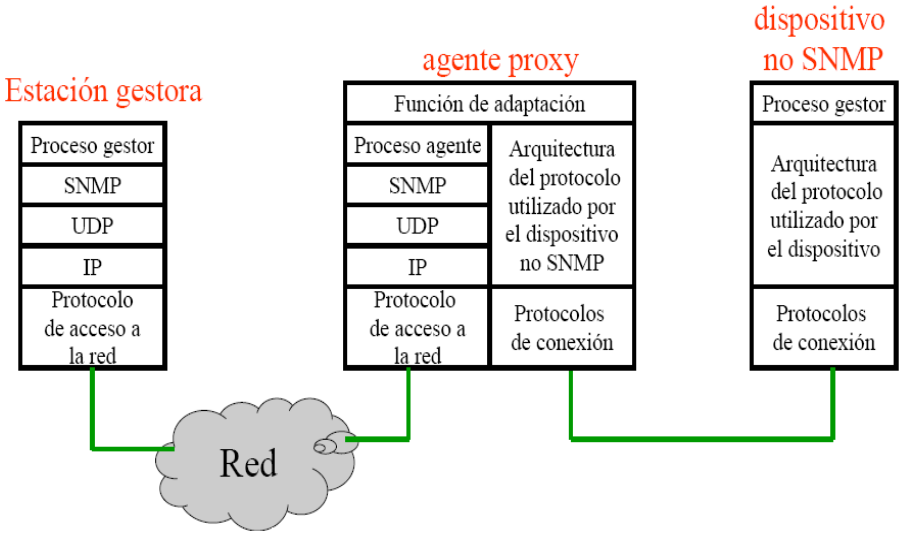


Figura 1.33 Agente Proxy [44]

Para que una red pueda ser gestionada con este modelo, todos los elementos deben soportar el protocolo SNMP y en caso que no lo hicieran, se debe utilizar un agente Proxy (Figura 1.33), el cual se encarga de receptar las peticiones de la estación y transformarlas a un lenguaje o protocolo entendible para el agente que no soporte SNMP y viceversa.

1.3.4.3 Información de Gestión SNMP [45]

La información de los elementos gestionados, se almacenan en la *MIB (Managemente Information Base)*. Cada objeto gestionado es visto desde un modelo orientado a objetos, por esta razón, la *MIB* es una colección estructurada de estos objetos. Una estación de gestión con su aplicación, puede administrar y controlar la red modificando los valores de estas *MIB*.

Una *MIB* presenta 2 objetivos primordiales:

- Los objetos usados para representar un recurso particular deben ser los mismos en todos los sistemas.
- Se necesita garantizar la interoperabilidad.

1.3.4.4 Estructura de la Información de Gestión (SMI)

La Estructura de la Información de Gestión utilizada por el modelo Internet. Está definido en el RFC 1155, donde se especifica el marco general dentro del cual una *MIB* puede ser especificada y construida. *SMI (Structure of Management. Information)* identifica los tipos de datos dentro de la *MIB* y especifica cómo se representan y denominan los recursos dentro de la MIB. El objetivo principal de la *SMI* es tener una *MIB* simple y extensible, razón por la cual, solo se puede utilizar tipo de datos simples como escalares o arreglos bidimensionales de escalares.

1.3.4.4.1 Estructura de una MIB

SNMP sigue una estructura tipo árbol, donde sus ramificaciones son los objetos a ser gestionados cada uno con una función específica en la red. Los objetos se agrupan en estructuras lógicas relacionadas entre sí.

Dentro de una *MIB* tenemos asociados objetos y a este un *OID (Object IDentifier)* que es un identificador de objeto, que es único para cada uno. Estos OID forman la estructura tipo árbol uniéndose con los OID que se siguen ramificando, es decir, sub-identificadores de jerarquía.

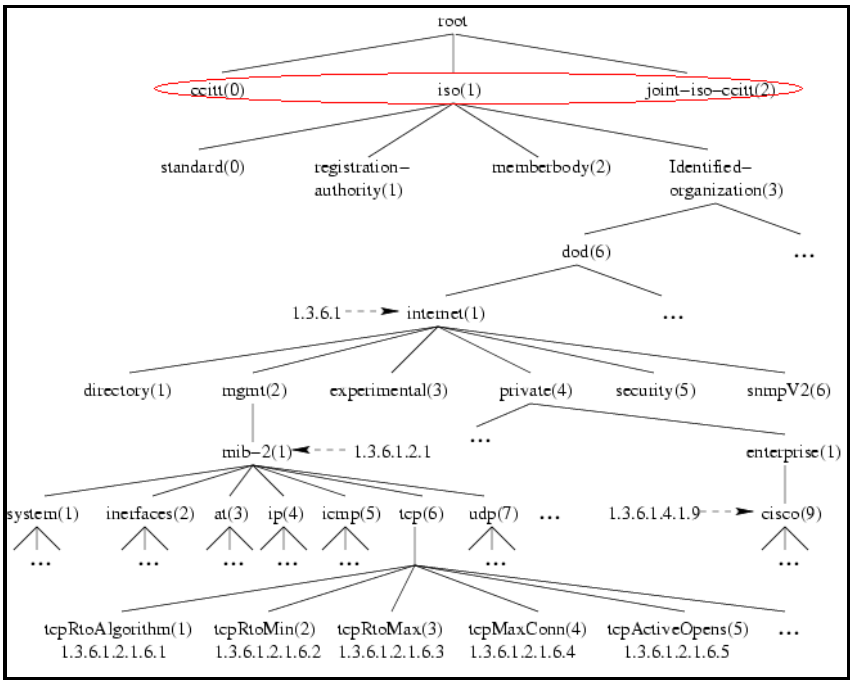


Figura 1.34 Estructura de un Árbol MIB con sus respectivos OID [43]

Para el primer nivel de la jerarquía como se puede ver en la figura 1.34, tenemos: iso-ccitt(2), ccitt(0) e iso(1), siendo de estos donde se ramifican las subdivisiones.

Debajo de Internet se tiene 6 estructuras definidas, las cuales se indican a continuación:

- *Directory*: Reservado para el uso con el *ISO – Directory*.
- *Management:* Usado para los objetos aprobados por el *IAB*[7].
- *Experimental:* Objetos referidos en los experimentos de Internet.

[7] IAB: Internet Activities Board: Junta de Actividades de Internet encargado de determinar las necesidades técnicas a medio y largo plazo, y de la toma de decisiones sobre la orientación tecnológica de la Internet, también aprueba las recomendaciones y estándares de Internet, recogidos en una serie de documentos *RFCs ("Request For Comments")* disponibles en la red.

- *Private*: Objetos definidos por los fabricantes.
- *Security*: Objetos definidos para la seguridad.
- *SNMP v2*: Objetos definidos para trabajar con SNMP v2.

1.3.4.4.2 Sintaxis de Objetos

Los objetos, se definen de una manera específica dentro de una MIB, definiendo el tipo de dato, el rango de valores, los estados permitidos y la relación con otros objetos. Así se distinguen dos tipos de datos: tipo universal como *integer, octetstring, null, object identifier, sequence, sequence-of*, etc, y los tipos de datos específicos para una aplicación, como: *ipaddress, counter, gauge, timesticks, opaque*, etc.

1.3.4.4.3 Definición de Objetos

Un objeto se define con el tipo de objeto y el valor. El tipo de objeto define una clase particular de objeto gestionado y la instancia de un objeto es una instancia particular que ha sido ligada a un valor.

```
IMPORTS ObjectName, ObjectSyntax      FROM RFC-1155-SMI

OBJECT-TYPE MACRO ::=
BEGIN
       TYPE NOTATION ::=     "SYNTAX"       type (TYPE ObjectSyntax)
                             "ACCESS"       Access
                             "STATUS"       Status
                             DescrPart
                             ReferPart
                             IndexPart
                             DefValPart
       VALUE NOTATION ::= value (VALUE ObjectName)

       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

       IndexPart ::= "INDEX" "{" IndexTypes "}"

       IndexTypes ::= IndexType|IndexTypes "."

       IndexType ::= value (indexobject ObjectName) --if indexobject, use the    SYNTAX
                                                    --value of the correspondent
                                                    --OBJECT-TYPE invocation
                            |type (indextype)       --otherwise use named SMI type:
                                                    --must conform to IndexSyntax below

       DefValPart ::= "DEFVAL" "{" value ObjectSyntax "}" |empty

       DisplayString ::= OCTECT STRING SIZE (0..255)

END

IndexSyntax ::= CHOICE {      number INTEGER (0..MAX),
                              string OBJECT STRING,
                              object OBJECT IDENTIFIER
                              address NetworkAddress
                              IpAddress IpAddress }
```

Figura 1.35 Macro para objetos gestionados en el Modelo Internet [42]

Las macros (Ver figura 1.35) son usadas para agrupar tipos de objetos relacionados entre sí. Entonces se tiene lo siguiente:

- *Macro*: Sintaxis de un conjunto de objetos relacionados entre sí.
- *Instancia de una macro*. Es una instancia de un tipo de objetos adicionando argumentos para definir su valor.
- *Valor de una instancia de una macro*. Es una entidad específica relacionada con un valor en particular.

1.3.4.4.4 Codificación

Los objetos de una MIB pueden ser codificados utilizando las reglas estandarizadas *BER (Basic Encoding Rules)*. Esto convierte a los objetos en cadenas de octetos estructuradas de la forma TLV (Tipo – Longitud – Valor).

En TLV hay tres maneras de codificar un valor:

- *Codificación primitiva de longitud definida*. Puede usarse para tipos de datos simples y derivados de tipos de datos simples con etiquetado implícito.
- *Codificación estructurada de longitud definida*. Utilizado para strings, tipos estructurados y derivados de estos mediante etiquetado implícito y cualquier tipo de dato con etiquetado explícito.
- *Codificación estructurada de longitud indefinida*. Igual que en el caso anterior pero en este no se necesita conocer la longitud del valor.

1.3.4.5 Seguridad en SNMP [42]

La seguridad en un sistema de gestión es importante al momento de establecer la comunicación. Por este motivo, se deben tener 3 aspectos en cuenta:

- *Autenticación*. La estación de gestión debe recibir notificaciones solo de las estaciones autorizadas.

- *Políticas de Acceso*. Las máquina de gestionadas deben considerar a que estaciones de gestión permitirles el acceso a la información y a cuanta información tienen acceso.
- *Servicio Proxy*. En un sistema amplio, una estación gestionada puede ser utilizada como Proxy para otras estaciones gestionadas, donde se necesitara un sistema de autenticación y políticas de acceso establecidas para el control del Proxy.

Para llevar a cabo estos tres pasos, se ha definido un sistema básico de seguridad para SNMP llamado comunidad.

1.3.4.5.1 Comunidad

Una comunidad es la relación existente entre un agente SNMP y una estación de gestión implementando características de autenticación, políticas de acceso y servicio Proxy. Cada comunidad tiene un nombre, la cual se debe incorporar en las peticiones *SET* o *GET*. Así varios agentes pueden presentar varias comunidades para comunicarse con varias estaciones de gestión, cada una con características propias de autenticación, políticas de acceso y Proxy.

Las políticas de acceso limitan el acceso a las MIB a un grupo de estaciones de gestión. Si se usan más de dos comunidades, se puede otorgar diversos niveles de acceso para distintas estaciones de gestión. Para esto se tienen dos modalidades:

- *SNMP MIB view*. Es un subconjunto dentro de una MIB. Se pueden tener varias vistas para cada comunidad.
- *SNMP Access mode*. Se define un modo de acceso que puede ser: *read – only* o *read – write*.

El *profile community* es la combinación de estos dos modos siendo que el modo de acceso se aplica a toda la *MIB view*. Dentro de un *profile community* deben conciliarse dos restricciones de acceso. Una cláusula de acceso correspondiente

a las MIB y la otra el *Access mode*. A continuación en la tabla 1.3 se detalla la manera de conciliación de las restricciones de acceso y las *MIB view*.

Cláusula ACCESO	Modos de Acceso SNMP	
	Read – Only	Read – Write
Read – only	Disponible para las operaciones get y trap	
Read – write	Disponible para las operaciones get y trap	Disponible para las operaciones get, set y trap
Write – only	Disponible para las operaciones get y trap pero el valor es específico de la implementación.	Disponible para las operaciones get, set y trap pero el valor es específico de la implementación para las operaciones get y trap
Not accesible	No disponible	

Tabla 1.3 Cláusulas de acceso y modos de acceso SNMP [42]

1.3.4.6 Orden Lexicográfico

Como las OIDs son secuencias de números enteros que siguen un ordenamiento lexicográfico. El ordenamiento padre e hijo del árbol de la MIB, es de una manera numérica secuencial. Garantizando así el acceso a pesar de no conocer la apariencia exacta de la MIB view ni de los nombres de los mismos.

El orden lexicográfico no es igual al orden numérico, aquí se presenta un ejemplo: Si $a = [19]$ y $b = [138]$ tenemos que $b < a$, porque el prefijo es $a_1 = b_1 = 1$ y $b_2 = 3 < a_2 = 9$. [57]

ipRouteDest	ipRouteMetricl	ipRouteNextHop
9.1.2.3	3	99.0.0.3
10.0.0.51	5	89.1.1.42
10.0.0.99	5	89.1.1.42

Figura 1.36 MIB view de la tabla ipRouteTable.

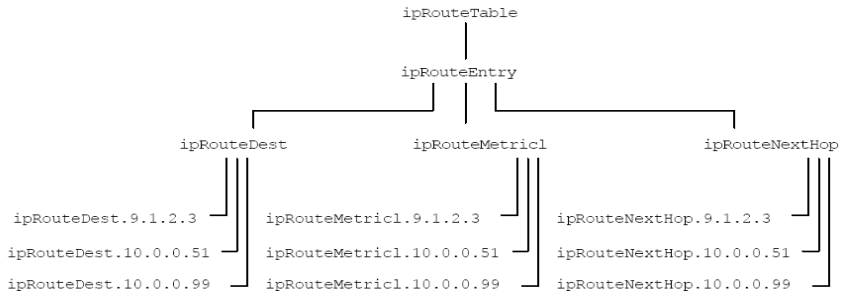


Figura 1.37 Subárbol de objetos e instancias correspondientes a la figura 1.36

1.3.4.7 Especificación del Protocolo

La comunicación se establece entre la máquina de gestión y la máquina gestionada, la información se envía mediante mensajes SNMP. Estos mensajes tienen 3 campos:

- *Versión*. Es el número de versión del protocolo. Por ejemplo, el valor es 0 para SNMPv1.
- *Comunidad*. Nombre de la comunidad.
- *PDU*. Especifica uno de los 5 tipos de PDU.

A continuación en la figura 1.38 se muestra los formatos de las PDUs para los mensajes que maneja *SNMP*:

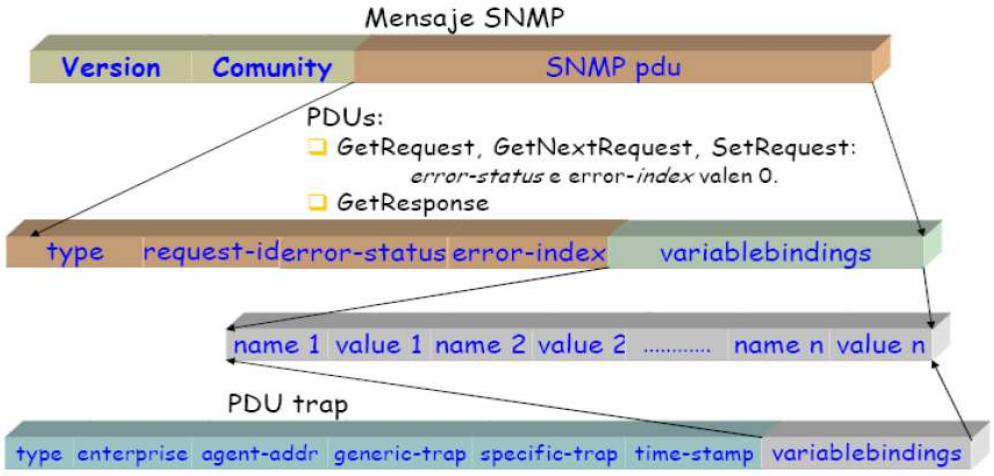


Figura 1.38 Formato de PDU SNMP [32]

1.3.4.8 Transmisión y Recepción de un Mensaje SNMP

En principio, para la transmisión de un mensaje *SNMP* se realiza lo siguiente:

- Construye la *PDU* usando la estructura *ASN.1.*
- Se envía la *PDU* a un servicio de autenticación junto con las direcciones de transporte fuente y destino y la comunidad. Este servicio se encarga de agregarle encriptación o algún código de autenticación.
- Luego, se construye el mensaje, incluyendo los campos versión y comunidad a los datos devueltos del paso anterior.
- Finalmente, se codifica el nuevo objeto *ASN.1* utilizando *BER* y se lo envía.

Para la recepción de un mensaje, se realiza lo siguiente:

- Primero se realiza una verificación de la sintaxis del mensaje, si falla, se descarta el mensaje.
- Luego, se verifica el número de versión e igualmente que en el caso anterior, si falla se descarta.
- Después, pasa a un servicio de autenticación en el cual, si falla, se le da un aviso a una entidad SNMP la cual genera un *trap* y descarta el mensaje, y, caso contrario, si la autenticación es exitosa, devuelve una *PDU* con formato *ASN.1.*
- Finalmente, se hace un chequeo de la sintaxis del *PDU*, si esta falla, se descarta el mensaje pero, si pasa la prueba, se selecciona una política de acceso dependiendo del nombre de comunidad asignado.

1.3.4.9 Tipos de PDU [46]

La *PDU SNMP* depende del tipo de operación a realizar. Esta puede ser:

- Si se trata de *GetRequest, GetNextRequest* o *SetRequest* se tiene:

PDU type	Request Id	0	0	Variable Bindings

Figura 1.39 *PDU* de *GetRequest, GetNextRequest* o *SetRequest* [46]

- *PDU type*. Indica el tipo de *PDU*.
- *Request Id*. Se utiliza para diferenciar las distintas peticiones, añadiendo a cada una de ellas un único identificador.
- *Variable Bindings*. Es una lista de nombres de variables y sus correspondientes valores. En algunos casos (*GetRequest*), el valor de las mismas es NULL. En el caso de las *Traps*, proporcionan información adicional relativa a la *Trap*, dependiendo el significado de este campo de cada implementación en particular.

- Si se trata de GetResponse se tiene:

PDU type	Request Id	Error-status	Error-index	Variable Bindings

Figura 1.40 PDU de GetResponse [46]

- *Error-status*. Se utiliza para indicar que ha ocurrido una excepción durante el procesamiento de una petición. Sus valores posibles son: *noError(0), tooBig(1), noSuchName(2), badValue(3), readOnly(4), genErr(5).*
- *Error-index*. Cuando el campo *Error-status* es distinto de 0, puede proporcionar información adicional indicando la variable que causó la excepción.

- Si se trata de un Trap se tiene:

PDU type	Enterprise	agent-addr	generic-trap	specific-trap	timestamp	Variable Bindings

Figura 1.41 PDU de Trap [46]

- *Enterprise*. Identifica el subsistema de gestión de red que ha emitido el Trap.
- *Agent-addr*. Dirección IP del agente que generó el Trap.
- *Generic-trap*. Tipo de Trap genérico predefinido. Puede ser:

- *coldStart(0)*. El agente se ha reinicializado, de forma que se puede alterar la configuración de los agentes o la implementación del protocolo. Típicamente reinicio por caída del sistema.
- *warmStart(1)*. La entidad emisora SNMP se ha reinicializado sin haberse alterado la configuración de los Agentes ni la implementación del protocolo. Usualmente es una rutina de tipo restart.
- *linkDown(2)*. Señaliza un fallo en alguno de los enlaces de comunicación del Agente. El primer elemento en el campo Variable-Bindings indicará el interfaz en cuestión.
- *linkUp(3)*. Señaliza el restablecimiento de uno de los enlaces de comunicación del Agente. El primer elemento en el campo Variable-Bindings indicará el interfaz en cuestión.
- *authentificationFailure(4)*. Indica que la entidad emisora del Trap ha recibido un mensaje en el que ha fallado la autentificación.
- *egpNeighborLoss(5)*. Indica que un EGP (External Gateway Protocol) vecino, para el cual la entidad emisora tenía asociado otro EGP, ha sido desmarcado y la relación entre ambos EGPs ha finalizado.
- *enterpriseSpecific(6)*. Significa que la entidad emisora reconoce que algún evento específico del fabricante ha ocurrido. El campo specific-trap indica el tipo de Trap.

- *Specific-trap*. Código de Trap específico e indica de una forma más específica la naturaleza del Trap.
- *Timestamp*. Tiempo transcurrido entre la última reinicialización de la entidad de red y la generación del trap.

1.3.4.10 MIB – II [47]

La MIB – II es la segunda versión de la MIB – I. La MIB – II define 10 grupos cada una con funciones específicas:

- *System(1)*. Provee una información general del sistema gestionado.
- *Interface(2)*. Contiene la información de las interfases físicas del sistema, incluyendo información de configuración y estadísticas sobre los eventos que ocurren en cada interfase.
- *at (adress translation)(3)*. Este grupo contiene la información para le mapeo de direcciones de red a direcciones físicas. Es importante cuando se tiene nodos con múltiples protocolos, en donde una dirección física tendrá asociada más de una dirección de subred, y, cuando se necesita mapear la dirección en ambos sentidos.
- *ip (internet protocol)(4)*. Este grupo contiene la información más importante sobre la implementación y operación del protocolo *IP* en un nodo.
- *icmp (Internet Control Message Protocol)(5)*. Provee información sobre los problemas suscitados en el entorno de comunicaciones.
- *tcp (Transmission-Control-Protocol)(6)*. Contiene la información más importante sobre la implementación y operación del protocolo *TCP* en un nodo.
- *udp (User Datagram Protocol)(7)*. Contiene la información relevante sobre la operación e implementación del protocolo *UDP* en un nodo.
- *egp (External Gateway protocol)(8)*. Contiene la información de operación e implementación del protocolo EGP.
- *dot3(10)*. Contiene objetos que provean detalles sobre el medio de transmisión subyacente para cada interfase del sistema.
- *snmp(11)*. Contiene la información para la implementación y operación del protocolo SNMP en un nodo.

1.3.4.11 Protocolo SNMPv2 [48]

Dado el vertiginoso aumento de las capacidades y dificultades de administración de redes, se desarrolló la versión 2 del protocolo SNMP. Como puntos nuevos de esta versión se puede mencionar las siguientes:

- Nueva estructura de la SMI.
- Capacidad de gestión entre dos estaciones de gestión (agente-agente).

- Nuevas operaciones.
- Desarrollo de una MIB SNMP V2.

1.3.4.11.1 Operación del Protocolo

Al igual que SNMPv1 la información se transmite a través de mensajes, donde la PDU transporta la acción a tomar por el agente o por la estación de gestión.

Todo lo mencionado para SNMPv1 como comunidad, perfiles de comunidad y políticas de acceso son válidas para SNMPv2, y cuando se utiliza el formato de mensaje SNMPv1 para transportar PDUs de SNMPv2 se conoce como community – based (SNMPv2C).

1.3.4.11.2 Transmisión y Recepción de un mensaje en SNMPv2

Es similar a SNMPv1, solo que se agregan más restricciones como se observa a continuación:

Cláusula MAX – ACCESS	Modos de Acceso SNMPv2	
	Read – Only	Read – Write
Read – only	Disponible para las operaciones get y trap	
Read – write	Disponible para las operaciones get y trap	Disponible para las operaciones get, set y trap
Read – create	Disponible para las operaciones get y trap	Disponible para las operaciones get, set y trap
Accesible – for – notification	Disponible para operaciones TRAP	
Not accesible	No disponible	

Tabla 1.4 Relación entre MAX - ACCESS y el Modo de Acceso [42]

1.3.4.11.3 Formato de mensaje SNMPv2 y PDUs

El formato de mensaje y PDUs es muy similar a SNMPv1 (Ver figura 1.42). Aquí se incorpora un nuevo PDU llamado GetBulkRequest, InformRequest y Response (Ver figura 1.43).

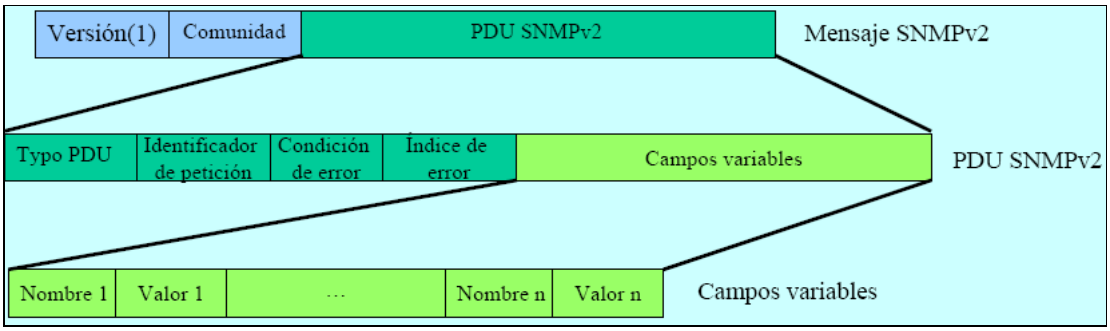


Figura 1.42 Formato de mensajes de SNMPv2 [49]

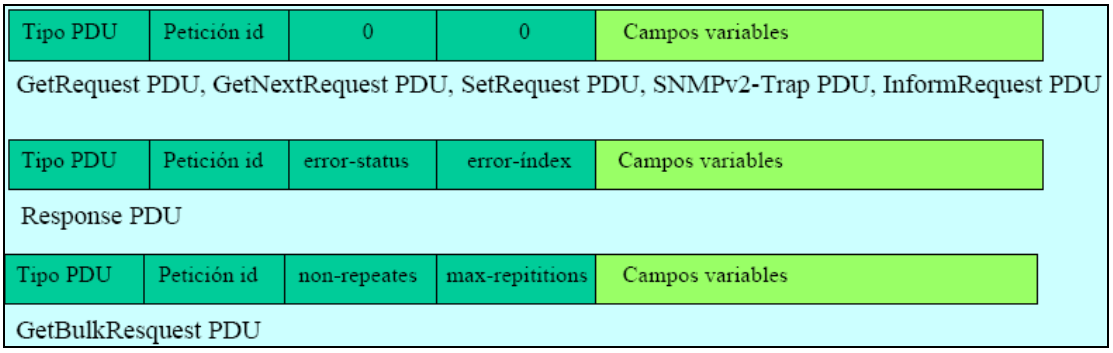


Figura 1.43 Formato de PDU de los mensajes de SNMPv2 [49]

- *GetRequest*. Su formato de la *PDU* es idéntico a *SNMPv1*, la diferencia radica en su respuesta. En *SNMPv2* la ejecución no es atómica, es decir, que se devuelven valores de las operaciones ejecutadas, y de las que no, igual se devuelve un valor pero indicando que no se pudo ejecutar.

- *GetNextRequest*. Al igual que en el caso anterior, es idéntica al formato de *SNMPv1*, pero puede devolver resultados parciales. Al igual que en la

versión 1, se rige al elemento siguiente en orden lexicográfico, si es el último y no existe un siguiente, el valor se establece en *endOfMibView*.

- *GetBulkRequest*. El propósito de esta nueva *PDU* es el minimizar el intercambio de información cuando la solicitud es de gran tamaño. Esta *PDU* puede recuperar gran cantidad de información, su único limitante sería el tamaño del mensaje.

- *SetRequest*. Al igual que en los casos anteriores, la diferencia está en el manejo de las respuestas. Primero el agente determina el tamaño del mensaje que encapsula una *PDU* con la misma lista de variables vinculadas con sus nombres y valores. Si esta tamaño excede al permitido se genera una *PDU* con un error – *status de tooBig*, caso contrario, se construye una *PDU* de respuesta donde todos los campos tienen el mismo valor que los campos correspondientes del pedido recibido.

- *SNMPv2 – Trap*. Tiene la misma función que las *Trap* de *SNMPv1* pero con formato diferente. Esto facilita el procesamiento en el receptor.

- *InformRequest*. Esta *PDU* se envía a nivel de estaciones de gestión y se utiliza para proporcionar información de gestión a la aplicación de la entidad receptora del mensaje.

- *Report*. No se tiene definido ni su utilización ni cuándo se debe utilizar. Solo se tiene una referencia sobre esta PDU en el documento de desarrollo.

1.3.4.11.4 Agente Proxy

El agente Proxy permite intercambiar información entre el gestor *SNMPv2* y el agente *SNMPv1*. Para poder conversar entre protocolos, se necesita hacer un mapeo de las *PDU* de las dos versiones. A continuación, en la figura 1.44 se muestra como se hace el mapeo.

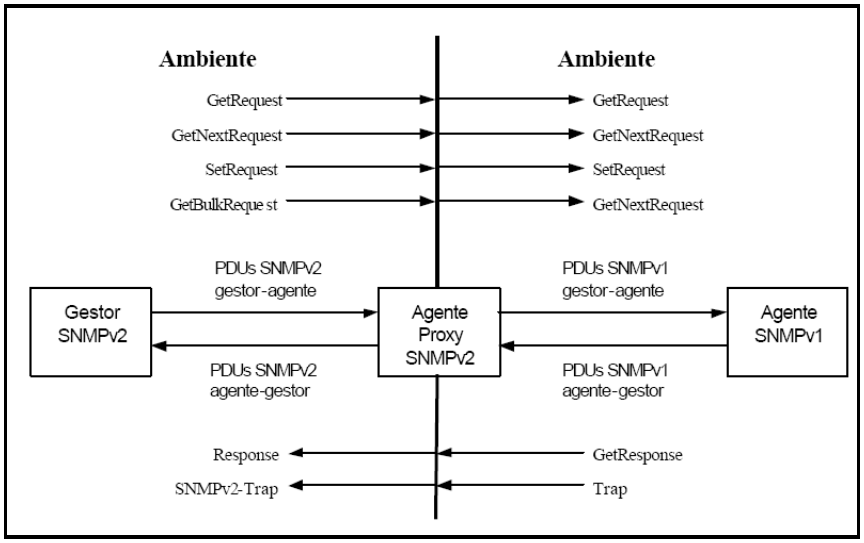


Figura 1.44 Mapeo de PDU en un Agente Proxy

1.3.4.11.5 Gestor Bilingüe

El gestor bilingüe es una máquina de gestión que entiende las dos versiones de SNMP. Toda comunicación se realiza con SNMPv2, cuando sea necesario, el gestor convertirá a versión 1. A continuación, se detalla cómo funciona el gestor bilingüe. (Ver figura 1.45)

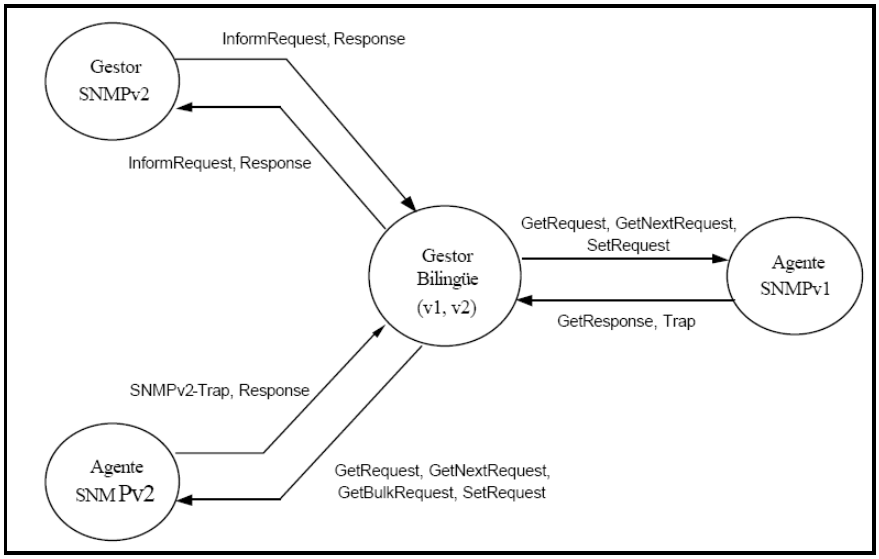


Figura 1.45 Gestor Bilingüe

1.3.4.11.6 MIB SNMPv2

En la versión 2 se agregan nuevos objetos para describir entidades SNMPv2. Así, se modifica esencialmente 3 grupos:

- *System*. Se agrega nuevos objetos al grupo system original para poder describir objetos que pueden ser configurados remotamente.
- *SNMP*. Provee objetos básicos para monitorear y controlar elementos del protocolo.
- *Objetos MIB*. Es una colección de objetos que gestionan la *PDU SNMPv2 – Trap* y que permite cooperar con entidades *SNMPv2*, todas operando en el rol de gestor.

1.3.4.12 Protocolo SNMP v3 [51]

SNMPv3 es la última versión de SNMP, que fue presentada en una serie de recomendaciones en 1998, como se puede ver en la figura 1.46.

Número de RFC	Titulo
2271	An Architecture for Describing SNMP Mangement Framework
2272	Message Processing and Dispatching for Simple Network Management Protocol (SNMP)
2273	SNMPv3 Applications
2274	User-Based Security Model for SNMPv3
2275	View-Based Access Control Model (VACM) for SNMP

Figura 1.46 RFCs donde se describe a SNMPv3 [51]

Cabe resaltar, que SNMPv3 no se trata de un estándar que reemplaza a SNMPv1 y/o SNMPv2, sino es un protocolo que define una serie de capacidades adicionales de seguridad y administración a ser utilizadas en conjunto con SNMPv2 (preferiblemente) o SNMPv1 (Ver figura 1.47)

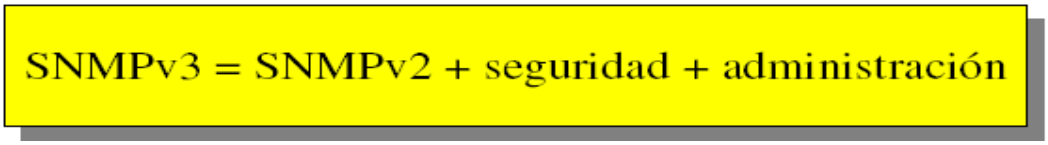


Figura 1.47 Formación de SNMPv3

Este protocolo de gestión, brinda seguridad de acceso a los dispositivos por medio de una combinación de autenticación y encriptación de paquetes que trafican por la red. Las capacidades de seguridad que SNMPv3 proporcionan son:

- *Integridad del Mensaje*: Porque asegura que el paquete no haya sido violado durante la transmisión.
- *Autenticación*: Porque determina que el mensaje proviene de una fuente válida.
- *Encripción*: Porque encripta el contenido de un paquete como forma de prevención.

SNMPv3 proporciona tanto modelos como niveles de seguridad.

- *Un modelo de seguridad:* Es una estrategia de autenticación que es configurada para los usuarios y los grupos en los cuales estos residen.
- *Los niveles de seguridad:* Se refieren al nivel permitido a un usuario dentro de un modelo de seguridad. La combinación de ambas cosas determinará que mecanismo de seguridad será el empleado cuando se maneje un paquete *SNMP*.

1.3.4.12.1 Arquitectura Utilizada

SNMPv3 presenta una arquitectura modular para ofrecer los servicios de seguridad, que son:

- Autenticación.
- Privacidad.
- Control de Acceso.

Para dar estos servicios *SNMPv3* utiliza una entidad en la cual la mayor parte de los servicios son proporcionados ó procesados. Esta entidad puede actuar en forma individual en un rol particular, como aplicación o conjunto de aplicaciones. Esta entidad opera desde una estación gestora y envía comandos *SNMP* hacía los agentes. El trabajo en conjunto de la entidad y del agente determinan las capacidades de seguridad que serán invocadas, incluyendo autenticación, privacidad y control de acceso.

SNMPv3 se puede definir de una forma modular (Ver figura 1.48). Cada Entidad *SNMP* incluye un simple *SNMP Engine*. Un *SNMP Engine* implementa funciones para enviar / recibir, autenticar y encriptar / desencriptar mensajes, además de controlar el acceso a los objetos manejados. Estas funciones son proporcionadas como servicios para una ó más aplicaciones que son configuradas con el *SNMP Engine* para así formar la *SNMP Entity (Entidad SNMP)*.

a. Elementos de una Entidad SNMP

a.1 SNMP Engine

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

a.2 Aplicaciones

- *Generador de Comandos*: Recibe los *PDUs SNMP Get, GetNext, GetBulk* ó *SetRequest* y procesa la respuesta a una requisición que ha sido generada.

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

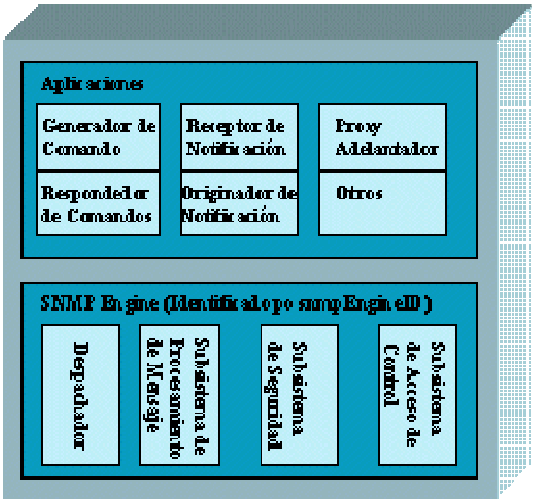


Figura 1.48 Entidad SNMPv3 [51]

b. Modelo de Procesamiento del Mensaje [53]

Este modelo es responsable de aceptar los *PDUs* del Despachador, encapsularlo entonces en mensajes, e invocar el *USM (Modelo de Seguridad del Usuario)* para insertar los parámetros relacionados con la seguridad en el encabezado del

mensaje. El modelo de procesamiento del mensaje también se encarga de aceptar mensajes entrantes, invocar el *USM* para procesar los parámetros de seguridad que se encuentran en el encabezado del mensaje y entrega el *PDU* al despachador. [54]

1.3.4.12.2 Estructura de un mensaje SNMPv3

Como se puede ver en la figura 1.49, los primeros cinco campos son generados por el modelo de procesamientos de mensajes entrantes o salientes. Los siguientes seis campos muestran los parámetros de seguridad usados por el *USM*. Finalmente el *PDU*, junto con el *ContextEngineID* y *ContextName* constituyen el *PDU* a ser procesado.

Los primeros cinco campos son los siguientes:

- *msgVersion*: Configurado para SNMPv3.
- *MsgID*: Un identificador único usado entre dos entidades SNMP para coordinar los mensajes de requisición y respuesta. Su rango es de 0 a 2^{31} – 1.
- *MsgMaxSize*: Se refiere al tamaño máximo de un mensaje en octetos soportado por el que envía, con un rango de 484 a 2^{31} – 1. Este es el máximo tamaño que una entidad que envía puede aceptar de otra SNMP Engine.
- *MsgFlag*: Un arreglo de octetos que contiene tres banderas en los tres bits menos significativos:

  - *ReportableFlag*: Utilizada igual a 1 para los mensajes enviados conteniendo una requisición o un Inform, e igual a 0 para mensajes conteniendo una Respuesta, Trap ó Reporte PDU.
  - *PriorFlag y AuthFlag*: Son configuradas por el que envía para indicar el nivel de seguridad que le fue aplicado al mensaje.

- *MsgSecurityModel*: Es un identificador en el rango de 2^{31} – 1 que indica que modelo de seguridad fue utilizado por el que envió el mensaje, para que así el receptor tenga conocimiento de que modelo de seguridad deberá usar para procesar el mensaje. Existen valores reservados:

- 1 para SNMPv1.
- 2 para SNMPv2.
- 3 para SNMPv3.

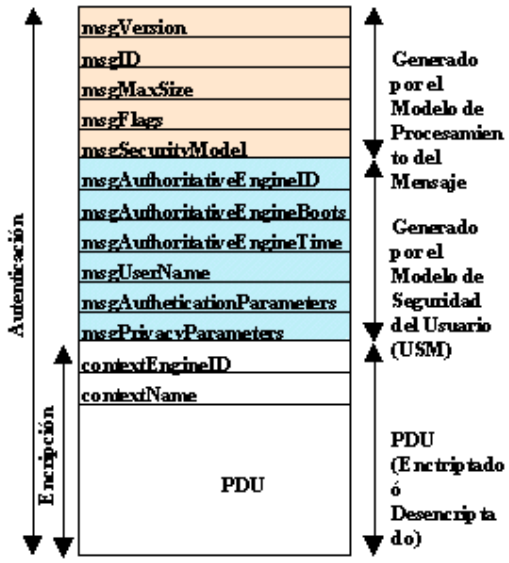


Figura 1.49 Formato del mensaje SNMPv3 [51]

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

- *MsgAuthoritativeEngineID*: Se refiere al valor de la fuente de un Trap, Response ó Report y al destino de un Get, GetNext, GetBulk, Set ó Inform.
- *MsgAuthoritativeEngineBoots*: Es un entero que representa el número de veces que el SNMP Engine se ha iniciado o reiniciado desde su configuración inicial.
- *MsgAuthoritativeEngineTime*: Es un valor entero en el rango de $2^{31} – 1$ que representa el número de segundos desde que el snmpEngineBoots del SNMP Engine fue incrementado.
- *MsgUserName*: Usuario principal desde el cual el mensaje ha sido enviado.

- *MsgAuthenticationParameters*: Parámetro de autenticación. Si la autenticación no es utilizada, este valor es nulo. Este parámetro es generado usando un algoritmo llamado HMAC.
- *MsgPrivacyParameters*: Parámetro de privacidad. Si la privacidad no es utilizada, este valor es nulo. Este parámetro es generado usando un algoritmo llamado DES.

1.3.4.13 Monitoreo Remoto (RMON) [55]

RMON es una MIB extendida a MIB – II, que permite monitorear no sólo los dispositivos conectados en una red, sino la red en sí. RMON.

RMON nos presenta las siguientes características:

- *Operación offline*. Esta característica permite que, aunque exista una falla entre el gestor y el monitor de la red, este siga generando información de tráfico, rendimiento, etc. Y cuando la conexión se restaure, el monitor envía la información requerida por el gestor, además, el monitor recopila información sin necesidad del polling del gestor, con lo cual se ahorra una gran cantidad de ancho de banda.
- *Detección y reporte de fallas*. RMON facilita herramientas para analizar la información recolectada y enviar alarmas si algún parámetro está funcionando de mala manera y así preveer o detectar inconvenientes antes de que estos sucedan.
- *Datos con valor agregado*. El monitor analiza la información de la subred a la que pertenece, indicando parámetros tales como quien utiliza mayor cantidad de recursos o en su defecto, quien está provocando fallas en la red.
- *Múltiples Gestores de Red*. Para redes extensas y grandes, se pueden utilizar varios gestores los cuales coordinan trabajos para gestionar la red.

1.3.4.13.1 MIB RMON [42]

RMON se integra al grupo de las MIB-II con el ID 16. Define 9 grupos para gestionar una red, los cuales son:

- *Statistics*. Almacena la información recopilada de las subredes gestionadas.
- *History*. Contiene almacenada información de eventos pasados y se utiliza para evaluar la evolución de algunos parámetros de la red.
- *Alarms*. Monitorea el rendimiento de la red, definiendo umbrales, lo cuales si son cruzados, se genera un evento asociado a la alarma.
- *Host*. Se encarga de monitorear a todos los equipos detectados y almacena su información.
- *hostTopN*. Muestra los primeros N host ordenados en función de un parámetro, además de indicar el intervalo de tiempo en el cual se recolectara los datos a ser tomados en cuenta.
- *matrix*. Recolecta información del tráfico entre dos hosts dentro una misma subred y los almacena en forma de matriz.
- *filter*. Permite discriminar datos de interfaces, permitiendo recolectar información de paquetes seleccionados o de una interfaz en particular.
- *capture*. Permite la captura de paquetes siguiendo un parámetro de filtrado.
- *event*. Su implementación es opcional, y define los eventos a ejecutarse luego de generada una alarma del grupo *alarm.*
- *token ring*. Su implementación es opcional y permite obtener información estadística en una interfaz *token ring*.

1.3.4.13.2 RMON v2 [56]

Es una extensión de la *MIB* de *RMON*. *RMON v2* está diseñado para que pueda monitoriar tráfico por encima del nivel *MAC*, es decir puede monitoriar paquetes desde la capa 3 hasta la capa 7 del modelo de red *OSI*.

RMON puede monitoriar tráfico a nivel de aplicación tales como el www, ftp, mails, etc. Además de esta manera se supera la barrera del tráfico con direcciones MAC, es decir con RMON-2 se puede monitoriar el tráfico a base de direcciones

de nivel de red y de esta manera se puede verificar tráfico de distintos segmentos de una *LAN*.

a. Grupos añadidos a RMON v2

- *ProtocolDir*. Definen todos los protocolos que puede interpretar este agente.
- *ProtocolDist*. Ofrece estadísticas del tráfico por cada protocolo y segmento de LAN.
- *AddressMap*. Define pares de direcciones de cada interface de red (MAC's y IP's).
- *nlHost*. Brinda las estadísticas del tráfico de y para un host (en base a direcciones de red).
- *alHost*. Brinda las estadísticas del tráfico de y para un host (en base a direcciones de aplicación).
- *nlMatrix*. Brinda las estadísticas del tráfico entre pares de hosts (en base a direcciones de red).
- *alMatrix*. Brinda las estadísticas entre pares de hosts (en base a direcciones de aplicación).
- *usrHistory*. Permite el muestreo periódico de variables y registro de estados.
- *ProbeConfig*. Define parámetros estándar para RMON.

Entre las nuevas características de RMON2 están:

- Facilita la obtención de la tabla de datos sin necesidad de conocer la instancia de la tabla de control que la relaciona.
- Mejora el uso de las tablas en la MIB.
- Añade la capacidad de pre-filtrado de información .indexado por filtro temporal.

1.4 COMPARACIÓN ENTRE LOS MODELOS DE GESTIÓN

Aquí se presenta una breve comparación entre los diferentes modelos de gestión y administración de red estudiados en el presente capítulo:

Comparación entre Modelos de Gestión y Administración de Redes				
Nombre del Modelo	**Auspiciante del Modelo**	**Tipo de red que gestiona**	**Funciones principales**	**Estado del Modelo**
FCAPS	ISO	Todas.	Fallos, Configuración, Contabilidad, Rendimiento y Seguridad.	Marco referencial muy popular para la gestión de redes.
TMN (Telecommunications Management Network)	ITU-T	Redes de Telecomunicaciones.	Gestión de negocio, gestión de servicio, gestión de red y gestión de elemento.	Marco referencial para muchos sistemas de gestión de redes proveedoras de servicios.
TOM (Telecoms Operations Map)/ **e-TOM** (enhanced Telecom Operations Map)	TeleManagement Forum	Redes de Proveedores de Servicios.	Gestión de sistemas y redes, operaciones y desarrollo de servicios, atención de usuarios.	Todavía se encuentra en una etapa conceptual.
ISO/OSI (CMIP)	OSI	Redes basadas en la arquitectura OSI.	Monitoreo, gestión de rendimiento, Fallos y Configuración.	Su desempeño está limitado a redes con base en la arquitectura OSI.
Internet **(SNMP)**	IETF	Redes de datos	Monitoreo, gestión de rendimiento y fallos.	Ampliamente desarrollado y aplicado en redes de datos, especialmente en redes basadas en la arquitectura *TCP/IP*.

Tabla 1.5 Comparación de los Modelos de Gestión y Administración de Red

Ventajas y Desventajas de los Modelos		
Nombre del Modelo	**Ventajas**	**Desventajas**
TMN (Telecommunications Management Network)	Proporciona una arquitectura de capas para todas las funciones y aspectos dentro de la gestión de una empresa.	Su complejidad debido a que trabaja con sistemas distribuidos antiguos, y solo soporta el protocolo de comunicación CMIP.
TOM (Telecoms Operations Map)/ **e-TOM** (enhanced Telecom Operations Map)	El modelo abarca todos los procesos dentro de una empresa proveedora de servicios	Todavía no se encuentra ampliamente difundido y está desarrollado solo para empresas grandes proveedoras de servicios.
ISO/OSI (CMIP)	El modelo es un marco referencial completo para redes basadas en la arquitectura de redes OSI.	Su protocolo de comunicación CMIP es complejo, y no es soportado ampliamente por equipos de interconexión de redes, además de que requiere muchos recursos de la red.
Internet **(SNMP)**	Su protocolo de comunicaciones SNMP está ampliamente difundido y lo soportan la mayoría de elementos que forman la red. Además de su sencillez, lo cual reduce costes y tiempo en desarrollo de aplicaciones para la gestión.	Su debilidad tiene que ver con las seguridades, pero esto se ha tratado de superar con la versión 3 del protocolo SNMP.

Tabla 1.6 Ventajas y desventajas de los Modelos de Gestión y Administración de Red

BIBLIOGRAFÍA DEL CAPÍTULO I

[1] Alexander Clemm, PhD. Cisco Press. NETWORK MANAGEMENT FUNDAMENTALS. 2007.

[2] Allan Leinwand. Karen Fang Conroy. Addison Wesley Inc. Network Management: A Practical Perspective-Unix and Open System Series. 2da Edición.

[3] Salah Aidarous. Thomas Plevyak. IEEE Press. Telecommunications Network Management: Technologies and Implementations-IEEE.

[4] Divakara K. Udupa. *TMN*-McGraw-Hill Telecommunications.

[5] William Stallings. PEARSON Prentice Hall. Comunicaciones y Redes de Computadoras. 7ma Edición. 2004.

[6] James F.Kurose, Keith W. Ross. PEARSON Addison Wesley. Redes de Computadoras: Un Enfoque Descendente Basado en Internet. 2da Edición. 2004.

[7] http://80.34.206.133/netica/com/gestion-*TMN*-v1.pdf

[8] http://ocw.upm.es/teoria-de-la-senal-y-comunicaciones-1/sistemas-detelecomu
nicacion/Contenidos/Apuntes/2_interconexion_y_gestion_redes.pdf

[9] http://www.personal.us.es/jluque/Conferencias/1997%20SAINCO-1.pdf

[10] http://chemary.com/apuntes/gx.pdf

[11] http://www.eie.fceia.unr.edu.ar/ftp/Tecnologias%20de%20banda%20angosta/Notas_sobre_TMN.pdf

[12] http://www.mincomunicaciones.gov.co/minintranet/src/user_docs/conocimiento/desarrollosector/OTROS(GestionRedTelecomunicaciones2000)703.pdf

[13] http://www.personal.us.es/toni/_private/ManagementNetwork.pdf

[14] http://jci.uniautonoma.edu.co/_oldweb/docentes/gangulo/Aplicaciones/Gestion/Mod-ST724-Rmon.pdf

[15] http://www.geocities.com/alinamqn/*TMN*7.htm

[16] http://www.itba.edu.ar/capis/epg-tesis-y-tf/douglas-paredes-tfe.pdf

[17] http://www.cesat.com/area3.htm

[18] http://www.cesat.com/area3.sgrt.htm

[19] http://it.aut.uah.es/alarcos/docente/gr_itig/tema6.pdf

[20] http://jci.uniautonoma.edu.co/_oldweb/docentes/gangulo/Aplicaciones/Gestion/03-*TMN*.pdf

[21] http://www.inf-cr.uclm.es/www/jprozas/GdR/T3_ArquitecturasGestion.pdf

[22] http://www.gdsig.com.ar/xconferenciasig/P8.pdf SIGy *TMN*

[23] http://www.coit.es/publicac/publbit/bit125/sociedad.htm

[24] http://seguridad.internet2.ulsa.mx/congresos/2006/cudi1/wireless.pdf

[25] http://www.gatv.ssr.upm.es/stelradio/STEL/adjuntos/material_consulta/2_apuntes_interconexion_y_gestion_redes.pdf

[26] http://support.microsoft.com/kb/252648/es

[27] http://www.arcesio.net/osinm/asn1.html

[28] http://es.wikipedia.org/wiki/Organizaci%C3%B3n_Internacional_para_la_Estandarizaci%C3%B3n

[29] http://www4.ujaen.es/~mdmolina/grr/Tema%204.pdf

[30] http://www.arcesio.net/osinm/osinmorganizacion.html

[31] http://www.geocities.com/jcredesii/REDES2-36.htm

[32] http://tvdi.det.uvigo.es/~mramos/gprsi/gprsi3.pdf

[33] http://ericktellez.iespana.es/iso.pdf

[34] http://books.google.com.ec/books?id=11DSMYYKvL0C&pg=PA71&lpg=PA71&dq=CCR+(Commitment,+Concurrency+and+Recovery)&source=web&ots=z02Peq7NeA&sig=ZJTGsGtJhecb7VnliP8-Gd5ZJyk&hl=es&ei=A_-ZSd7wEpDamQfDv7yYCg&sa=X&oi=book_result&resnum=5&ct=result#PPA72,M1

[35] http://www.csae.map.es/csi/silice/Redges7.html

[36] Recomendaciones UIT-T/M.3200 y UIT-T/M.3400

[37] Recomendaciones UIT-T/M.3010 y UIT-T/M.3100

[38] http://www.networkdictionary.com/telecom/TOM.php

[39] http://es.wikipedia.org/wiki/ETOM

[40] http://espanol-itil.com/content/view/45/

[41] http://www.piramidedigital.com/Documentos/BSC/pdbscparte2modulogestion.pdf

[42] LESCHENNE, Sebastián; SALAZAR Martín. Modelo de Gestión de Internet SNMP - RMON. Universidad Nacional de Rosario. 2002.

[43] http://www.tcil-india.com/new/new_site/white%20paper/RK-7%20final_snmp.ppt

[44] http://zeus.unex.es/~victor/software/RAL/Monitorizacion/tema3.pdf

[45] http://www.chaco.gov.ar/UTN/AdmRedes/Traduccion/Cap8.doc

[46] http://www.tlmat.unican.es/siteadmin/submaterials/89.pdf

[47] RFC 1213

[48] RFC 1901 al RFC 1908

[49] http://www4.ujaen.es/~mdmolina/grr/Tema%203.pdf

[50] http://www.ramonmillan.com/tutorialeshtml/snmpv3.htm

[51] http://neutron.ing.ucv.ve/revista-e/No6/Valles%20Kirssy/SNMPV3/Snmpv3.htm

[52] RFC 2271

[53] RFC 2272

[54] RFC 2274

[55] RFC 1757 y RFC 2021

[56] http://alumno.ucol.mx/al986138/public_html/MARIO/adm_redes/Resumen%20Protocolos%20de%20Monitorizacion%20por%20Mz%20v1-0.pdf

[57] http://wapedia.mobi/es/Orden_lexicogr%C3%A1fico

CAPÍTULO II
ANÁLISIS DE LA SITUACIÓN Y REQUERIMIENTOS ACTUALES DE LA RED DE DATOS DE LA UTEQ

En este capítulo se analiza el estado actual de la red de datos de la UTEQ. Aquí se especifican los recursos físicos (Backbone de la red, routers, conmutadores, elementos de seguridad, etc.) que componen la red, así como, los recursos de tipo lógico (plataformas de trabajo, software de aplicación y monitoreo).

Luego, se desarrolla un diagnóstico sobre el estado de la red de datos de la UTEQ, para posteriormente detallar los requerimientos que esta necesita y deben ser cubiertos por el modelo de gestión de datos seleccionado en capítulos posteriores.

2.1. INTRODUCCIÓN

La UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO (UTEQ) se encuentra ubicada en Quevedo, ciudad central y capital económica de la Provincia de Los Ríos.

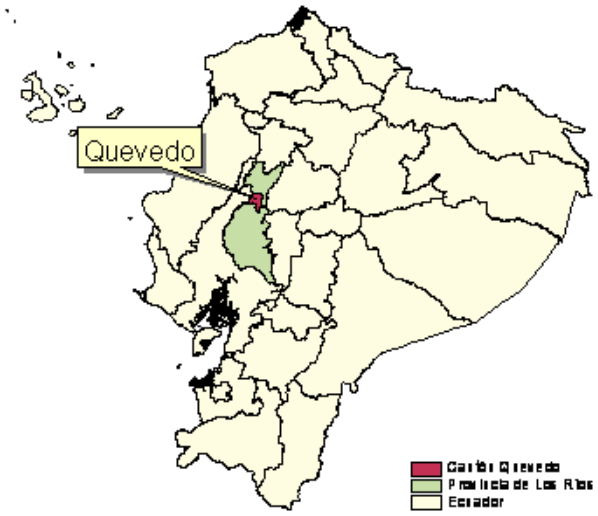


Figura 2.1 Macro localización de la UTEQ

Figura 2.2 Micro localización de los Predios de la UTEQ

Esta institución se inició el 22 de enero de 1976, como Extensión Universitaria con la carrera de Ingeniería Forestal e Ingeniería Zootécnica, dependiente de la Facultad de Ciencias Agropecuarias de La Universidad "Luís Vargas Torres" de Esmeraldas.

Fue creada como Universidad Técnica Estatal de Quevedo (UTEQ) mediante Ley de la República del 26 de enero de 1984, publicada en el Registro Oficial No. 674 del 1 de Febrero de 1984.

La Universidad Técnica Estatal de Quevedo (UTEQ) cuenta en total con cuatro campus de estudios, el campus principal ubicado en la Ciudad de Quevedo (Avenida Quito, Km 1 ½ Vía a Santo Domingo. QUEVEDO-LOS RÍOS-ECUADOR), y los otros tres campus, Finca “La María”, Finca “La Represa y Finca “La Buseta”, ubicadas a las afueras de la ciudad.

La institución tiene una infraestructura para brindar sus servicios a más de 3000 estudiantes presenciales, y unos 2000 más en modalidad a distancia.

La misión de la UTEQ es de "Formar integralmente profesionales en las distintas áreas del conocimiento, líderes, creativos y competitivos, de pensamiento crítico y con valores humanos, comprometidos en el desarrollo de una sociedad justa y solidaria, a través de la docencia, investigación, extensión y producción de bienes y servicios"

La visión de la UTEQ es "La UTEQ alcanzará la excelencia institucional, líder en el desarrollo sustentable, acreditada nacional e internacionalmente".

La Universidad tiene actualmente cuatro Facultades de Ciencias. Entre las que constan la Facultad de Ciencias Agrarias, que se compone de las Escuelas de Ingeniería Agronómica, Administración de Empresas Agropecuarias, Horticultura y Fruticultura y Economía agrícola. La Facultad de Ciencias Ambientales, con sus Escuelas de Ingeniería Forestal y Gestión Ambiental. También, está la Facultad de Ciencias Pecuarias con sus Escuelas de Zootecnia y Agropecuaria. Y por último la Facultad de Ciencias Empresariales con sus Escuelas: Escuela de Economía y Finanzas, Escuela de Ingeniería en Gestión Empresarial, Escuela de Ingeniería en Marketing, Escuela de Ingeniería en Sistemas, Escuela de Tecnología en Telemática, Escuela de la Carrera de CC. Jurídicas, Escuela de la Carrera de Psicología en Gestión Laboral y Desarrollo Organizacional.

La institución también cuenta con la Unidad de Estudios a Distancia (UED), el Centro de Idiomas Extranjeros (CEDI), la Unidad de Posgrado, un Instituto de Informática, una extensión universitaria en la ciudad de La Maná, provincia de Cotopaxi, y diversas oficinas de apoyo en varios cantones dentro y fuera de la Provincia de Los Ríos.

Esquema del Campus Principal de la Universidad Técnica Estatal de Quevedo se lo puede ver en la Figura 2.3.

Figura 2.3 Vista Aérea del Campus Central [1]

1. DIRECCION ADMINISTRATIVA
2. SALON AUDITORIUM
3. IMPRENTA
4. RECTORADO
5. HONORABLE CONSEJO UNIVERSITARIO - H.C.U.
6. SECRETARIA GENERAL
7. VICERRECTORADO
8. BODEGA
9. PROVEEDURIA
10. UNIDAD DE POSGRADO
11. ASOCIACION DE DOCENTES - ADUTEQ
12. FACULTAD DE CIENCIAS AGRARIAS
    ESCUELAS
    INGENIERIA AGRONOMICA
    INGENIERIA EN ADM. EMPRESAS AGROPECUARIAS
    INGENIERIA EN HORTICULTURA Y FRUTICULTURA
    ECONOMIA AGRICOLA
    BIBLIOTECA
    UNIDAD DE ESTUDIOS A DISTANCIA - UED
    DEPARTAMENTO DE PLANEAMIENTO ACADEMICO
    CENTRO DE NEGOCIOS
    PROCURADURIA
13. ASOCIACION DE EMPLEADOS Y TRABAJADORES - AET
14. COPIADORA
15. COMEDOR UNIVERSITARIO
16. CENTRO DE IDIOMAS - CEDI
17. DECANATO DE LA FACULTAD DE CIENCIAS AMBIENTALES
    SUBDECANATO DE LA FACULTAD DE CIENCIAS AMBIENTALES
18. SECRETARIA DE LA FACULTAD DE CIENCIAS AMBIENTALES
19. DIRECCIONES DE ESCUELAS DE LA FACULTAD DE CIENCIAS AMBIENTALES
    INGENIERIA FORESTAL
    GESTION AMBIENTAL
20. SECRETARIA DE LA UNIDAD DE ADMISION - PREUNIVERSITARIO
21. SALA DE REUNIONES DE FEUE
22. AULAS DEL PREUNIVERSITARIO
23. AULAS DE LA FACULTAD DE CIENCIAS AMBIENTALES
24. AULAS DE LA FACULTAD DE CIENCIAS AGRARIAS
25. CANCHAS
26. JEFATURA DE PERSONAL
27. OFICINA DE TRANSPORTE
28. DEPARTAMENTO DE EXTENSION Y TRANSFERENCIA DE TECNOLOGIAS - DETTEC
29. MECANICA
30. FACULTAD DE CIENCIAS EMPRESARIALES
    ESCUELAS
    ECONOMIA Y FINANZAS
    GESTION EMPRESARIAL
    MERCADOTECNIA
    CIENCIAS JURIDICAS
    CONTADORES PUBLICOS Y ASOCIADOS - CPA
    INGENIERIA EN SISTEMAS
31. INSTITUTO DE INFORMATICA
    LABORATORIO DE COMPUTO
    DIRECCION DEL INSTITUTO
    DEPARTAMENTO DE REDES
    LABORATORIOS DE INTERNET
    UNIDAD DE INFORMATICA AGROPECUARIA - UNIAGRO
    DEPARTAMENTO DE MANTENIMIENTO
    DESARROLLO Y DISEÑO DE SISTEMAS
    DEPARTAMENTO DE RELACIONES PUBLICAS
32. LABORATORIO BASICO
33. LABORATORIO DE BROMATOLOGIA
34. LABORATORIO DE BIOTECNOLOGIA
35. LABORATORIO DE FOTOGRAMETRIA
36. DEPARTAMENTO DE BIENESTAR UNIVERSITARIO - DBU
37. DEPARTAMENTO FINANCIERO
38. DEPARTAMENTO DE CONTABILIDAD
39. DEPARTAMENTO DE TESORERIA
40. DEPARTAMENTO DE PLANEAMIENTO ESTRATEGICO
41. DEPARTAMENTO DE PLANEAMIENTO FISICO - DPF
42. DEPARTAMENTO DE AUDITORIA

	Nº EDIFICIO
AUTORIDADES UNIVERSITARIAS	
HONORABLE CONSEJO UNIVERSITARIO - H.C.U.	5
RECTORADO	4
VICERECTORADO	7
SECRETARIO GENERAL Y PROCURADURIA	6
DEPARTAMENTOS ADMINISTRATIVOS	
DIRECCION ADMINISTRATIVA	1
DEPARTAMENTO FINANCIERO	37
DEPARTAMENTO DE CONTABILIDAD	38
DEPARTAMENTO DE TESORERIA	39
DEPARTAMENTO DE PLANEAMIENTO ESTRATEGICO	40
DEPARTAMENTO DE PLANEAMIENTO FISICO - DPF	41
DEPARTAMENTO DE PLANEAMIENTO ACADEMICO	12
JEFATURA DE PERSONAL	26
AUDITORIA	42
FACULTADES	
CIENCIAS EMPRESARIALES	30
ECONOMÍA	
- Ingeniería en Administración Financiera	
- Economía	
- Contaduría Pública Autorizada	
INGENIERIA EN GESTIÓN EMPRESARIAL	
INGENIERIA EN MARKETING	
INGENIERÍA EN SISTEMAS	31
TECNOLOGIA EN TELEMATICA	
PROGRAMA CARRERA DE CIENCIAS JURÍDICAS	
PROGRAMA CARRERA DE PSICOLOGIA EN GESTION LABORAL Y DESARROLLO ORGANIZACIONA	
CONTADURIA PUBLICA AUTORIZADA	
CIENCIAS AGRARIAS	12
INGENIERIA AGRONOMICA	
ADM. EMPRESAS AGROPECUARIAS	
HORTICULTURA Y FRUTICULTURA	
ECONOMIA AGRICOLA	
CIENCIAS AMBIENTALES	18
INGENIERIA FORESTAL	
GESTION AMBIENTAL	
UNIDADES ACADEMICAS	
UNIDAD DE ESTUDIOS A DISTANCIA	12
UNIDAD DE POSGRADO	10
CENTRO DE ESTUDIOS DE IDIOMAS	16
UNIDADES DE INVESTIGACION	
DEPARTAMENTO DE EXTENSION Y TRANSFERENCIA	28
UNIDAD DE INFORMATICA AGROPECUARIA	31
UNIDADES DE PRODUCCION	
IMPRENTA	3
TALLER DE MECANICA	29
OTRAS DEPENDENCIAS	
UNIDAD DE ADMISION - PRE	20
INSTITUTO DE INFORMATICA	31
PROVEEDURIA	8
BODEGA	9
ASOCIACION DE DOCENTES - ADUTEQ	11
ASOCIACION DE EMPLEADOS Y TRABAJADORES - AET	13
COPIADORA	14
COMEDOR	15
SALON AUDITORIUM	2

Tabla 2.1 Distribución de las Facultades de la UTEQ [1]

Figura 2.4 Facultad de Ciencias Agrarias

Figura 2.5 Campus Central de la UTEQ

Figura 2.6 Instituto de Informática (Derecha) y La Facultad de Ciencias Empresariales (Izquierda)

2.1.1 ORGANIGRAMA DE LA UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO

El diagrama de flujo sobre la situación organizacional de la Universidad Técnica Estatal de Quevedo se lo puede ver en detalle en el ANEXO A.

2.2. EQUIPOS UTILIZADOS EN LA RED DE DATOS DE LA UTEQ

A continuación se mencionan los equipos que están integrando la red de la UTEQ y más adelante se muestran los diagramas de ubicación de los equipos.

2.2.1 SWITCH CISCO CATALYST 2960G SERIES

Son switches de alto rendimiento diseñados para pasar de las redes LAN compartidas tradicionales a redes completamente conmutadas. La Universidad utiliza como elemento de interconexión de su red de datos, los Switches CISCO Catalyst 2960G porque ofrecen un alto rendimiento, administración y escalabilidad. Estos equipos cuentan con puertos con configuraciones *PoE (Power over Ethernet).* Para las seguridades cuenta con un amplio rango de métodos de autenticación, tecnologías para encriptación de datos. Además posee *Smartports* para autoconfiguraciones de aplicaciones especializadas. Para mayor información del equipo referirse al ANEXO B1.

Figura 2.7 Switch CISCO Catalyst 2960G

Figura 2.8 Switch CISCO C2960G-24TC-L

Características	Especificación
Número de puertos	24
Velocidad por puerto	10/100/1000 Mbps.
Escalabilidad	4 puertos que pueden ser usados para UPLINK
Control de red y ancho de banda	Se tiene habilitado QoS, ACLs y Servicios multicast
Seguridad	A nivel de filtrado MAC
Sistemas de BackUp	A través del protocolo STP[8]

Tabla 2.2 Cuadro de características de los switch CISCO 2960G de la UTEQ

2.2.1.1 Rendimiento de los equipos de red de la UTEQ

Cuadro de rendimiento de los principales equipos de interconectividad de la red de la UTEQ se encuentran en el ANEXO C.

Como se puede observar en los gráficos y más detenidamente, en el rendimiento valorado en 1 minuto, el procesamiento de cada switch no supera el 20% pico de utilización. Entonces, el dimensionamiento de los equipos de core se ajustan a las necesidades actuales y sobre todo dejan un amplio margen para futuras expansiones de la Universidad.

En el ANEXO C de rendimiento, podemos observar que el rango de conexiones en los horarios más conflictivos (11:00 AM, 15:00 pm y 17:00 pm), está entre los 200 y 300 computadores o conexiones simultaneas, con lo cual se afirma, que el dimensionamiento actual de la universidad está al momento acorde con los sistemas que se manejan internamente y no presentan indicios de saturación en los canales de comunicación.

[8] STP Spanning Tree Protocol. Protocolo que evita la generación de lazos de enrutamiento.

2.2.2 ROUTER CISCO 2600 SERIES

Este equipo es un router modular multiservicio, ya que permite la integración de voz y datos. Este equipo es propiedad de TELCONET para dar acceso a la universidad a la red Internet. Las características de este equipo también permiten los servicios de acceso a redes privadas virtuales con opciones de firewall. Además, permite servicios de acceso telefónico analógico y digital, enrutamiento con gestión de ancho de banda y enrutamiento entre VLAN. Para mayores detalles sobre este equipo ver ANEXO B2.

Figura 2.9 Router CISCO 2600

Características	Especificaciones
Número de puertos	4 puertos Fast Ethernet 3 puertos seriales (se utilizan tarjetas WIC)
Velocidad de puerto	Fast Ethernet 10/100 Interface serial a 5 Mbps (Proveedor de Internet)
Control de red, ancho de banda y ruteo	Se tiene habilitado QoS, VLANs y ruteo mediante BGP y OSPF
Seguridad	No se tiene habilitado
Sistemas de BackUp	A través de tarjetas WIC para la interfaz serial

Tabla 2.3 Cuadro de características del router CISCO 2600 de la UTEQ

2.2.3 EQUIPO INALÁMBRICO OUTDOOR ROUTER ORINOCO OR 1100

Es un router inalámbrico de altas velocidades, utilizado para exteriores. Este dispositivo permite crear un sistema punto a punto para enlazar dos redes LAN. Este equipo opera sobre la banda de 2.4 GHz y logra un alcance de hasta 26 KM con una transmisión de datos de hasta 11 Mbps. Además este equipo posee interfaces 10/100Base-T, que le permiten su integración con redes Ethernet de 10 y 100Mb/s. Más detalles sobre este equipo los encuentra en el ANEXO B3.

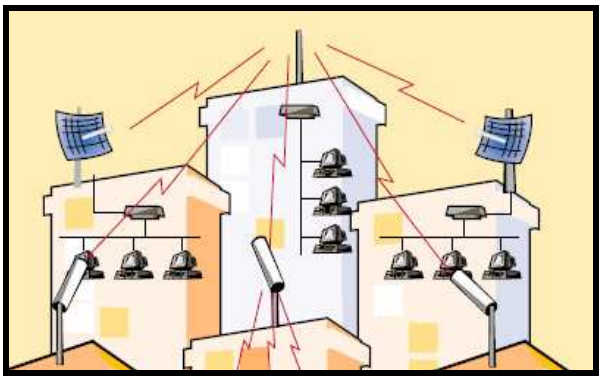


Figura 2.10 Esquema de una conexión con los equipos inalámbricos de Outdoor Router ORINOCO OR 1100

Características	Especificaciones
Enlaces	Punto-Punto o Punto-Multipunto, operando en banda 2.4 GHz.
Interfaces	10/100 Base-T Ethernet, permite integración de ambientes de 10 y 100 Mb/s Ethernet.
Velocidades	Velocidad de 11 Mbps y 5.5 Mbps, velocidades mayores que un E1/T, con alcance máximo de 26 Km.
Seguridades	Usa encriptación de 64-bit WEP y 128 bit RC4, Tabla de Control de Acceso basada en direcciones MAC.

Tabla 2.4 Cuadro de características del router inalámbrico ORINOCO OR 1100 de la UTEQ

2.2.4 EQUIPO INALÁMBRICO ACCESS POINT DLINK DWL 2100AP

Este *Access Point* es compatible tanto con los estándares 802.11b como con el 802.11g. Además cuenta con un Sistema de Distribución Inalámbrica (*WDS: Wireless Distribution System*), que le permite trabajar como puente (bridge) punto a punto o puente punto multipunto, con un alcance de 100m en interiores o 400m en exteriores. Soporta SNMPv3, para la administración del equipo y como técnica de acceso al medio utiliza CSMA/CA. La función de este equipo es como elemento de acceso a las redes inalámbricas implementadas en la UTEQ, las mismas que se explican más adelante. Para más detalles sobre este equipo referirse al ANEXO B4.

Figura 2.11 Equipo DWL 2100AP

Características	Especificaciones
Velocidad	Velocidades de hasta 54 Mbps o 108 Mbps utilizando productos Tecnología D-Link 108G.
Gestión de dispositivo	Web-Based, SNMP v3.
Sistema de Distribución Wireless	AP cliente, Punto-Punto, Punto-Multipunto, Repetidor.
Seguridades	64-,128 152-bit WEP, 802.1X, WPA, MAC Address Access Control.

Tabla 2.5 Cuadro de características del dispositivo inalámbrico DLINK DWL 2100AP de la UTEQ

2.2.5 EQUIPO INALÁMBRICO ACCESS POINT DLINK DWL 3200AP

Este equipo permite tener redes inalámbricas robustas y altamente gestionables y cuenta con dos antenas de alta ganancia para una óptima cobertura. Es

compatible con los estándares 802.11g y 802.11b. Además posee integrado la tecnología *Power over Ethernet* (PoE, 802.3af). Los alcances de este equipo son máximo 100m para interiores y 500m para exteriores. Para la gestión del equipo se cuenta con un *web browser, telnet*, SNMPv3. Para mayores detalles sobre el equipo referirse al ANEXO B5.

Figura 2.12 Equipo DWL 3200AP

Características	Especificaciones
Estándares que soporta	IEEE 802.11b, IEEE 802.11g, IEEE 802.3, IEEE 802.3af, IEEE 802.3u.
Velocidad	Velocidades de hasta 54 Mbps o 108 Mbps utilizando productos Tecnología D-Link 108G.
Gestión de dispositivo	HTTP, SNMP v3, AP Manager II, Telnet, Secure (SSH) Telnet.
Modos de Operación	Access Point, WDS con AP
Seguridades	64-, 128 152-bit WEP, WPA2 Enterprise, MAC Address Access Control List, Configuración de Seguridades individuals para cada SSID.

Tabla 2.6 Cuadro de características del dispositivo inalámbrico DLINK DWL 3200AP de la UTEQ

2.2.6 EQUIPO INALÁMBRICO LINKSYS WAP54G

Este dispositivo permite alcanzar velocidades de transmisión de hasta 54Mbps con el estándar 802.11g, sin perder también la capacidad de trabajar con equipos del estándar 802.11b que operan a 1Mbps. Este equipo tiene como función permitir el acceso inalámbrico a los usuarios finales. Como sistema de seguridad cuenta con encriptación *WEP*[9]. Para mayor información referirse al ANEXO B6.

Figura 2.13 Equipo Linksys WAP54G

Características	Especificaciones
Estándares que soporta	802.11g, 802.11b.
Velocidad	Hasta 54 Mbps (Wireless) y 10/100 Mbps (Ethernet).
Gestión de dispositivo	Web Browser.
Seguridades	Encriptación 128-bit WEP y Filtración de direcciones MAC.

Tabla 2.7 Cuadro de características del dispositivo inalámbrico LINKSYS WAP54G de la UTEQ

2.2.7 SWITCH 3COM BASELINE 2824

Son switches de capa dos no administrables. Poseen puertos con auto MDI/MDIX, que identifican y se adaptan al tipo de cable Ethernet, también son puertos

[9] Wired Equivalent Privacy, es un sistema de encriptación estándar implementado en la MAC y soportado por la mayoría de las soluciones inalámbricas.

autosensing de 10BASE-T/100BASE-TX/1000BASE-T, es decir, que se ajustan a la velocidad del dispositivo conectado. Este equipo tiene como función el dar acceso a la red LAN de las distintas facultades. Para más detalles sobre este equipo, referirse al ANEXO B7.

Figura 2.14 Switch 3COM Baseline 2824

Características	Especificaciones
Estándares que soporta	IEEE 802.1d, IEEE 802.1p, IEEE 802.3, IEEE 802.3ab, IEEE 802.3u, IEEE 802.3x, IEEE 802.3z.
Puertos	24 puertos con auto negociación 10BASE-T/100BASE-TX/1000BASE-T. Puertos configurados con auto MDI/MDIX.
Velocidad	Capacidad de switching hasta 48 Gbps.
Calidad de Servicio	IEEE 802.1p (CoS/QoS).

Tabla 2.8 Cuadro de características del Switch 3COM Baseline 2824 de la UTEQ

2.2.8 EQUIPO FAST-ETHERNET UNICOM DYNA SWITCH/16

Este switch cuenta con 16 puertos con ancho de banda dedicado de 10/100 Mbps y con modo de operación full-dúplex, que le permite tener el doble de ancho de banda en cada puerto, es decir, 20Mbps y 200Mbps, respectivamente. Además cuenta con características de autoconfiguración MDI/MDIX. Para mayores detalles sobre este equipo, referirse al ANEXO B8.

Figura 2.15 UNICOM Dyna Switch/16

Características	Especificaciones
Estándares que soporta	IEEE 802.3, IEEE 802.3u
Puertos	16 puertos 10/100 Base-TX Fast Ethernet.
Ancho de banda	Puede incrementar de 10 Mbps Ethernet y 100 Mbps Ethernet a 20 y 200 Mbps Ethernet por puerto.
Protocolo	CSMA/CD.

Tabla 2.9 Cuadro de características del UNICOM Dyna Switch/16 de la UTEQ

2.3. DESCRIPCIÓN DE LA RED DE DATOS DE LA UTEQ

La siguiente parte comprende la descripción de la red LAN de la UTEQ. Aquí se explican, el backbone de la red, sus enlaces inalámbricos principales entre los diferentes campus y las subredes Fast Ethernet.

2.3.1. BACKBONE PRINCIPAL DE LA RED DE DATOS DE LA UTEQ

La red de la Universidad tiene un backbone de fibra óptica de tendido aéreo instalada en su campus principal. La fibra es de tipo monomodo de 12 hilos (6 hilos para transmisión y 6 hilos para recepción). Este tipo de tecnología le permite a la estructura principal de la red llevar datos a velocidades que se encuentran en

los rangos de decenas de Gbps con distancias de hasta un límite de 100 km como máximo.

La topología del backbone es tipo estrella alrededor de todo el campus de la universidad, como se puede ver en la figura 2.16. El backbone incluye 12 switches CISCO Catalyst 2960G de 24 puertos TC-L. Así como un enlace redundante entre Rectorado y el Pre-Universitario.

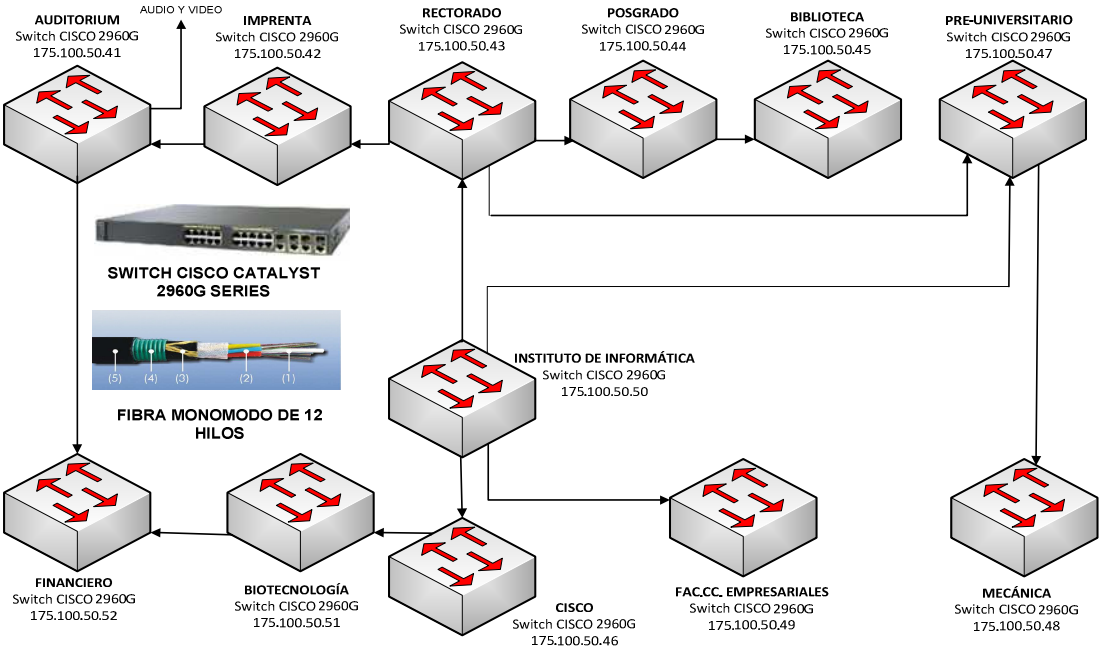


Figura 2.16 Diagrama general del Backbone de Fibra Óptica de la UTEQ

Los hilos de fibra, se encuentran en los siguientes estados (Tabla 2.10), y están distribuidos cómo se indica en el ANEXO D.

	Color	Función
1	AZUL	OPERANDO
2	NARANJA	
3	VERDE	BACKUP
4	CAFÉ	
5	GRIS	RESERVA
6	BLANCO	

Tabla 2.10 Estados de los hilos de fibra óptica de la red UTEQ

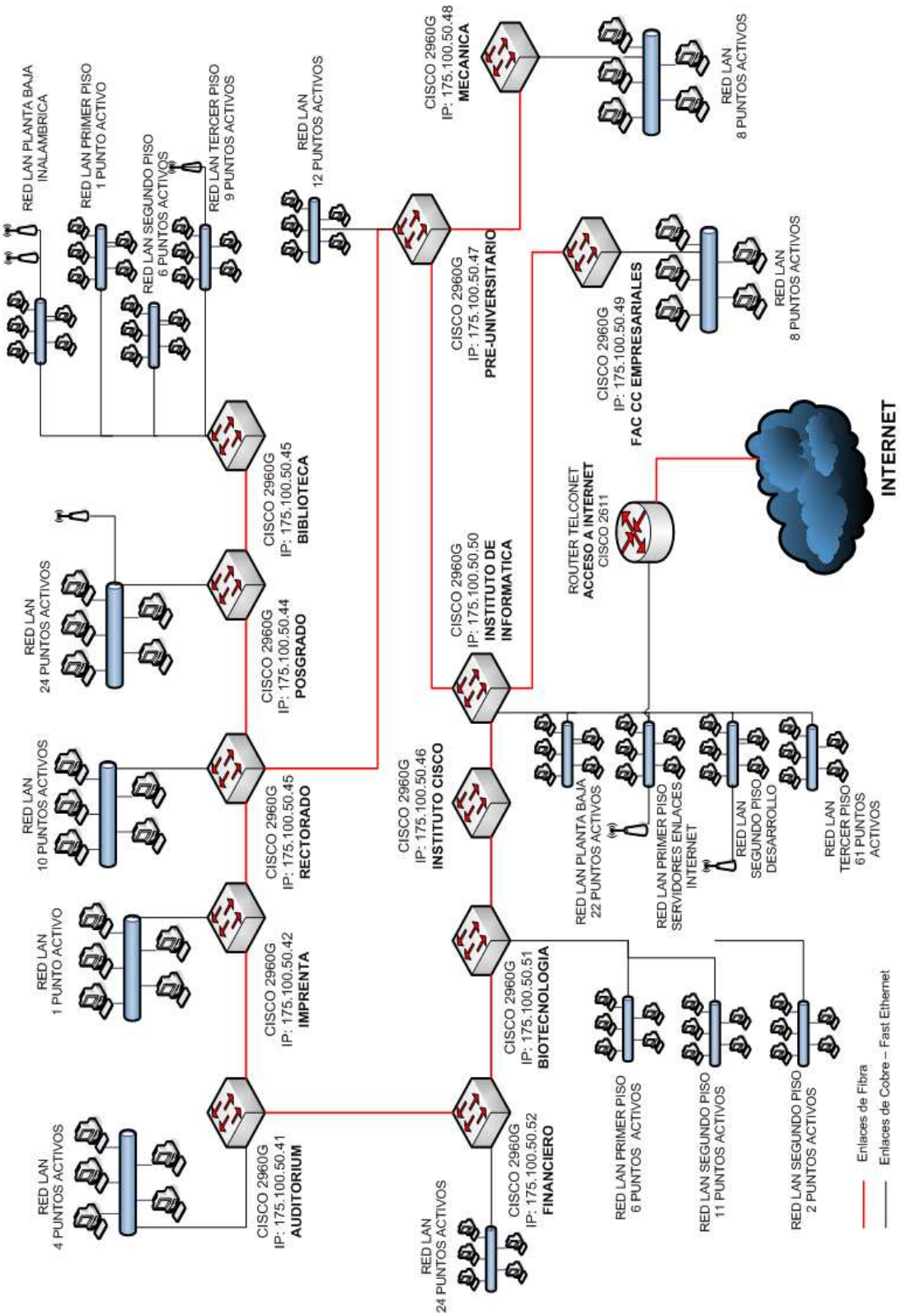


Figura 2.17 Diagrama general de la red de la UTEQ

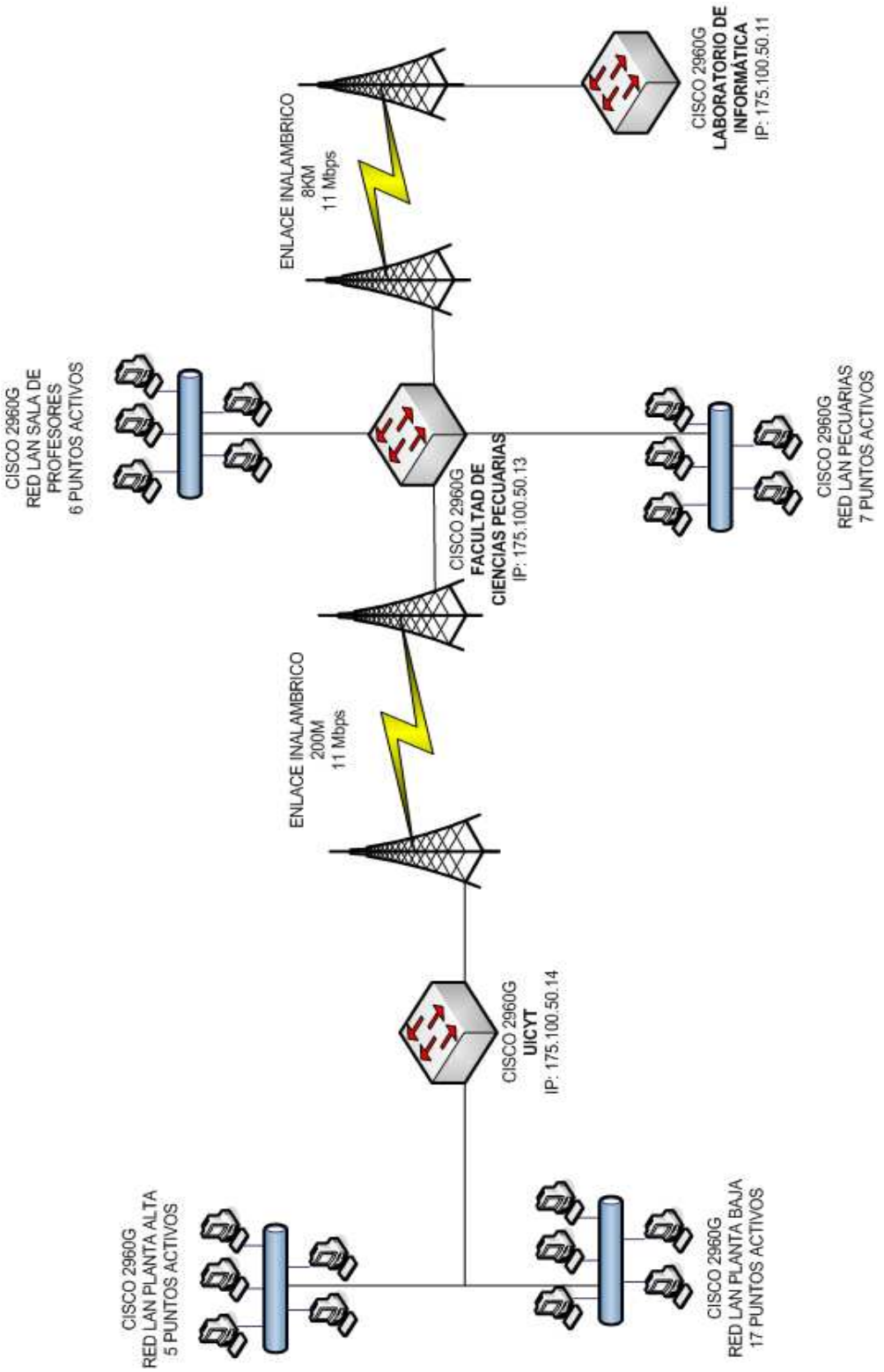


Figura 2.18 Diagrama de la red inalámbrica de la UTEQ

2.3.2. ENLACE INALÁMBRICO ENTRE LOS PREDIOS DEL CAMPUS CENTRAL DE LA UTEQ Y LA FACULTAD DE CIENCIAS PECUARIAS

La UTEQ tiene como segundo campus, la finca “La María”, ubicada a 8 Km de los predios centrales. En esta finca se encuentran ubicadas las instalaciones de la Facultad de Ciencias Pecuarias (FCP) y de la Unidad de Investigación de Ciencia y Tecnología (UICYT), importantes en la generación de la información e investigación.

Para comunicar los predios del campus principal y la Facultad de Ciencias Pecuarias en “La María”, se cuenta con un enlace inalámbrico que utiliza tecnología 802.11b. Este enlace utiliza routers para exteriores ORINOCO OR 1100. La distancia del enlace es de 8 Km con velocidades de hasta 11Mbps, y sobre una frecuencia de 2.4 GHz.

El router ORINOCO OR 1100 le permite a la red inalámbrica integrarse con redes cableadas ya existentes o nuevas, de tipo Ethernet 10/100BASE-T. Cabe indicar que trabaja con el protocolo CSMA/CD para acceso de LAN IEEE 802.3.

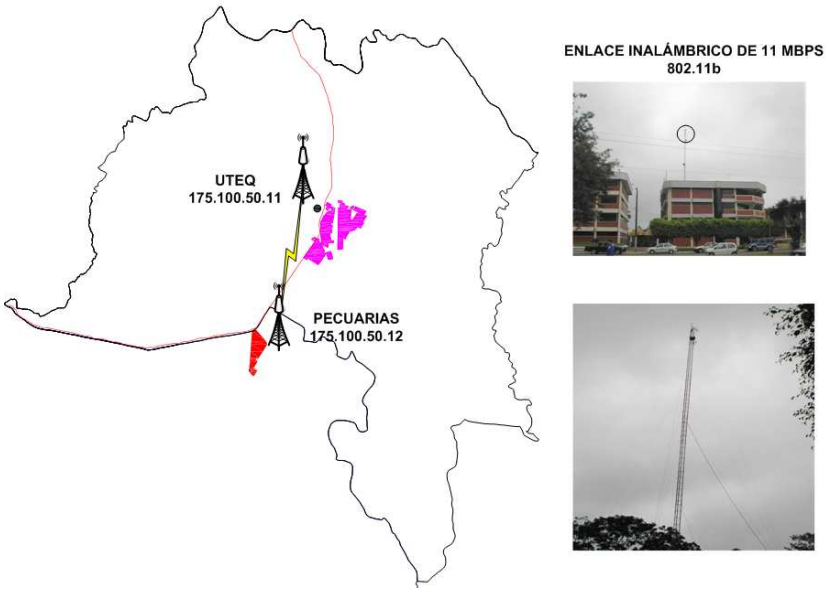


Figura 2.19 Enlace inalámbrico de los Predios del Campus Central de la UTEQ y la Facultad de Ciencias Pecuarias (Campus finca “La María”)

ENLACE CAMPUS CENTRAL UTEQ – FACULTAD CIENCIAS PECUARIAS	
DIRECCIÓN IP	**UBICACIÓN**
175.100.50.11	ACCESS POINT UTEQ (INSTITUTO DE INFORMÁTICA)
175.100.50.12	ACCESS POINT FAC.CC.PECUARIAS

Tabla 2.11 Direcciones IP del enlace UTEQ – Pecuarias de la Figura 2.19

2.3.3. ENLACE INALÁMBRICO ENTRE LA FACULTAD DE CIENCIAS PECUARIAS Y LA UICYT

Para la comunicación de las instalaciones que se encuentran en “La María”, se cuenta con un enlace inalámbrico implementado con los equipos Outdoor Router ORINOCO OR 1100 al igual que el numeral anterior. El enlace tiene una distancia de 200 m, con transmisión de datos de hasta 11Mbps sobre la banda de frecuencia de 2.4 GHz.

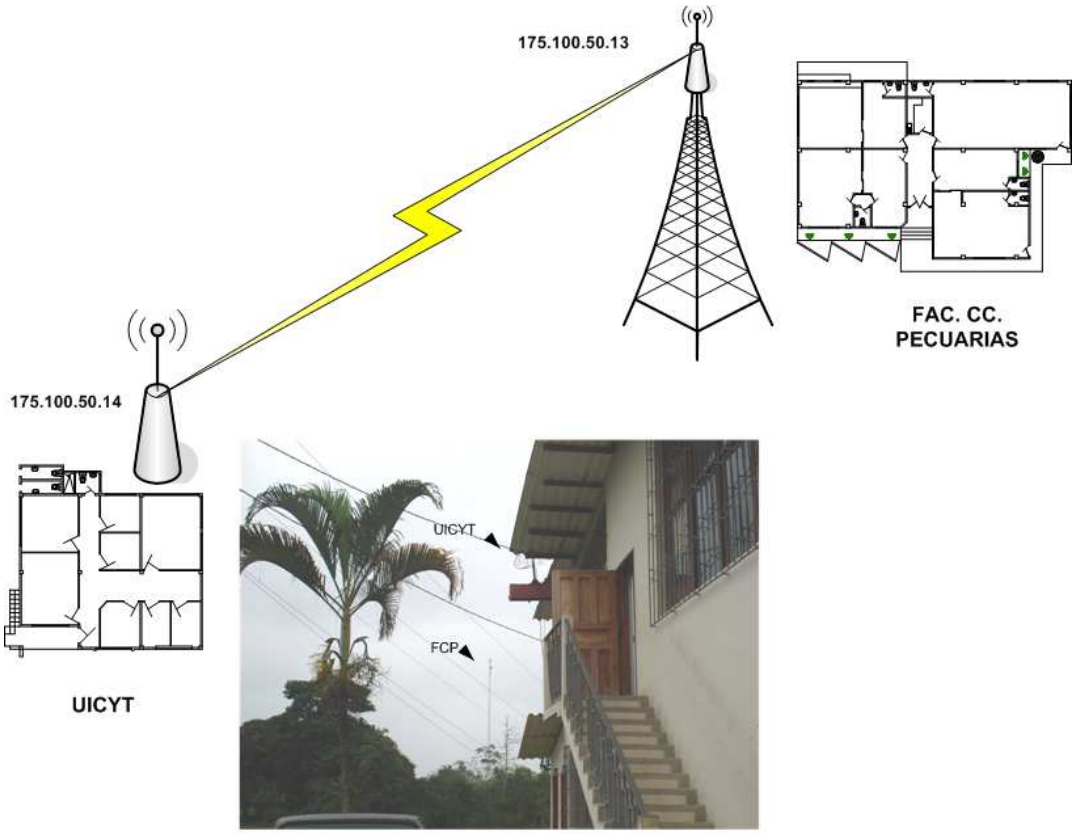


Figura 2.20 Enlace Inalámbrico entre la Facultad de Ciencias Pecuarias y la UICYT

ENLACE FAC. CC. PECUARIAS - UICYT	
DIRECCIÓN IP	**UBICACIÓN**
175.100.50.14	ACCESS POINT UICYT
175.100.50.13	ACCESS POINT FAC.CC.PECUARIAS

Tabla 2.12 Direcciones IP de los Puntos de Acceso de la Figura 2.20

2.3.4. SUBRED LAN FAST ETHERNET DE LA FACULTAD DE CIENCIAS PECUARIAS

Las subredes Fast Ethernet de la LAN de la UTEQ son redes cableadas Fast Ethernet tipo 100Base-T[10]. Las subredes tienen topologías físicas en estrella que se concentran en switches (del backbone) CISCO Catalyst 2960G de 24 puertos administrable, ubicados en cada uno de los racks de comunicaciones principales de la red. Cabe indicar que la LAN utiliza direccionamiento IPv4.

La subred de la Facultad de Ciencias Pecuarias a su vez se compone de subredes más pequeñas, como son la Subred 1 compuesta por Sala de Profesores, Sala de Internet y la Dirección de Escuela, la Subred 2 compuesta por 7 puntos de red activos.

2.3.4.1.Subred 1. Sala de Profesores, Sala de Internet y la Dirección de Escuela

Esta subred cuenta con 6 puntos activos para la Sala de Internet, 2 puntos activos para la Sala de Profesores y 1 punto activo para la Dirección de la Escuela. La subred posee todas las características referidas anteriormente para Fast Ethernet en el primer párrafo del numeral 2.3.4.

[10] Redes con par trenzado, uno para transmisión y otro para recepción, usan STP o UTP de categoría 5 y esquema de señalización MLT3

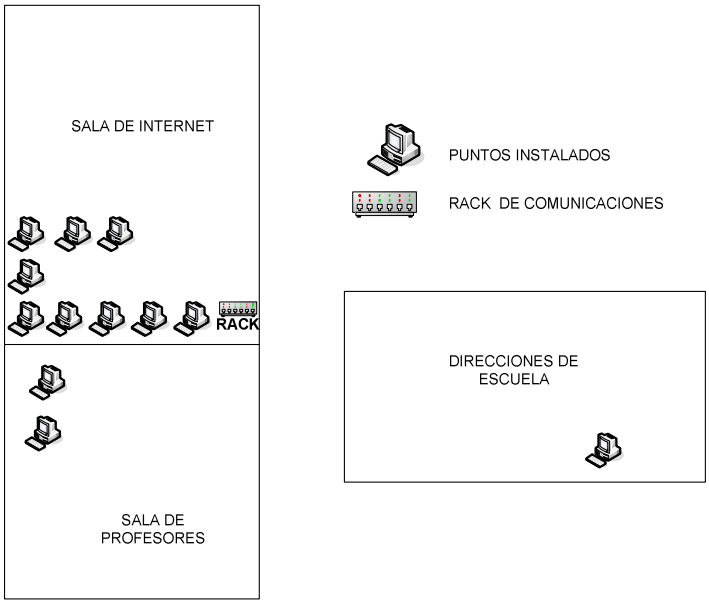


Figura 2.21 Subred Fast Ethernet de la Sala de Profesores, Sala de Internet y Dirección de Escuela de la Facultad de Ciencias Pecuarias (FCP)

PUNTOS ACTIVOS	
DIRECCIÓN IP	**UBICACIÓN**
175.100.50.208	DIRECCIONES DE ESCUELA
175.100.50.209	SALA DE INTERNET
175.100.50.210	SALA DE INTERNET
175.100.50.211	SALA DE INTERNET
175.100.50.212	SALA DE INTERNET
175.100.50.213	SALA DE INTERNET
175.100.50.214	SALA DE INTERNET
175.100.50.233	SALA DE DE PROFESORES
175.100.50.234	SALA DE PROFESORES

Tabla 2.13 Direcciones IP de los Puntos Activos de Figura 2.21

2.3.4.2.Subred 2. Facultad de Ciencias Pecuarias

Esta subred se compone de 7 puntos activos, distribuidos cada uno para: la secretaria del Decano, Subdecano, Secretario del Abogado, secretarias y la Comisión de Evaluación de la Facultad de Ciencias Pecuarias. Es una subred Fast Ethernet con características antes mencionadas en el numeral 2.3.4, que se

concentra en un rack de comunicaciones principal ubicado en la secretaría del decano, donde se encuentra un switch CISCO de la serie 2960 administrable, de especificaciones mencionadas anteriormente.

Adicionalmente la subred consta de equipos inalámbricos, que le permiten la comunicación a la red cableada con el campus central y también con UICYT.

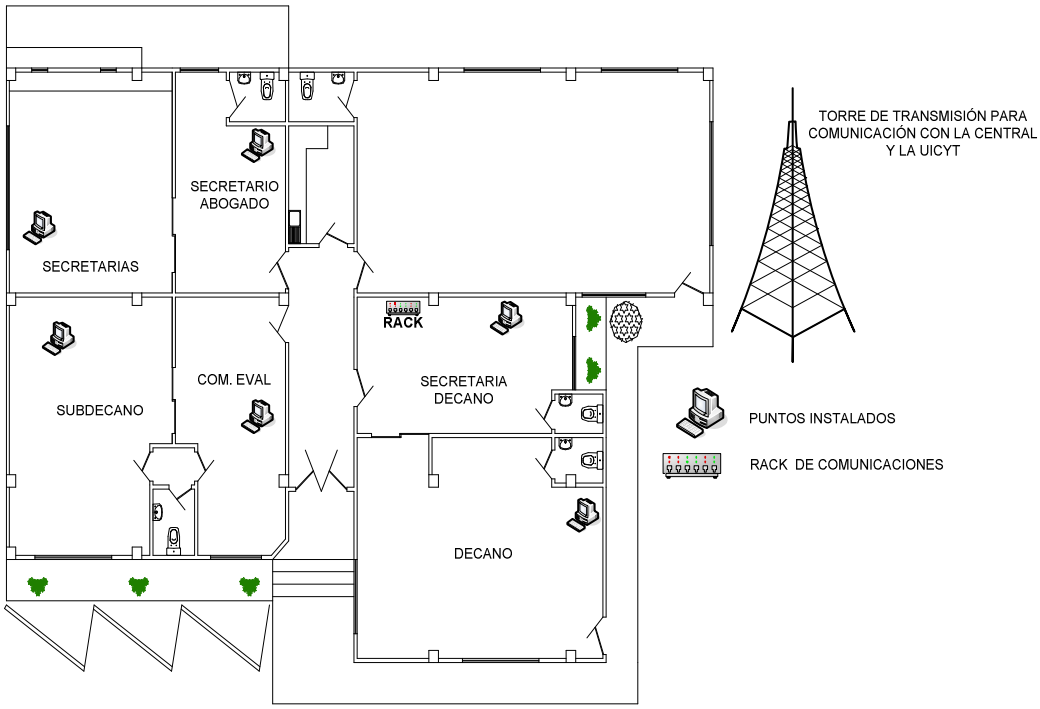


Figura 2.22 Subred Fast Ethernet de la Facultad de Ciencias Pecuarias

PUNTOS ACTIVOS	
DIRECCIÓN IP	**UBICACIÓN**
175.100.50.13	ACCESS POINT FAC. PEC - UICYT
175.100.50.12	ACCESS POINT FAC. PEC - CENTRAL
175.100.50.201	SUBDECANO
175.100.50.202	SECRETARIO - ABOGADO
175.100.50.203	SECRETARIA DECANO
175.100.50.204	SECRETARIA
175.100.50.237	COM. EVAL. FAC. CC. PECUARIAS

Tabla 2.14 Direcciones IP de los Puntos Activos de Figura 2.22

2.3.5. SUBRED LAN FAST ETHERNET DE LA UNIDAD DE INVESTIGACIÓN DE CIENCIA Y TECNOLOGÍA (UICYT)

Esta subred está compuesta por las subredes de la planta alta y planta baja de la UICYT.

En la **planta alta** la subred se compone de 5 puntos, destinados para los investigadores que trabajan en esta Unidad. Es una subred Fast Ethernet con las características antes mencionadas en el numeral 2.3.4, que se concentra en un rack de comunicaciones principal ubicado en la planta baja del edificio de la Unidad de Investigación de Ciencia y Tecnología (UICYT), donde se encuentra un switch CISCO de la serie 2960, con características de tipo Administrable.

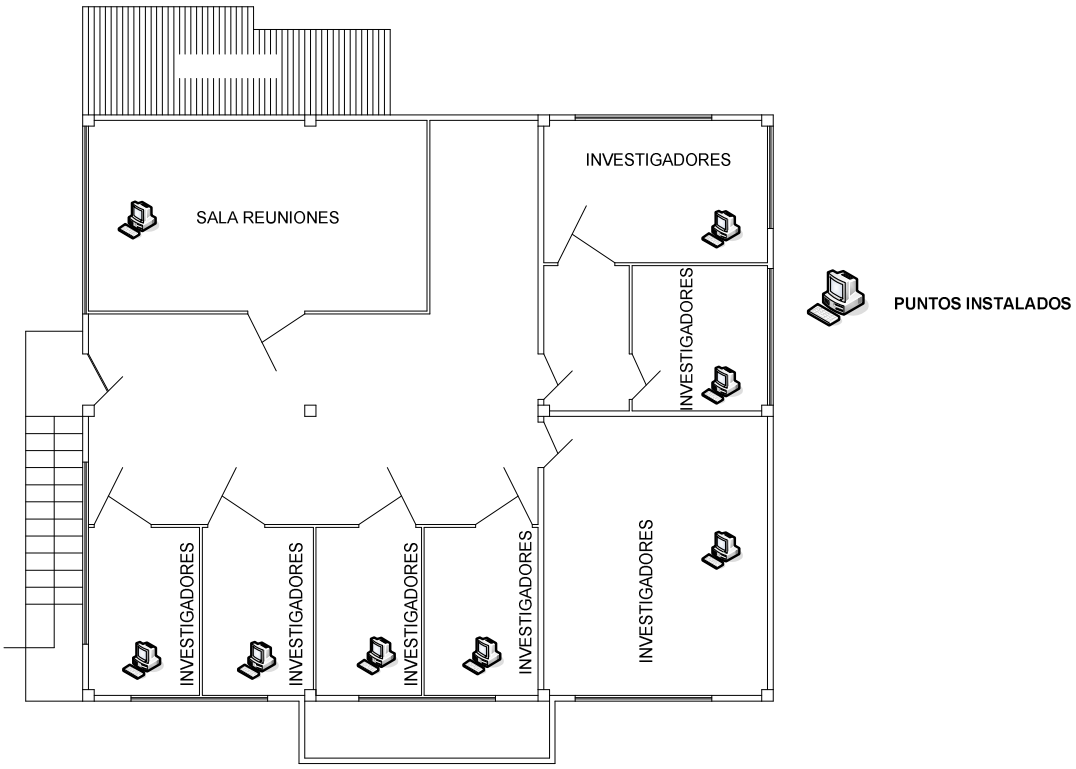


Figura 2.23 Subred de la Planta Alta de la UICYT

PUNTOS ACTIVOS	
DIRECCIÓN IP	**UBICACIÓN**
175.100.50.224	INVESTIGADOR
175.100.50.225	INVESTIGADOR
175.100.50.230	INVESTIGADOR
175.100.50.238	INVESTIGADOR
175.100.50.243	INVESTIGADOR

Tabla 2.15 Direcciones IP de los Puntos Activos de Figura 2.23

En la **planta baja** la subred se compone de 17 puntos activos, destinados a los investigadores, el Director de la UICYT, los Subdirectores de la UICYT, la secretaria, y el Administrador de la finca “La María”. La subred Fast Ethernet tiene las características antes mencionadas en el numeral 2.3.4.

Toda la subred se concentra en el rack de comunicaciones principal ubicado en una de las oficinas de los investigadores del edificio de la Unidad de Investigación de Ciencia y Tecnología (UICYT) como se puede ver en la figura 2.24. Donde se encuentra un switch CISCO de la serie 2960, con características de tipo Administrable, referido anteriormente**.**

La subred también tiene equipos inalámbricos, como el Access Point exterior marca ORINOCO antes mencionado, para permitir el enlace de la UICYT con la Facultad de Ciencias Pecuarias. Adicionalmente, la subred consta de un lector biométrico por cuestiones de identificación.

PUNTOS ACTIVOS	
DIRECCIÓN IP	**UBICACIÓN**
175.100.50.7	DISPOSITIVO BIOMÉTRICO
175.100.50.206	INVESTIGADOR
175.100.50.207	SUBDIRECTOR
175.100.50.215	INVESTIGADOR
175.100.50.216	INVESTIGADOR
175.100.50.217	INVESTIGADOR
175.100.50.218	SECRETARIA
175.100.50.221	INVESTIGADOR
175.100.50.222	INVESTIGADOR

175.100.50.223	INVESTIGADOR
175.100.50.226	ADM. FINCA LA MARIA
175.100.50.227	SUBDIRECTOR
175.100.50.228	INVESTIGADOR
175.100.50.229	DIRECTOR
175.100.50.242	INVESTIGADOR
175.100.50.254	INVESTIGADOR

Tabla 2.16 Direcciones IP de los Puntos Activos de Figura 2.24

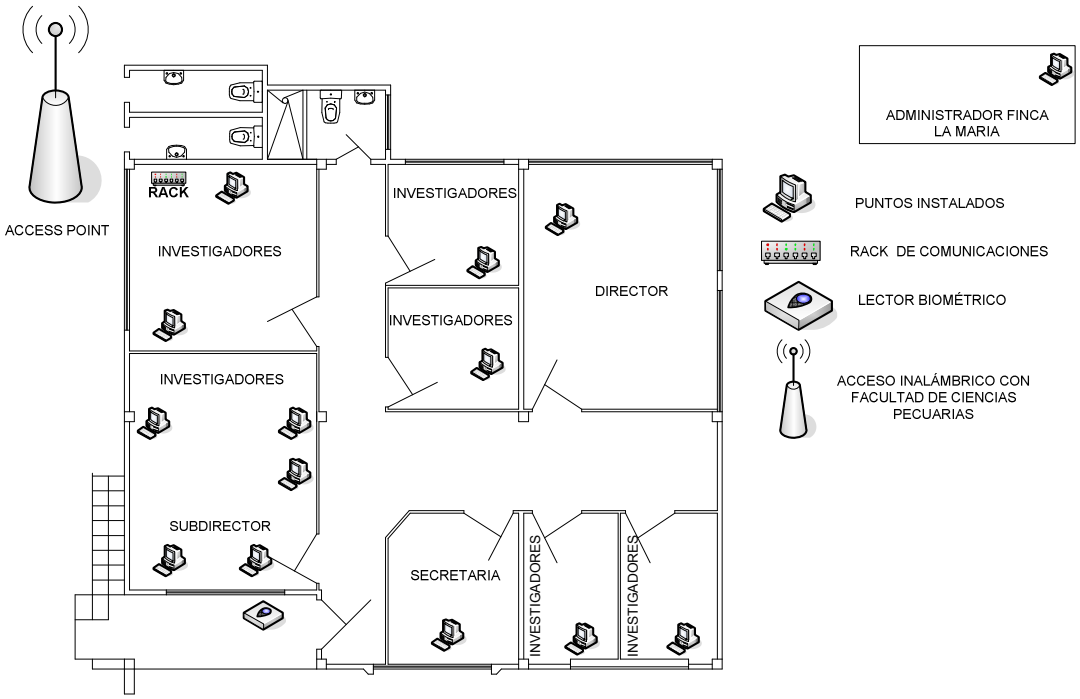


Figura 2.24 Subred de la Planta Baja de la UICYT

2.3.6. SUBRED LAN FAST ETHERNET DE LA MECÁNICA, DPF (DEPARTAMENTO DE PLANEACIÓN FÍSICA) Y DETTEC (DEPARTAMENTO DE TRANSFERENCIA DE TECNOLOGÍA)

Esta subred se compone de 8 puntos activos destinados al jefe de la Mecánica, al director, asistente y secretaria del Departamento de Planeación Física (DPF) y también al director, secretaria y extensionistas del DETTEC. Esta es una subred

Fast Ethernet con las características antes mencionadas numeral 2.3.4. La subred se concentra en el rack de comunicaciones principal ubicado en la oficina del DETTEC como se puede ver en la figura 2.25. Donde se encuentra un switch CISCO de la Serie 2960, con características de tipo Administrable, como ya antes se mencionó.

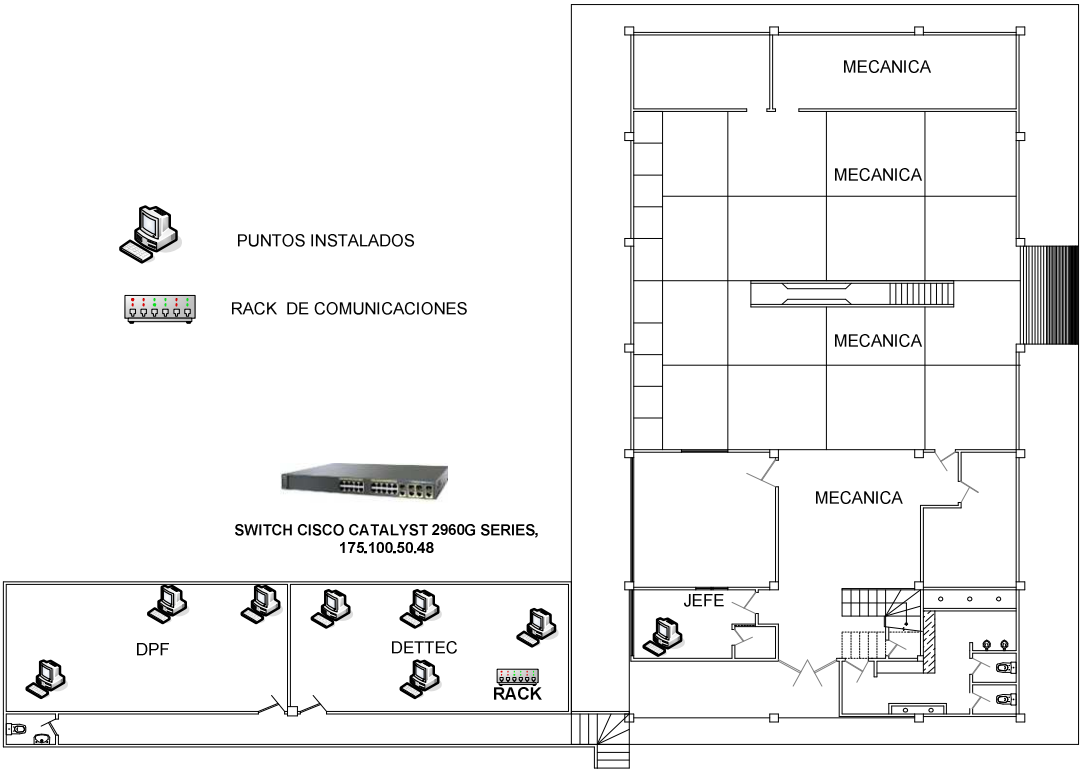


Figura 2.25 Subred de la Mecánica, DPF y DETTEC

PUNTOS ACTIVOS	
DIRECCIÓN IP	**UBICACIÓN**
175.100.50.125	DPF – DIRECTOR
175.100.50.126	DPF – ASISTENTE
175.100.50.188	DPF – SECRETARIA
175.100.50.189	DETTEC – DIRECTOR
175.100.50.195	DETTEC – SECRETARIA
175.100.50.196	DETTEC – EXTENSIONISTAS
175.100.50.220	MECANICA
192.168.1.247	DETTEC - EXTENSIONISTAS

Tabla 2.17 Direcciones IP de los Puntos Activos de Figura 2.25

2.3.7. SUBRED LAN FAST ETHERNET DEL CEDI, FACULTAD DE CIENCIAS AMBIENTALES, UNIDAD DE ADMISIÓN, FEUE - AFU – LIGA

Esta red se compone de 12 puntos activos, distribuidos para la Dirección CEDI (Centro de Estudios de Idiomas), las secretarias de CEDI, el Decano y Subdecano Facultad de Ciencias Ambientales, las secretarias tanto para la Facultad de Ciencias Ambientales como para Admisión, las Direcciones de Escuelas, para FEUE (Federación de Estudiantes Universitarios del Ecuador), AFU (Asociación Feminista Universitaria) y LIGA (nombre de Asociación de Deportes de la UTEQ). Esta es una subred Fast Ethernet que tiene las características antes mencionadas en el numeral 2.3.4. La subred se concentra en un rack de comunicaciones principal donde se ubica un switch CISCO de la Serie 2960, administrable.

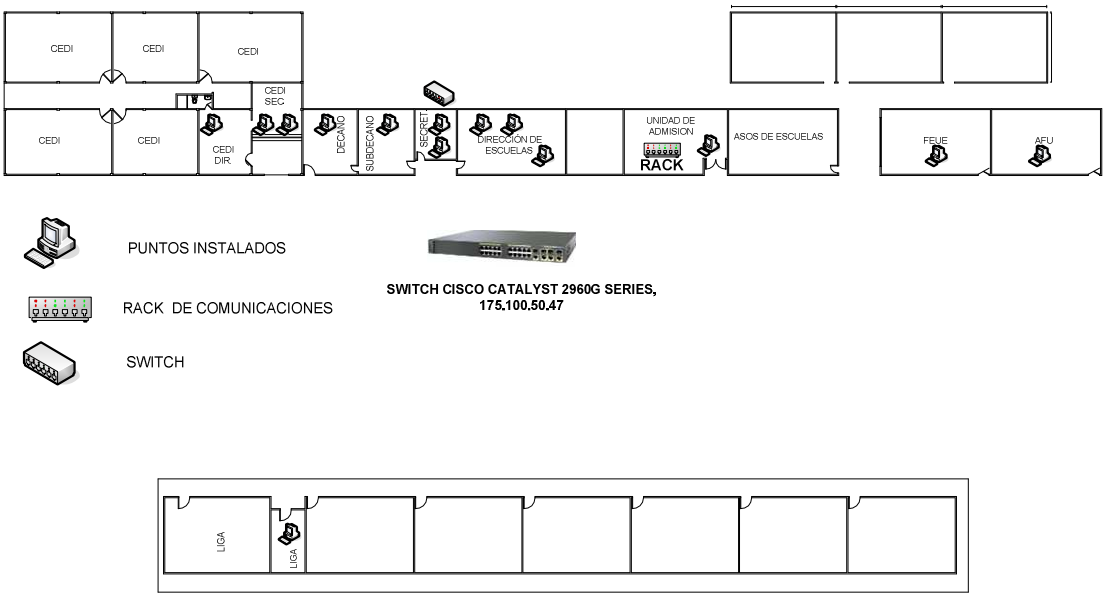


Figura 2.26 Subred CEDI, Facultad de Ciencias Ambientales (FCA), Unidad de Admisión, FEUE-AFU-LIGA

PUNTOS ACTIVOS	
DIRECCIÓN IP	**UBICACIÓN**
175.100.50.100	SECRETARIO – ABOGADO FAC. AMB
175.100.50.183	ADMISIÓN – DIRECTOR
175.100.50.184	CEDI - SECRETARIA

175.100.50.185	DECANO FAC .AMB.
175.100.50.186	SUBDECANO FAC. AMB
175.100.50.187	SECRETARIA FAC. AMB
175.100.50.190	SECRETARÍA - ADMISIÓN
192.168.1.249	DIR. ESC. FORESTAL
192.168.1.250	DIR. ESC. AMBIENTAL
192.168.1.251	LIGA
192.168.1.252	FEUE
192.168.1.253	AFU

Tabla 2.18 Direcciones IP de los Puntos Activos de Figura 2.26

2.3.8. SUBRED LAN FAST ETHERNET DE LA FACULTAD DE CIENCIAS AGRARIAS

Esta subred está compuesta por puntos activos de los pisos 1, 2, 3 y planta baja de la Facultad de Ciencias Agrarias. En este **primer piso** solo se encuentra un punto de red activo correspondiente al personal del IECE (Instituto Ecuatoriano de Crédito Educativo) que tienen sus oficinas en la institución. Este punto se une a las demás subredes.

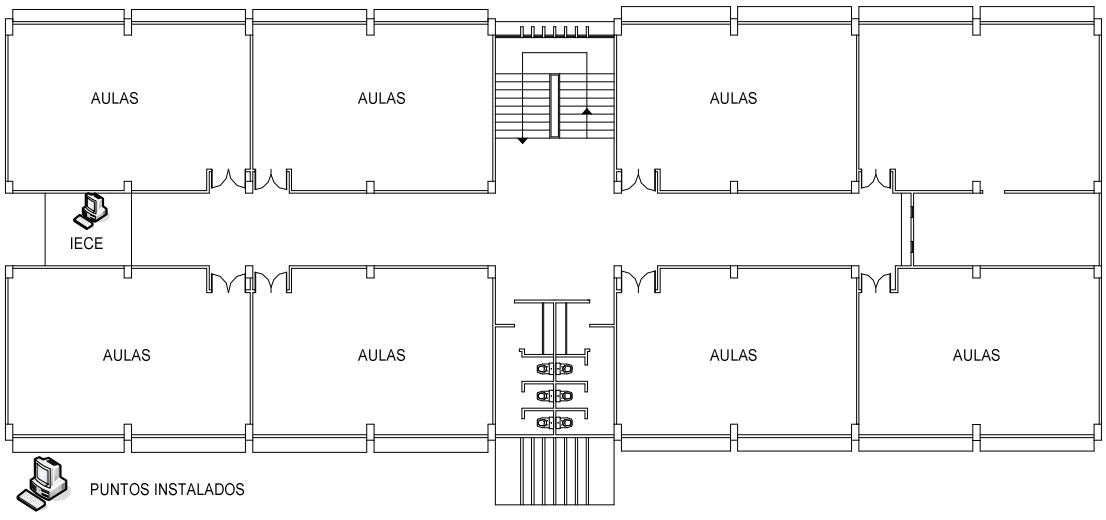


Figura 2.27 Puntos de red activos en el primer piso de la Facultad de Ciencias Agrarias

PUNTOS ACTIVOS	
DIRECCIÓN IP	**UBICACIÓN**
175.100.50.97	IECE

Tabla 2.19 Direcciones IP de los Puntos Activos de Figura 2.27

En el **segundo piso** se encuentran 6 puntos activos destinados a la UPA (Unidad de Planeamiento Académico) y al área destinada para el desarrollo de proyectos financiados por el FODI (Fondo de Desarrollo Infantil). Esta es una subred Fast Ethernet 100BASE-T con las características antes mencionadas en el numeral 2.3.4. La subred se concentra en el rack de comunicaciones principal ubicado en la planta baja del edificio de la Facultad de Ciencias Agrarias. Donde se ubica un switch CISCO de la Serie 2960, con características de tipo Administrable.

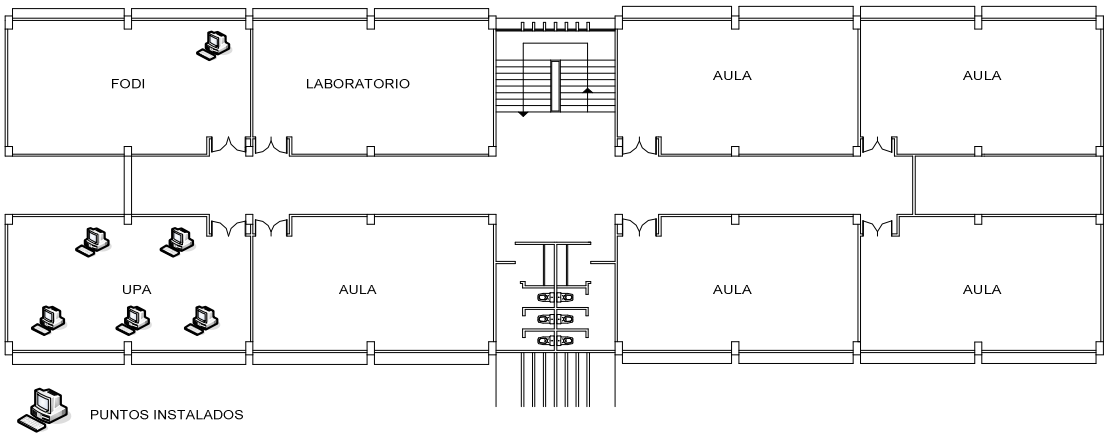


Figura 2.28 Puntos de red activos en el segundo piso de la Facultad de Ciencias Agrarias

PUNTOS ACTIVOS	
DIRECCIÓN IP	**UBICACIÓN**
175.100.50.175	UPA
175.100.50.176	UPA – DIRECTOR
175.100.50.177	UPA
175.100.50.178	UPA
175.100.50.198	UPA
192.168.1.248	FODI

Tabla 2.20 Direcciones IP de los Puntos Activos de Figura 2.28

En el **tercer piso** se encuentra una subred de 9 puntos de red activos destinados a la UED (Unidad de Educación a Distancia), UPA (Unidad de Planeación Académica) y a la Procuraduría. Esta es una subred en estrella con las características Fast Ethernet antes mencionadas en el numeral 2.3.4. La subred se concentra en el rack de comunicaciones principal ubicado en la UPA. Donde se encuentra un switch CISCO Catalyst de la Serie 2960 administrable.

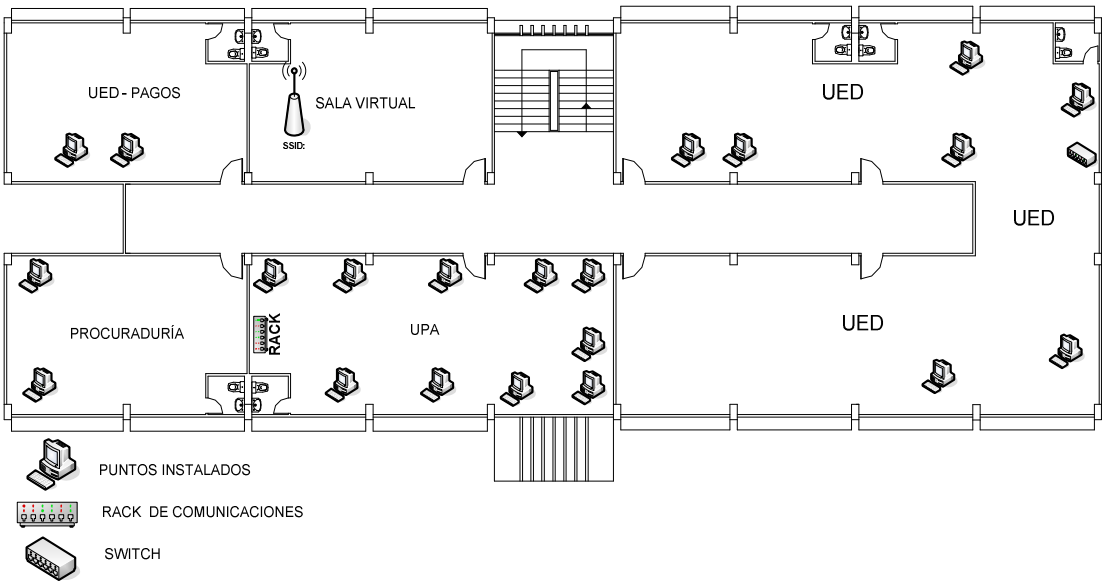


Figura 2.29 Puntos de red activos en el tercer piso de la Facultad de Ciencias Agrarias

PUNTOS ACTIVOS	
DIRECCIÓN IP	**UBICACIÓN**
175.100.50.132	PROCURADURÍA
175.100.50.133	PROCURADURÍA - ASISTENTE
175.100.50.179	UED - DIGITADORA
175.100.50.180	UED - SECRETARIA
175.100.50.181	UED - SECRETARIA
175.100.50.182	UED - PAGOS
175.100.50.199	UED - ASISTENTE
175.100.50.200	UED – DIRECTOR
192.168.1.234	UED – COM. EVALUACIÓN

Tabla 2.21 Direcciones IP de los Puntos Activos de Figura 2.29

En la **planta baja** se tiene de puntos de red activos destinados a la Biblioteca, Secretaría y Subdecanato. Existen 2 redes inalámbricas, la primera en la biblioteca y con acceso para los docentes previa configuración de sus equipos portátiles. La segunda red inalámbrica con acceso para los directores de las escuelas y los docentes que tengan la cobertura de la red. La biblioteca también cuenta con puntos activos de la red cableada para el servicio de los estudiantes.

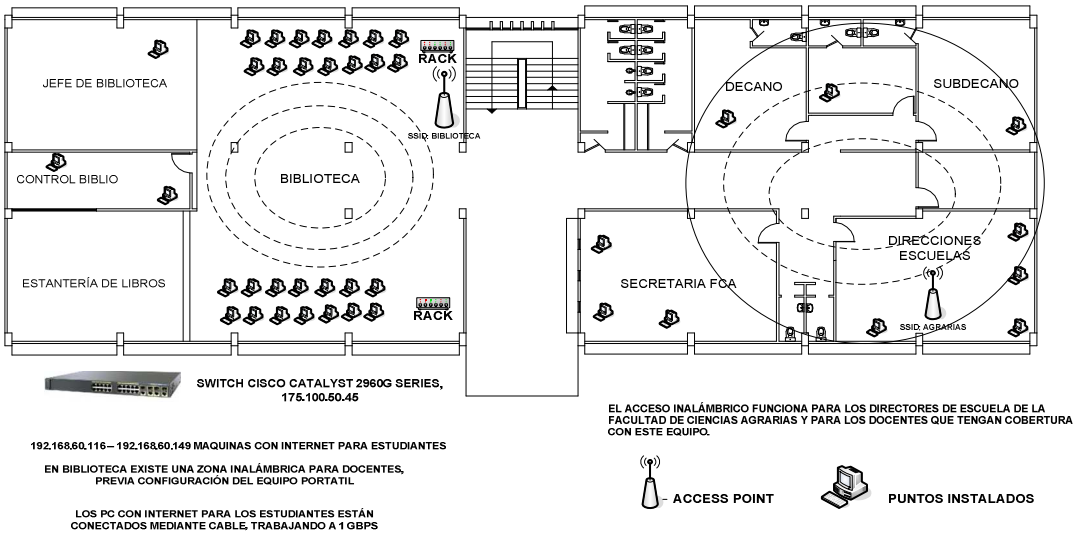


Figura 2.30 Puntos de red activos en la planta baja de la Facultad de Ciencias Agrarias

PUNTOS ACTIVOS	
DIRECCIÓN IP	**UBICACIÓN**
175.100.50.99	BIBLIOTECA
175.100.50.158	BIBLIOTECA - JEFE
175.100.50.160	SUBDECANO
175.100.50.163	SECRETARIA
175.100.50.164	SECRETARIA - ABOGADO
175.100.50.236	SECRETARIA

Tabla 2.22 Direcciones IP de los Puntos Activos de Figura 2.30

La subred se concentra en el rack de comunicaciones principal ubicado en la biblioteca. Donde se tiene un switch CISCO Catalyst de la Serie 2960 administrable.

2.3.9. SUBRED LAN FAST ETHERNET DE POSTGRADO

Esta subred se compone de 24 puntos activos, los cuales se distribuyen de la siguiente manera: 1 para el acceso inalámbrico 16 puntos para la sala de cómputo, 1 punto para bodega, 1 para Adquisiciones, 1 para la Secretaria de Postgrado y 1 para el Director de posgrado y finalmente 3 para la coordinación de maestría. Es una red Fast Ethernet 100 BASE-T con las características antes mencionadas en el numeral 2.3.4. La topología en estrella tiene su núcleo principal en un switch CISCO de la serie 2960 administrable, que se ubica en un rack de comunicaciones principales.

La red inalámbrica es utilizada por personal administrativo previa configuración de sus equipos portátiles.

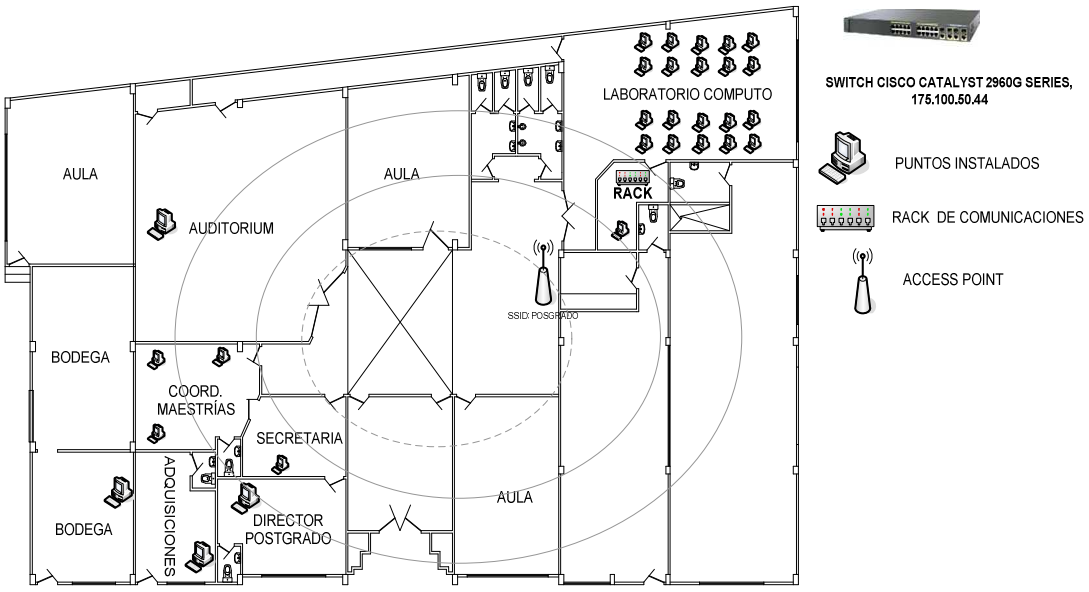


Figura 2.31 Puntos de red activos de la subred del Departamento de Postgrado

PUNTOS ACTIVOS	
DIRECCIÓN IP	**UBICACIÓN**
175.100.50.135	BODEGA
175.100.50.136	ADQUISICIONES

175.100.50.137	DIRECTOR POSTGRADO
175.100.50.138	SECRETARIA POSTRADO
175.100.50.139	COOR. MAESTRÍA
175.100.50.140	COOR. MAESTRÍA
175.100.50.141	COOR. MAESTRÍA
175.100.50.142 – 175.100.50.157	LABORATORIO DE COMPUTO

Tabla 2.23 Direcciones IP de los Puntos Activos de Figura 2.31

2.3.10. SUBRED LAN FAST ETHERNET DE RECTORADO

Esta subred se compone de puntos destinados al Rectorado, las secretarias del rectorado, Vicerrectorado, secretaria de vicerrectorado y Abogado Secretario. Además de tener un punto activo para el lector biométrico por cuestiones de identificación. Esta subred Fast Ethernet con características antes mencionada en el numeral 2.3.4. La subred se concentra en el rack de comunicaciones principal ubicado en la secretaria del Abogado, como se muestra en el gráfico 2.32, donde se encuentra un switch CISCO Catalyst de la Serie 2960, con características de tipo Administrable. También tienen una red inalámbrica que da cobertura a este departamento, previa configuración de los equipos portátiles del personal administrativo.

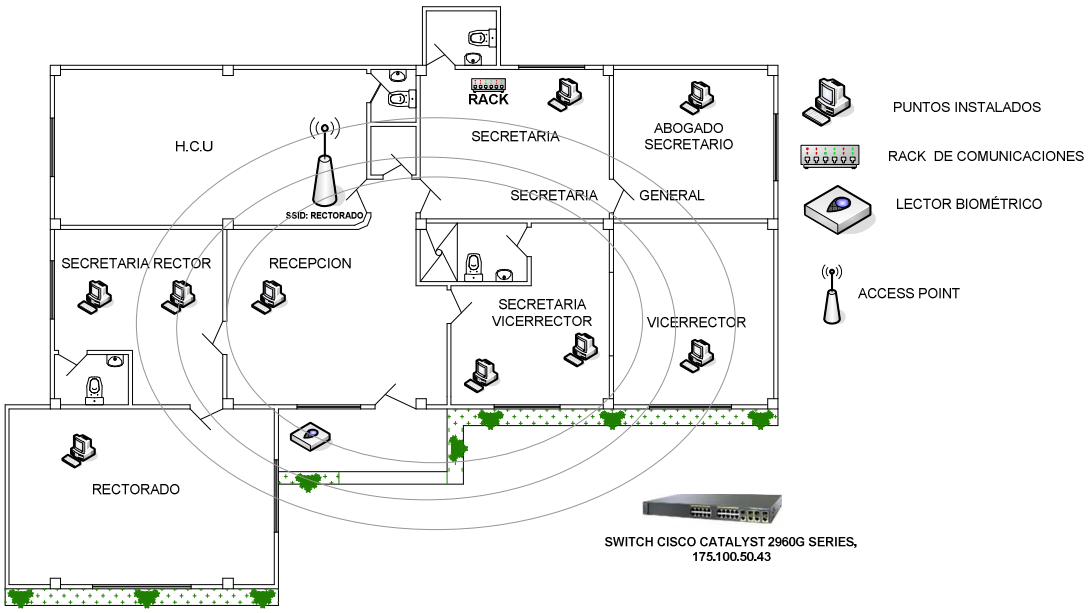


Figura 2.32 Puntos de red activos de la subred del Área de Rectorado

PUNTOS ACTIVOS	
DIRECCIÓN IP	**UBICACIÓN**
175.100.50.6	DISPOSITIVO BIOMÉTRICO
175.100.50.129	SECRETARIA RECTOR
175.100.50.130	VICERRECTOR
175.100.50.131	SECRETARIA - VICERRECTOR
175.100.50.134	ABOGADO - SECRETARIO
175.100.50.240	SECRETARIA – SECRETARÍA GENERAL
175.100.50.243	RECEPCIÓN
175.100.50.249	SECRETARIA RECTOR

Tabla 2.24 Direcciones IP de los Puntos Activos de Figura 2.32

2.3.11. SUBRED LAN FAST ETHERNET DE LA IMPRENTA

Esta red se compone de 1 solo punto activo. Es una mini – red Fast Ethernet 100 Base-T. Es full dúplex sobre cable de cobre – par trenzado. Tiene una conexión directa con un switch CISCO Catalyst de la serie 2960 administrable que se ubica en un rack de comunicaciones principal.

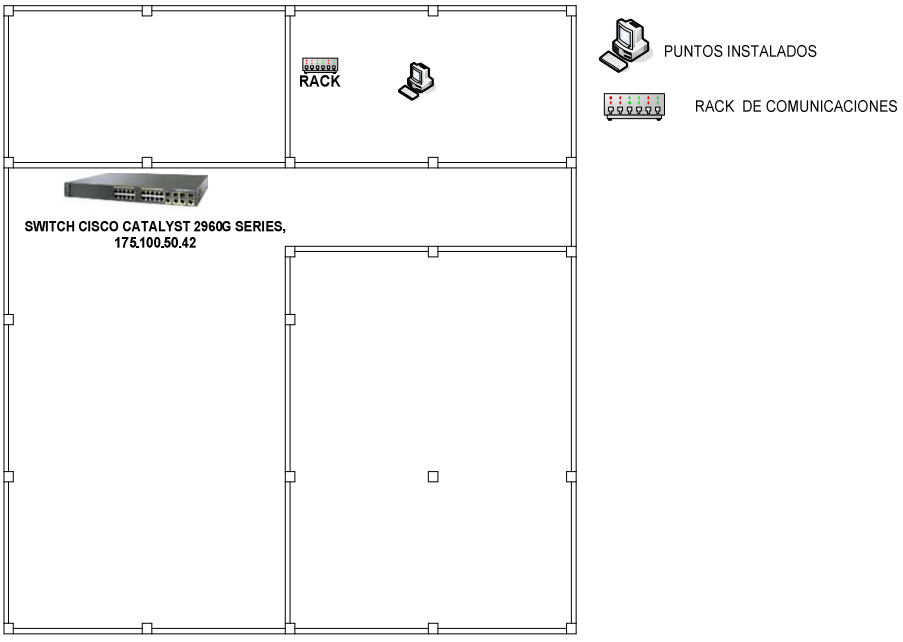


Figura 2.33 Puntos activos de la subred de la Imprenta

PUNTOS ACTIVOS	
DIRECCIÓN IP	**UBICACIÓN**
175.100.50.127	IMPRENTA

Tabla 2.25 Direcciones IP de los Puntos Activos de Figura 2.33

2.3.12. SUBRED LAN FAST ETHERNET DEL AUDITORIUM

Esta subred se compone de puntos activos destinados al Auditórium y la Dirección Administrativa. Además de tener un punto activo para el proyector del Auditórium. Esta es una LAN Ethernet 100Base-T en estrella con características antes mencionadas en el numeral 2.3.4. La subred se concentra en el rack de comunicaciones principal ubicado en la dirección administrativa, como se muestra en el gráfico 2.34. Donde se encuentra un switch CISCO Catalyst de la Serie 2960, con características de tipo administrable.

La subred también consta de un Access Point, para permitir enlaces de tipo inalámbrico a la red cableada.

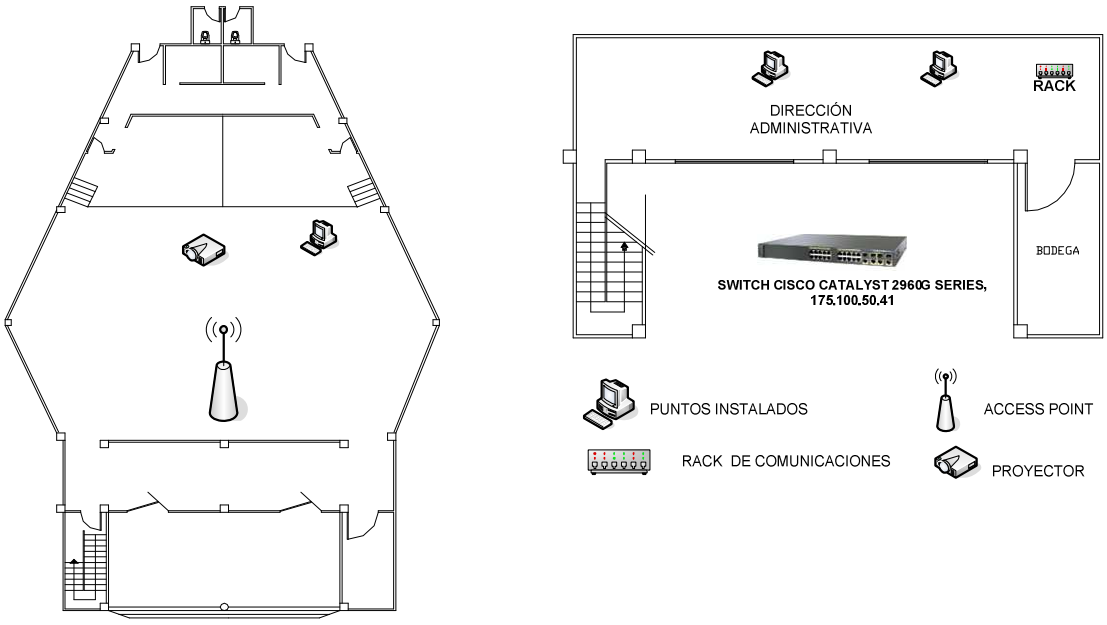


Figura 2.34 Puntos activos de la subred del Auditórium

PUNTOS ACTIVOS	
DIRECCIÓN IP	**UBICACIÓN**
175.100.50.121	DIRECCIÓN ADMINISTRATIVA - DIRECTOR
175.100.50.128	DIRECCIÓN ADMINISTRATIVA – ASISTENTE ADMINISTRATIVO
192.168.1.190	AUDITÓRIUM - PROYECTOR
192.168.1.191	AUDITÓRIUM – ACCESS POINT
192.168.1.192	AUDITÓRIUM – JEFE AUDIO – VIDEO

Tabla 2.26 Direcciones IP de los Puntos Activos de Figura 2.34

2.3.13. SUBRED LAN FAST ETHERNET DEL DEPARTAMENTO FINANCIERO, CEI (COMISIÓN DE EVALUACIÓN INTERNA) Y ÁREA DE PERSONAL

Esta subred se compone de 24 puntos activos de la siguiente manera: 4 para el área financiera, 1 para inventario, 5 para contabilidad, 2 para tesorería, 7 para CEI, 1 para Relaciones Internacionales, y 4 para personal. Es una red Fast Ethernet 100 Base-T, con las características antes mencionadas en el numeral 2.3.4. Tiene una topología en estrella que se concentra en un rack de comunicaciones principal donde se ubica un switch CISCO Catalyst de la Serie 2960 administrable, como se puede ver en la figura 2.35.

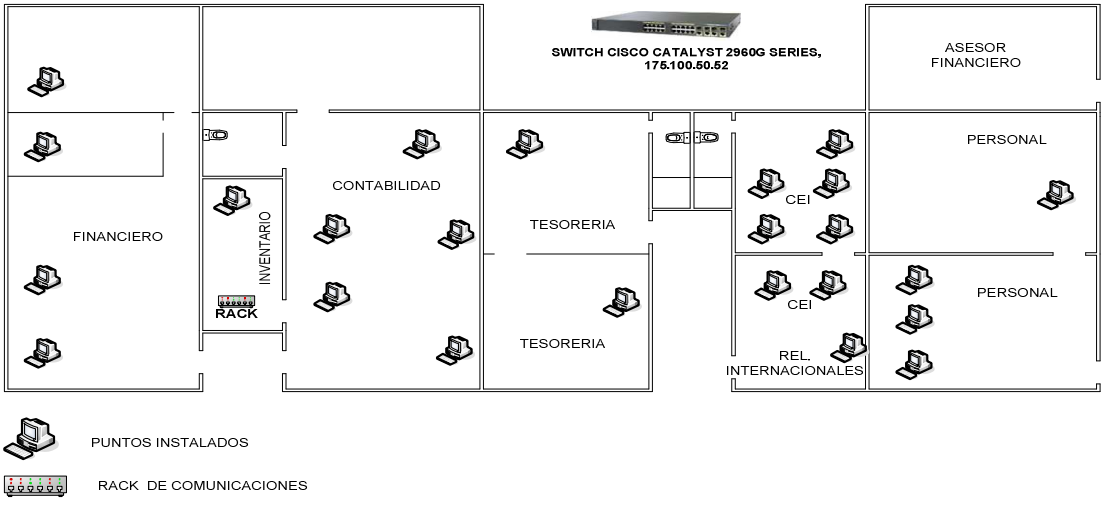


Figura 2.35 Puntos activos de la subred del Departamento Financiero, CEI (Comisión de Evaluación Interna) y Área de Personal

PUNTOS ACTIVOS	
DIRECCIÓN IP	**UBICACIÓN**
175.100.50.107	FINANCIERO - DIRECTOR
175.100.50.108	FINANCIERO - PRESUPUESTO
175.100.50.109	FINANCIERO - SECRETARIA
175.100.50.110	FINANCIERO – PRESUPUESTO
175.100.50.111	CEI
175.100.50.112	CONTABILIDAD – CONTADORA 1
175.100.50.113	CONTABILIDAD – CONTADORA 2
175.100.50.114	CONTABILIDAD – CONTADORA 3
175.100.50.115	CONTABILIDAD – CONTADORA 4
175.100.50.117	INVENTARIOS
175.100.50.119	TESORERÍA – TESORERO
175.100.50.120	TESORERÍA - RECAUDADOR
175.100.50.122	CEI
175.100.50.123	CEI
175.100.50.124	CEI
175.100.50.192	PERSONAL – ANALISTA R.H
175.100.50.193	PERSONAL – SECRETARIA
175.100.50.194	PERSONAL – JEFE
175.100.50.240	REL. INTERNACIONALES
192.168.1.241	CEI
192.168.1.242	CEI
192.168.1.243	PERSONAL – SECRETARIA
192.168.1.245	CEI

Tabla 2.27 Direcciones IP de los Puntos Activos de Figura 2.35

2.3.14. SUBRED LAN FAST ETHERNET DEL DEPARTAMENTO DE BIENESTAR UNIVERSITARIO (DBU)

Esta subred se compone de puntos de red destinados al área médica, área de encuestas y secretaría. Esta es una subred Fast Ethernet 100BASE-T con las características antes mencionadas en el numeral 2.3.4. Esta subred se concentra en el rack de comunicaciones principal ubicado en el Laboratorio de Fotogrametría del que se puede ver en la figura 2.37. Donde se encuentra un switch marca CISCO Catalyst de la Serie 2960 administrable.

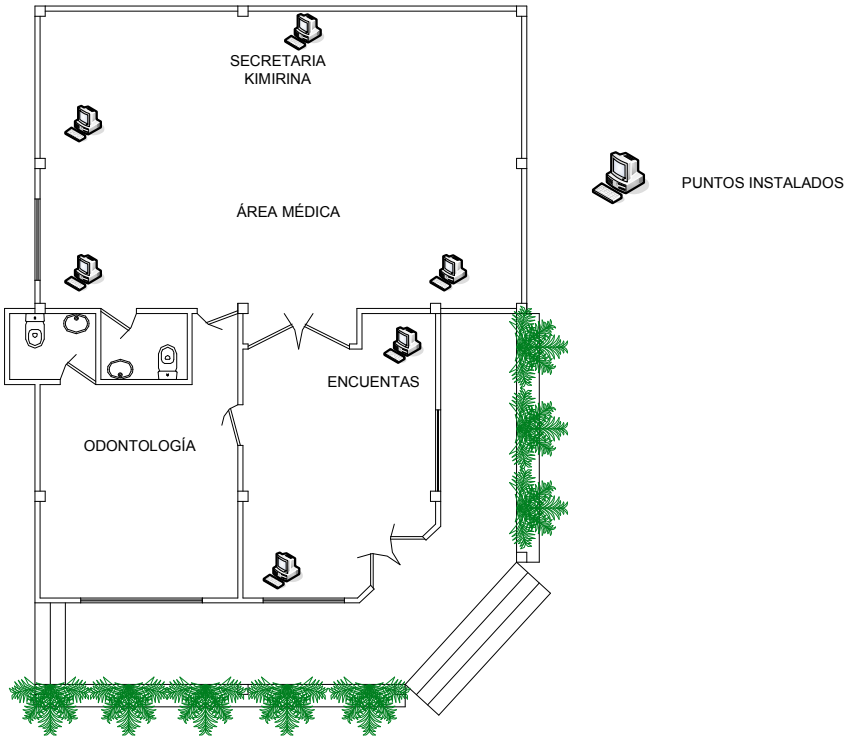


Figura 2.36 Puntos activos de la subred del Departamento de Bienestar Universitario (DBU)

PUNTOS ACTIVOS	
DIRECCIÓN IP	**UBICACIÓN**
175.100.50.98	ÁREA MÉDICA
175.100.50.105	ENCUESTAS
175.100.50.106	SECRETARIA - KIMIRINA
175.100.50.116	ÁREA MÉDICA
175.100.50.235	ÁREA MÉDICA

Tabla 2.28 Direcciones IP de los Puntos Activos de Figura 2.36

2.3.15. SUBRED LAN FAST ETHERNET DE LOS LABORATORIOS DE BIOTECNOLOGÍA Y FOTOGRAMETRÍA

Esta subred se compone de 11 puntos activos de la siguiente manera: 10 para el laboratorio de biotecnología y 1 para el laboratorio de Fotogrametría - Microbiología. Es una subred Fast Ethernet con características antes

mencionadas en el numeral 2.3.4, con topología en estrella que se concentra en un switch CISCO Catalyst de la Serie 2960 administrable, ubicado en el rack de comunicaciones principal que está en el Área del Laboratorio de Fotogrametría.

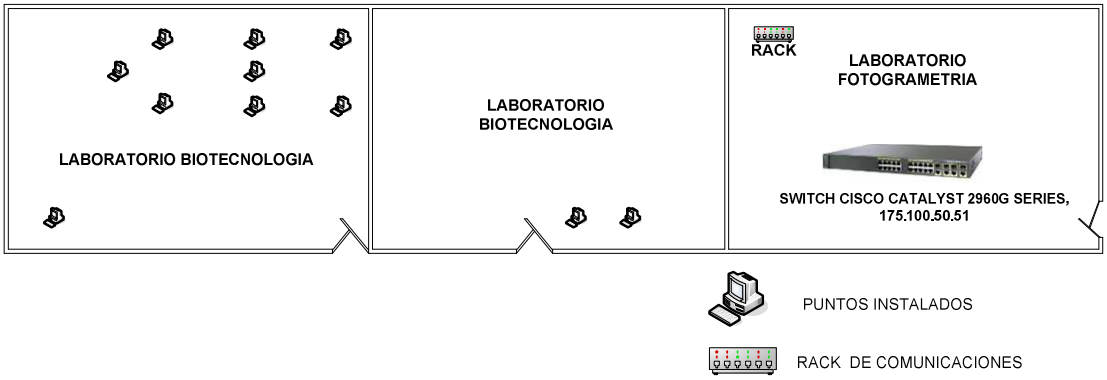


Figura 2.37 Puntos activos de la subred de los Laboratorios de Biotecnología y Fotogrametría

PUNTOS ACTIVOS	
DIRECCIÓN IP	**UBICACIÓN**
175.100.50.102	LAB. MICROBIOLOGÍA
175.100.50.103	LAB. BIOTECNOLOGÍA
175.100.50.104	LAB. BIOTECNOLOGÍA
175.100.50.231	LAB. BIOTECNOLOGÍA
175.100.50.245	LAB. BIOTECNOLOGÍA
175.100.50.246	LAB. BIOTECNOLOGÍA
175.100.50.247	LAB. BIOTECNOLOGÍA
175.100.50.248	LAB. BIOTECNOLOGÍA
175.100.50.250	LAB. BIOTECNOLOGÍA
192.168.1.254	LAB. BIOTECNOLOGÍA
192.168.0.229	LAB. BIOTECNOLOGIA

Tabla 2.29 Direcciones IP de los Puntos Activos de Figura 2.37

2.3.16. SUBRED LAN FAST ETHERNET DEL DEPARTAMENTO DE LOS LABORATORIOS BÁSICOS

Esta subred se compone de puntos de red destinados al jefe de los laboratorios básicos y del laboratorio clínico. Esta es una LAN Ethernet 100BASE-T en estrella

con características antes mencionadas en el numeral 2.3.4. La subred se concentra en el rack de comunicaciones principal ubicado en el Laboratorio de Fotogrametría que se puede ver en la figura 2.37. Donde se encuentra un Router marca CISCO Catalyst de la Serie 2960, con características de tipo administrable.

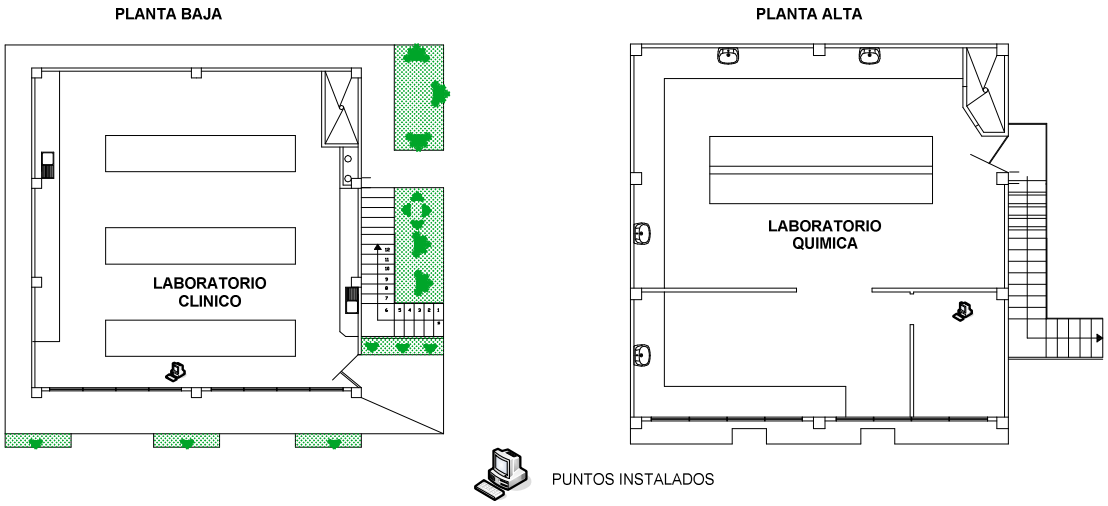


Figura 2.38. Puntos activos de la subred del Departamento de los Laboratorios Básicos

PUNTOS ACTIVOS	
DIRECCIÓN IP	**UBICACIÓN**
175.100.50.101	JEFE LABORATORIOS BÁSICOS
175.100.50.251	LABORATORIO CLÍNICO

Tabla 2.30 Direcciones IP de los Puntos Activos de Figura 2.38

2.3.17. SUBRED LAN FAST ETHERNET DEL INSTITUTO DE INFORMÁTICA

Esta subred está compuesta a su vez por las subredes de los pisos planta baja, 1, 2 y 3 del Instituto de Informática.

En la **planta baja** del Instituto se tiene 22 puntos activos, de los cuales, 1 es para el Access Point, 1 es para la Coordinación del Laboratorio de Cómputo, mientras

que las demás PCs son para los laboratorios. También se cuenta con un punto de acceso inalámbrico, para ser usado por estudiantes o personal administrativo, previa configuración de los equipos portátiles.

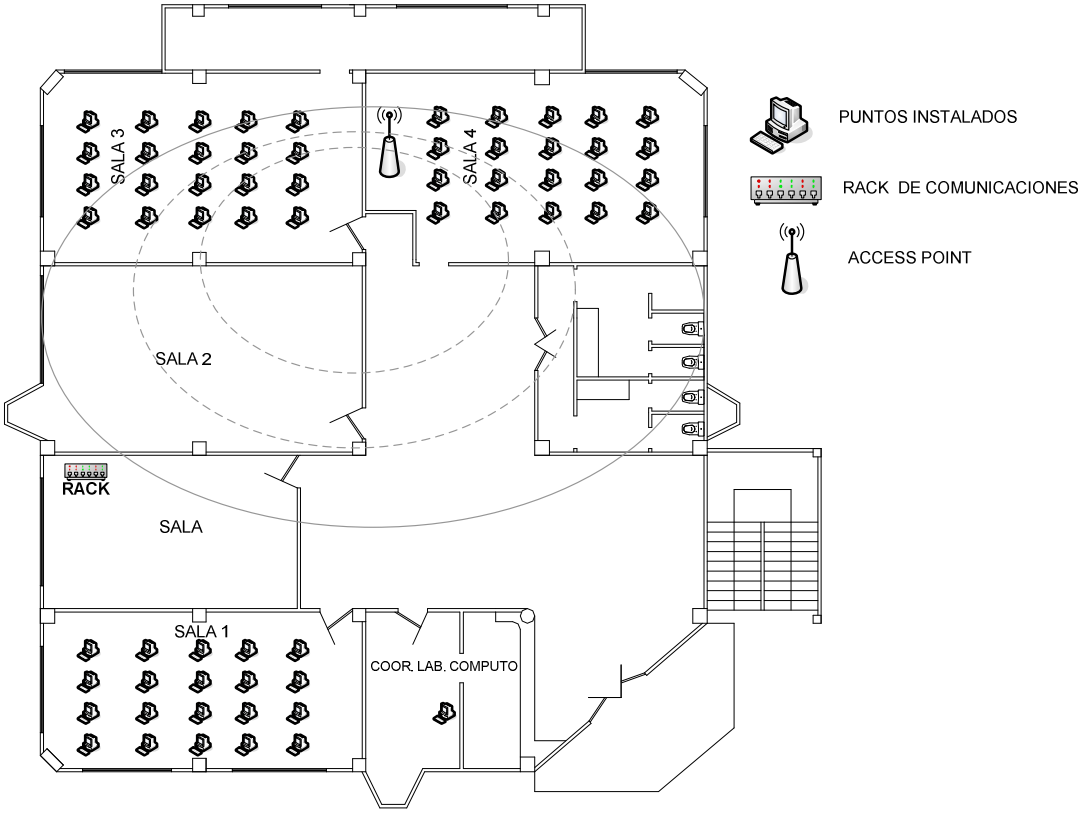


Figura 2.39 Puntos activos de la subred la Planta Baja del Instituto de Informática

PUNTOS ACTIVOS	
DIRECCIÓN IP	**UBICACIÓN**
175.100.50.67	COORD. LABORATORIO COMPUTO
196.168.60.169 – 192.168.60.189	SALA 4

Tabla 2.31 Direcciones IP de los Puntos Activos de Figura 2.39

Como se puede ver en la figura 2.39, el punto de concentración es en el rack de comunicaciones, el cual se distribuye a los pisos superiores hasta llegar al rack Principal ubicado en el Primer Piso (Figura 2.40). Esta subred es Fast Ethernet con las características antes mencionadas en el numeral 2.3.4.

En el **primer piso** es donde convergen una serie de aplicaciones tanto de intranet como de Internet, donde vamos a encontrar puntos activos que contiene servidores de datos, servidores proxy, enlaces inter – facultades y puntos para personal administrativo, así como IPs públicas para administración remota y servicios.

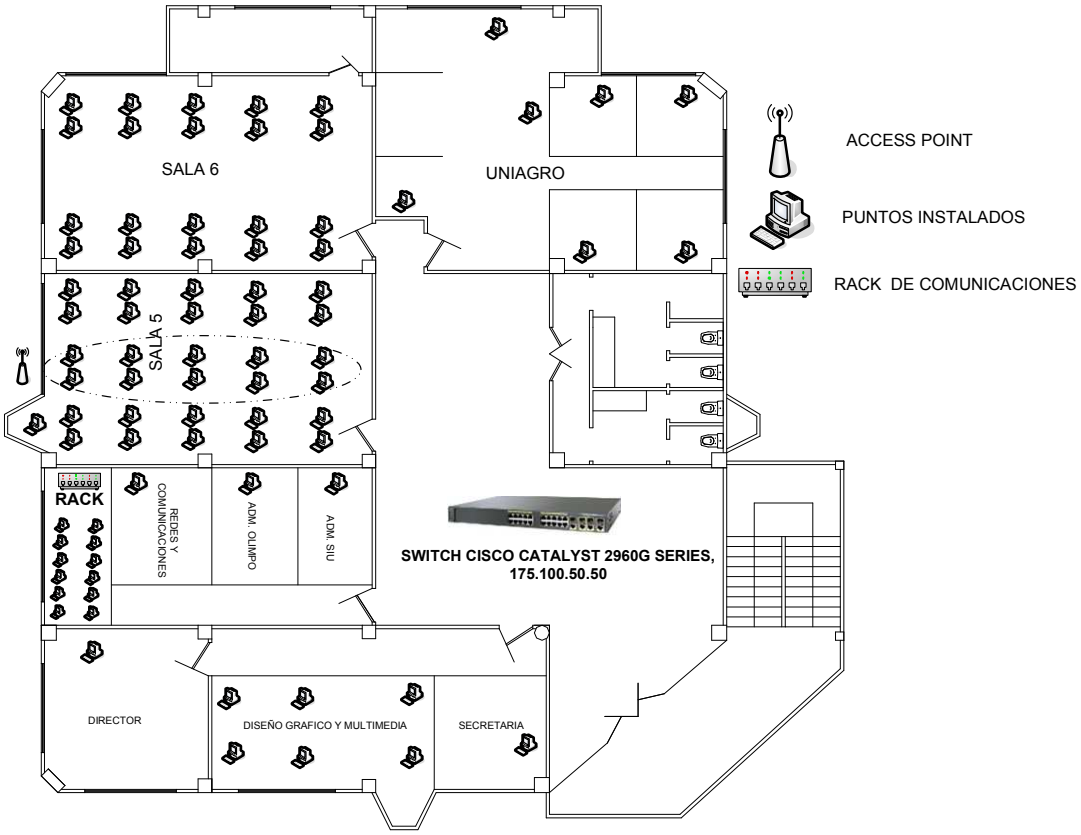


Figura 2.40 Puntos activos de la subred del Primer Piso del Instituto de Informática

PUNTOS ACTIVOS	
DIRECCIÓN IP	**UBICACIÓN**
175.100.50.1	PROXY 1
175.100.50.2	SERVIDOR WEB
175.100.50.3	SERVIDOR R.R.H.H
175.100.50.4	SERVIDOR SIU
175.100.50.5	SERVIDOR FINANCIERO
175.100.50.9	UNIAGRO – PLOTER

175.100.50.11	ENLACE CENTRAL – MARIA
175.100.50.15	DISEÑO GRAFICO Y MULTIMEDIA
175.100.50.16	REDES Y COMUNICACIONES
175.100.50.20	UNIAGRO
192.168.60.5	ACCESS POINT SALA 5
192.168.60.20 – 175.100.50.49	SALA 5 (LAB. INTERNET)
192.168.60.50	CONTROL SALA5 (LAB. INTERNET)
192.168.60.51 - 192.168.60.70	SALA 6
175.100.50.53	DISEÑO GRAFICO Y MULTIMEDIA
175.100.50.61	DIRECTOR INSTITUTO
175.100.50.62	SECRETARIA INSTITUTO
175.100.50.71	ADMINISTRADOR SIU
175.100.50.72	DISEÑO GRAFICO Y MULTIMEDIA
175.100.50.73	DISEÑO GRAFICO Y MULTIMEDIA
175.100.50.74	ADMINISTRADOR OLIMPO
175.100.50.79	DISEÑO GRAFICO Y MULTIMEDIA
175.100.50.82	PORTÁTIL INSTITUTO
175.100.50.86	UNIAGRO – DIRECTOR
175.100.50.87	UNIAGRO
175.100.50.88	DISEÑO GRAFICO Y MULTIMEDIA
175.100.50.89	UNIAGRO
175.100.50.90	UNIAGRO
175.100.50.96	UNIAGRO

Tabla 2.32 Direcciones IP de los Puntos Activos de Figura 2.40

IP PÚBLICAS	
DIRECCIÓN IP	**UBICACIÓN**
200.110.72.218	WEB - MAIL
200.110.72.227	PROXY 1
200.110.72.230	PROXY 2
200.110.72.226	PROXY DIAL -UP
200.110.72.228	EVALUACIÓN DE DOCENTES UTEQ

Tabla 2.33 Direcciones IP Públicas

Es una subred Fast Ethernet 100Base-T con las características antes mencionadas en el numeral 2.3.4. La topología en estrella de la subred se concentra en un switch CISCO Catalyst de la Serie 2960 administrable que se ubica en un rack de comunicaciones principal que se encuentra en el Cuarto de

Equipos del área de Redes y Comunicaciones en el primer piso, como se puede ver en el gráfico 2.40.

En la sala 5 se encuentra una red inalámbrica, a la cual pueden acceder estudiantes y docentes, previa configuración de sus equipos portátiles.

El **segundo piso**, tiene puntos de red activos dedicados al desarrollo de sistemas y mantenimiento.

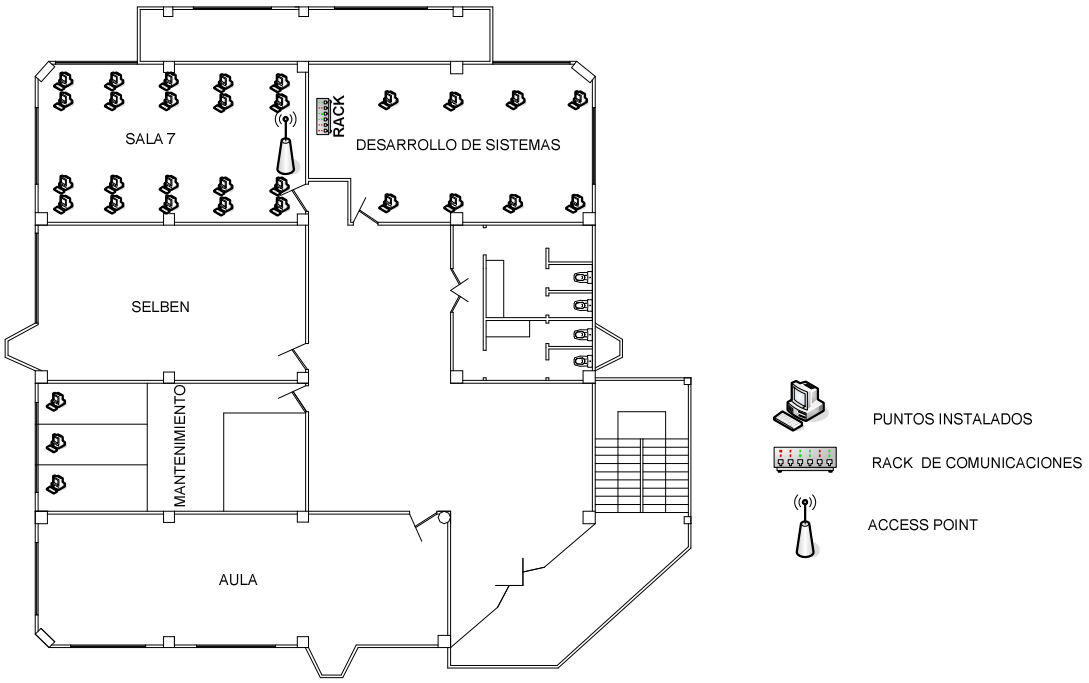


Figura 2.41 Puntos activos de la subred del Segundo Piso del Instituto de Informática

PUNTOS ACTIVOS	
DIRECCIÓN IP	**UBICACIÓN**
175.100.50.8	DESARROLLO DE SISTEMAS
175.100.50.76	COORDINADOR DESARROLLO DE SISTEMAS
175.100.50.77	DESARROLLO DE SISTEMAS
175.100.50.78	DESARROLLO DE SISTEMAS
175.100.50.91	COORDINADOR MANTENIMIENTO
175.100.50.92	MANTENIMIENTO

175.100.50.93	MANTENIMIENTO
175.100.50.94	MANTENIMIENTO (USOS VARIOS)
175.100.50.95	MANTENIMIENTO (USOS VARIOS)
192.168.1.236	COMISIÓN
192.168.1.237	COMISIÓN
192.168.1.238	COMISIÓN
192.168.60.4	ACESS POINT SALA 7
192.168.60.71 – 192.168.60.90	SALA 7

Tabla 2.34 Direcciones IP de los Puntos Activos de Figura 2.41

El **tercer piso** tiene 61 puntos activos de red, distribuidos de la siguiente manera: 20 puntos para la sala 7, 20 para la sala 8 y 20 para la sala CISCO y 1 punto para el Departamento de Relaciones Públicas.

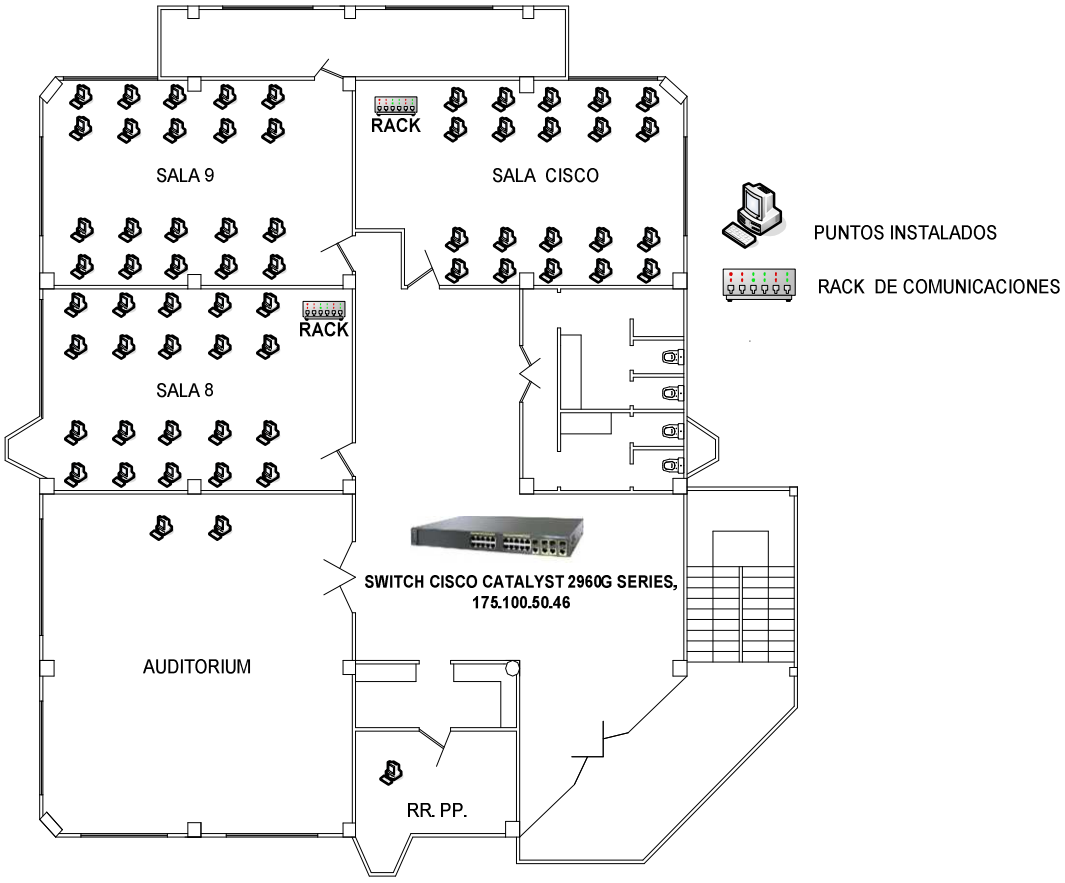


Figura 2.42 Puntos activos de la subred del Tercer Piso del Instituto de Informática

PUNTOS ACTIVOS	
DIRECCIÓN IP	**UBICACIÓN**
175.100.50.69	RELACIONES PUBLICAS
192.168.60.91 – 192.168.60.110	SALA 8
192.168.60.200 – 192.168.60.219	SALA 9
192.168.1.170 – 192.168.1.189	SALA CISCO

Tabla 2.35 Direcciones IP de los Puntos Activos de Figura 2.42

Es una subred Fast Ethernet 100Base-T con las características antes mencionadas en el numeral 2.3.4. La subred se concentra en un switch CISCO Catalyst de la Serie 2960 administrable que se ubica en un rack de comunicaciones principal ubicado en el Cuarto de Equipos del área de Redes y Comunicaciones en el primer piso.

2.3.17.1. Servidores de la red de la UTEQ

Las comunicaciones en la UTEQ están coordinadas por el Área de Redes y Comunicaciones del Instituto de Informática (Figura 2.40). En este departamento se tiene 8 servidores, uno dedicado exclusivamente para manejar el sistema OLIMPO del Departamento Financiero, otro encargado del Sistema de Información Universitaria (SIU), otro dedicado al Departamento de Recursos Humanos (RRHH).

La red tiene tres servidores Proxy: el Servidor Proxy1 dedicado a la parte estudiantil, las bibliotecas, laboratorios y la red en general, el Proxy2 dedicado a la parte administrativa y de docencia, y el Proxy Dial-Up para las conexiones Dial-Up de la red. Además, tienen el Servidor encargado del WEB y Correos Electrónicos y el Servidor dedicado exclusivamente para la Evaluación de los Docentes de la UTEQ.

Los diferentes servidores y como sus respectivas interconexiones a través de los dispositivos de red para mantener conectada a toda la red de la UTEQ se puede ver en la Figura 2.43.

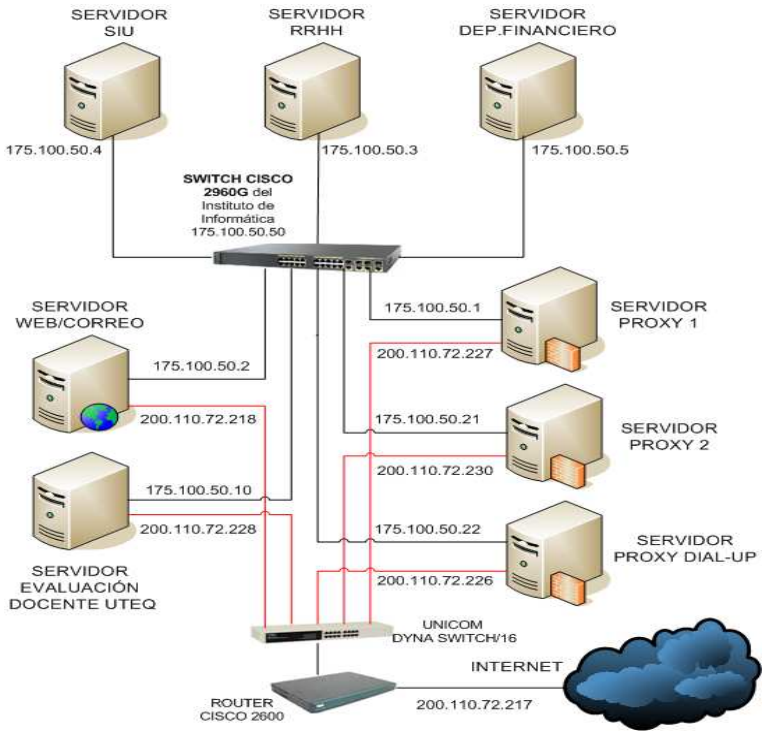


Figura 2.43 Interconexión de los Servidores de la Red de la UTEQ

Servidor	Tipo	Procesador	RAM	Disco Duro
SIU	HP Proliant ML370	Intel Xeon	512 MBytes	1 disco de 72,8 Gigas
Departamento Financiero	HP Proliant ML370	Intel Xeon	2 GBytes	2 discos de 36,46 y 149,86 GBytes
Recursos Humanos	HP Proliant ML370	Intel Xeon	2 GBytes	2 discos de 72 GBytes utilizando RAID 10
Evaluación Docente	HP Proliant ML 370GS	Intel Xeon	3,25GBytes	4 discos de 146 GBytes utilizando RAID 10
Servidor WEB / CORREO	Acer ALTOS 22000	Intel Xeon	1 GByte	3 discos de 18 GBytes
Proxy 1	CLON	Intel Core 2 DUO	2 GBytes	1 disco de 160 GBytes
Proxy 2	CLON	Intel Core 2 DUO	2 GBytes	1 disco de 160 GBytes
Proxy Dial UP	CLON	Intel Pentium 4	512 MBytes	40 GBytes

Tabla 2.36 Cuadro de características de los servidores de la UTEQ

2.3.17.2. La conexión de INTERNET en la UTEQ

La Universidad contrató el servicio de Internet con TELCONET en Enero del 2007. Actualmente cuenta con un enlace de Internet de 5Mbps, con última milla de Fibra Óptica. La Figura 2.44 muestra las interconexiones externas con el Proveedor TELCONET y como este se enlaza con la red INTERNET. Para mayores detalles sobre las conexiones externas del Proveedor referirse al ANEXO E.

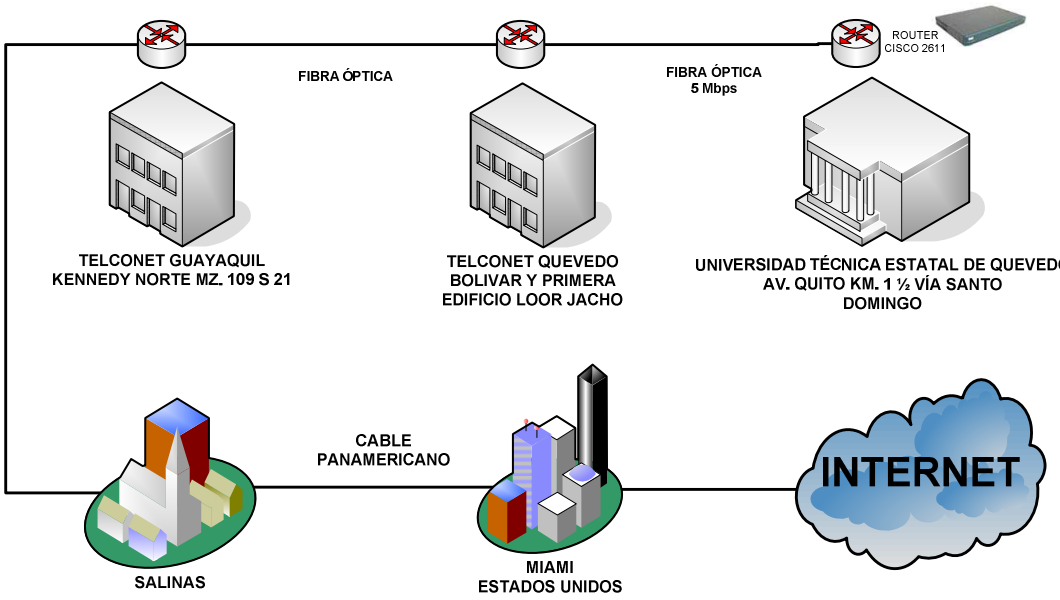


Figura 2.44 Diagrama de Conexión con Proveedor de Servicios de Internet

2.3.18. SUBRED LAN FAST ETHERNET DE FACULTAD DE CIENCIAS EMPRESARIALES

Esta red está compuesta por las subredes de los pisos planta baja, 1, y 3 de la Facultad de Ciencias Empresariales.

En la **planta baja** se tiene una subred con puntos activos destinados al Decanato, Subdecanato, secretarias, Secretario Abogado y las Direcciones de Escuelas. Esta subred al igual que el resto es Fast Ethernet con las características antes mencionadas en el numeral 2.3.4. La topología en estrella de la subred se

concentra en el rack de comunicaciones principal ubicado en la Sala del Honorable Consejo Directivo, donde se encuentra un switch marca CISCO Catalyst de la Serie 2960, con características de tipo administrable.

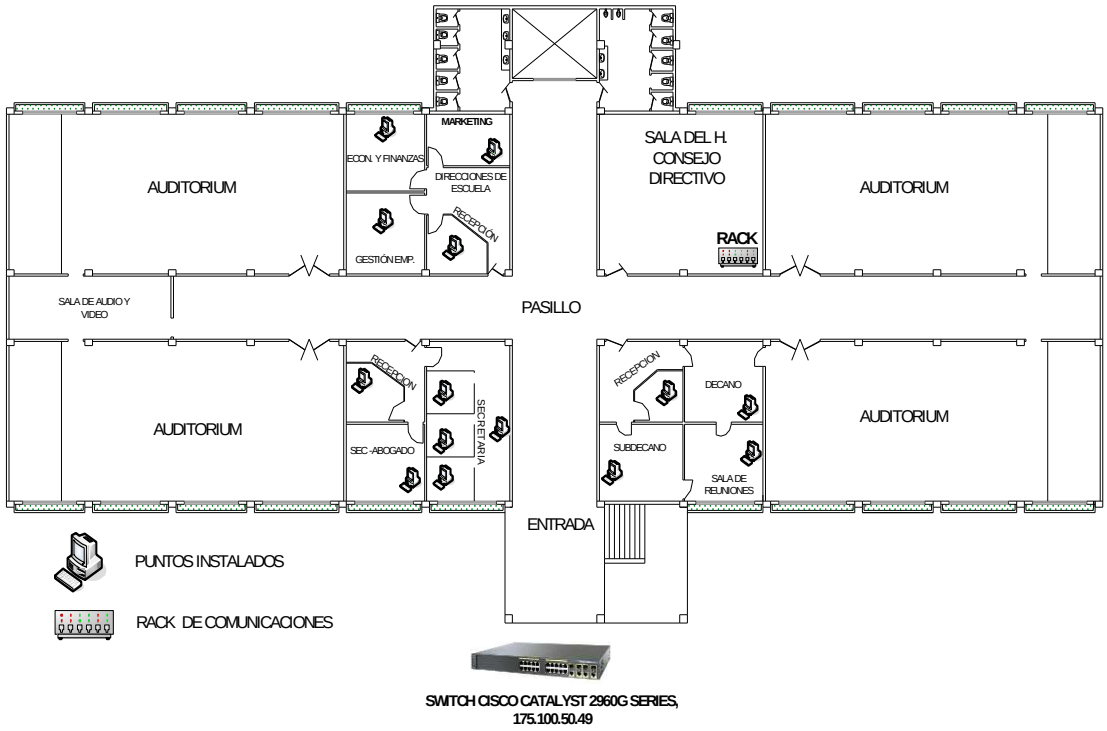


Figura 2.45 Puntos activos de la subred de la Planta Baja de la Facultad de Ciencias Empresariales

PUNTOS ACTIVOS	
DIRECCIÓN IP	**UBICACIÓN**
175.100.50.162	SECRETARIO ABOGADO
175.100.50.165	SUBDECANO
175.100.50.166	DECANATO
175.100.50.167	SECRETARIA
175.100.50.168	SECRETARIA
175.100.50.169	SECRETARIA
175.100.50.170	SECRETARIA
175.100.50.172	DIR. ESC. MARKETING
175.100.50.173	DIR. ESC. GESTION
175.100.50.174	DIR. ESC. ECON. Y FINANZAS

Tabla 2.37 Direcciones IP de los Puntos Activos de Figura 2.45

En el **primer piso** se tiene una subred con puntos activos dedicados al Director de la Escuela de Derecho, a la Secretaría de la Escuela de Derecho, al Director de la Escuela de Sistemas, al Coordinador de la Carrera de Telemática y a la Sala de Audiovisuales de la Escuela de Gestión Empresarial. Esta es una LAN Ethernet 100BASE-T en estrella implementada con las características antes mencionadas en el numeral 2.3.4.

En este piso se encuentra un enlace inalámbrico para comunicar a la oficina del Director de Sistemas con la oficina de la Escuela de Derecho. La red inalámbrica se integra a la red cableada a través de 2 switches. Los switches de este piso a su vez se concentran en el rack de comunicaciones principal ubicado en la planta baja en la Sala del Honorable Consejo Directivo, donde se encuentra un switch CISCO Catalyst de la Serie 2960, de tipo administrable.

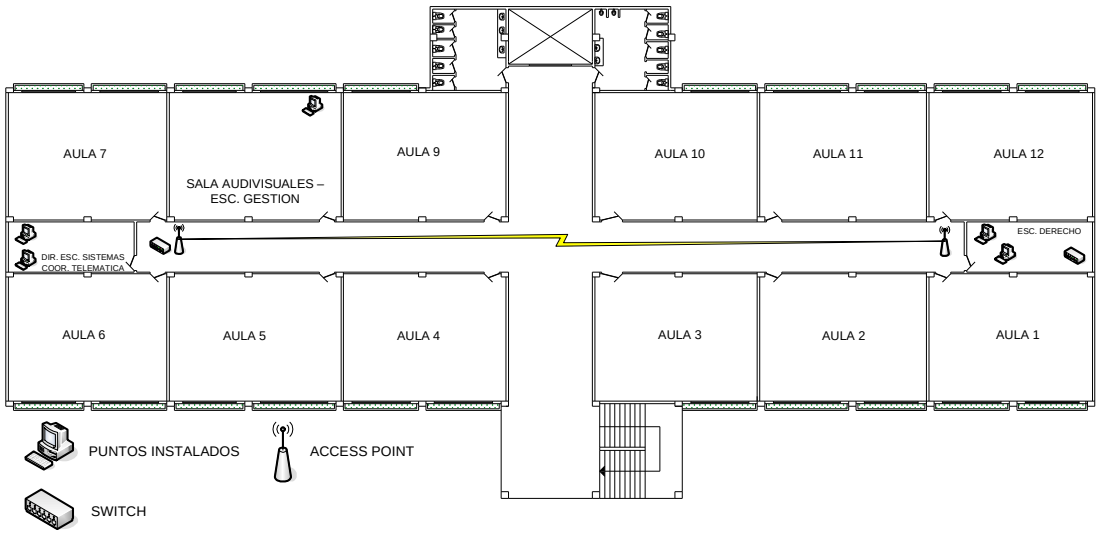


Figura 2.46 Puntos activos de la subred del Primer Piso de la Facultad de Ciencias Empresariales

PUNTOS ACTIVOS	
DIRECCIÓN IP	**UBICACIÓN**
175.100.50.17	ACCESS POINT
175.100.50.18	ACCESS POINT
175.100.50.60	SEC. ESC. DERECHO

175.100.50.63	DIR. ESC. SISTEMAS
175.100.50.66	CORD. CARRERA TELEMÁTICA
175.100.50.161	DIR. ESCUELA DERECHO
175.100.50.171	SALA. AUDIOVISUAL GESTIÓN EMPRESARIAL

Tabla 2.38 Direcciones IP de los Puntos Activos de Figura 2.46

En el **tercer piso** se encuentra la subred compuesta por 3 puntos activos destinados a la Comisión de Investigación de la Facultad de Ciencias Empresariales. Esta es una subred Fast Ethernet 100Base-T en estrella con las características antes mencionadas en el numeral 2.3.4. La subred se concentra en un primer switch, el mismo que luego se conecta en el rack de comunicaciones principal ubicado en la planta baja en la Sala del Honorable Consejo Directivo de la Figura 2.45.

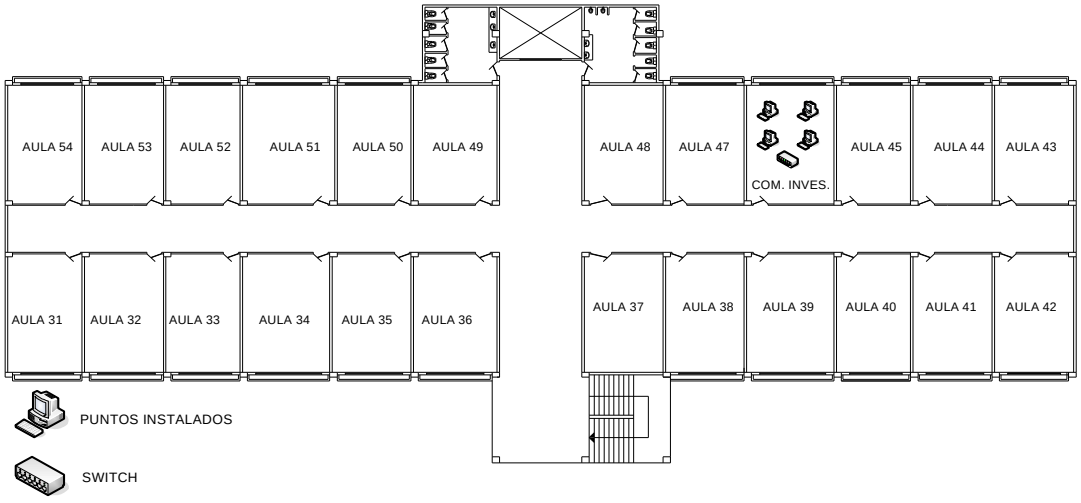


Figura 2.47 Puntos activos de la subred del Tercer Piso de la Facultad de Ciencias Empresariales

PUNTOS ACTIVOS	
DIRECCIÓN IP	**UBICACIÓN**
175.100.50.81	COM. INVESTIGACIÓN FAC.CC. EMPRESARIALES
175.100.50.159	COM. INVESTIGACIÓN FAC.CC. EMPRESARIALES
175.100.50.219	COM. INVESTIGACIÓN FAC.CC. EMPRESARIALES

Tabla 2.39 Direcciones IP de los Puntos Activos de Figura 2.47

2.4. GESTIÓN ACTUAL DE LA RED DE DATOS DE LA UTEQ

La gestión de red que se realiza sobre la red de la UTEQ, es muy básica, y no existe actualmente ningún modelo de gestión desarrollado para ser implementado en la red.

La gestión actualmente solo se la hace a la subred del Departamento Financiero de la UTEQ y sobre el Internet.

Para la gestión, utilizan el software SQUINT, que en realidad es un servidor Proxy y un "*web cache daemon*".

SQUINT es un Proxy analizador de logs, que genera un detallado reporte acerca de quién está haciendo uso del mayor tiempo y recursos accediendo al Internet, para ser entregados a las autoridades y clientes en caso de ser solicitados.

El software revela los usuarios que están abusando de la red en términos de transferencia de datos, número de archivos transmitidos, y el tiempo en línea.

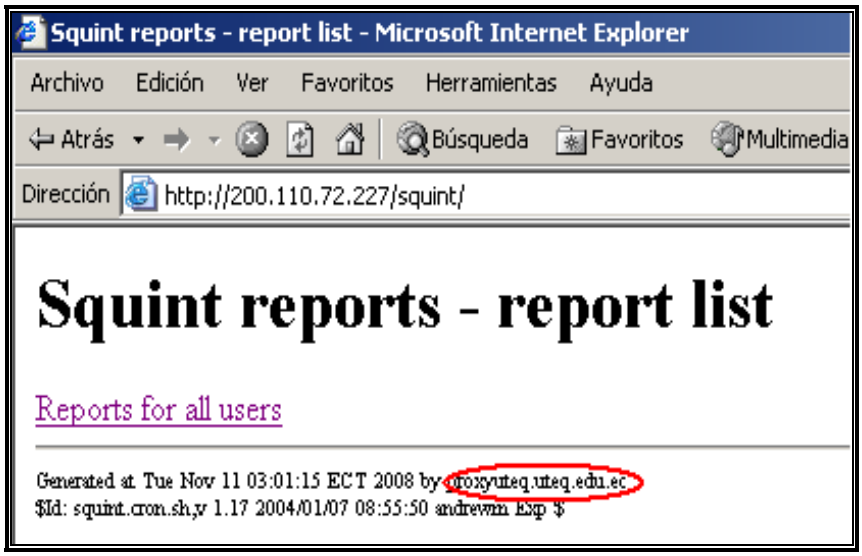
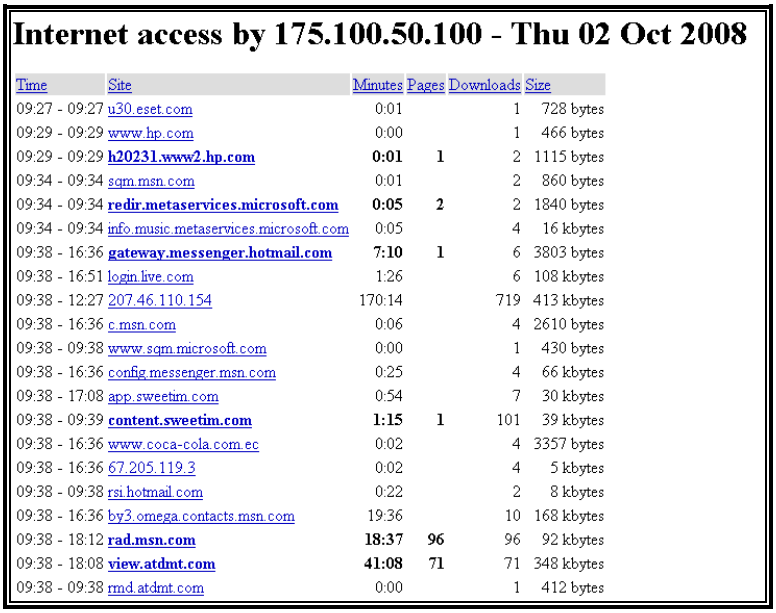


Figura 2.48 Pantalla principal del Software Squint



Internet access by 175.100.50.100 - Thu 02 Oct 2008

Time	Site	Minutes	Pages	Downloads	Size
09:27 - 09:27	u30.eset.com	0:01		1	728 bytes
09:29 - 09:29	www.hp.com	0:00		1	466 bytes
09:29 - 09:29	**h20231.www2.hp.com**	**0:01**	**1**	2	1115 bytes
09:34 - 09:34	sqm.msn.com	0:01		2	860 bytes
09:34 - 09:34	**redir.metaservices.microsoft.com**	**0:05**	**2**	2	1840 bytes
09:34 - 09:34	info.music.metaservices.microsoft.com	0:05		4	16 kbytes
09:38 - 16:36	**gateway.messenger.hotmail.com**	**7:10**	**1**	6	3803 bytes
09:38 - 16:51	login.live.com	1:26		6	108 kbytes
09:38 - 12:27	207.46.110.154	170:14		719	413 kbytes
09:38 - 16:36	c.msn.com	0:06		4	2610 bytes
09:38 - 09:38	www.sqm.microsoft.com	0:00		1	430 bytes
09:38 - 16:36	config.messenger.msn.com	0:25		4	66 kbytes
09:38 - 17:08	app.sweetim.com	0:54		7	30 kbytes
09:38 - 09:39	**content.sweetim.com**	**1:15**	**1**	101	39 kbytes
09:38 - 16:36	www.coca-cola.com.ec	0:02		4	3357 bytes
09:38 - 16:36	67.205.119.3	0:02		4	5 kbytes
09:38 - 09:38	rsi.hotmail.com	0:22		2	8 kbytes
09:38 - 16:36	by3.omega.contacts.msn.com	19:36		10	168 kbytes
09:38 - 18:12	**rad.msn.com**	**18:37**	**96**	96	92 kbytes
09:38 - 18:08	**view.atdmt.com**	**41:08**	**71**	71	348 kbytes
09:38 - 09:38	rmd.atdmt.com	0:00		1	412 bytes

Figura 2.49 Ejemplo de la información generada por el Software Squint

La gestión de los equipos del backbone, como los switches CISCO de la Serie 2960, se la realiza, vía web, con interfaces gráficas propietarias.

2.5. SISTEMA DE SEGURIDAD ACTUAL DE LA UTEQ

Actualmente, las seguridades informáticas de la Universidad están dirigidas a proteger la información del SIU (Sistema de Información Universitaria) que contiene los records académicos de todos los estudiantes y el del Sistema OLIMPO que maneja todo lo referente al área financiera y contable de la UTEQ.

La institución cuenta con las seguridades básicas incorporadas que proporcionan los equipos de red. Posee un firewall básico de software para controlar el acceso a la red. Con este firewall se impide que los intrusos de Internet tengan acceso a los datos de la red privada. Y además permite controlar a los empleados que tienen acceso fuera de la red.

También cabe mencionar que el direccionamiento en gran parte es estático. Además, que las claves de los diferentes sistemas que se manejan en la UTEQ

se encriptan a través de cifrados monoalfabéticos (cifrado CESAR[11]), pero para la transmisión de datos actualmente no se utiliza ningún algoritmo de encriptación.

2.6. MONITOREO DE TRÁFICO DE LA RED DE DATOS DE LA UTEQ

En una red de datos, el mayor problema que se puede ocasionar es una saturación parcial o total del canal de comunicación, donde, tendremos problemas de descarte de paquetes, lentitud en la entrega, encolamiento en los dispositivos periféricos de red y por ende una confiabilidad baja de la red de datos.

El mayor inconveniente se genera donde el canal es más estrecho para el paso de información y generalmente en la mayoría de empresas, estos se localizan en las redes de datos WAN y en la conexión a Internet, esto debido a la infraestructura misma de los proveedores de estas tecnologías y los costos que originan los enlaces.

Por tal motivo y al realizar una evaluación de los equipos y encontrar que los mismos no están saturados, nos enfocamos en el canal de Internet del proveedor TELCONET, realizando un monitoreo de 24 horas por 7 días laborables. Este monitoreo, está detallado en el ANEXO F.

Como análisis, se encontró que el canal de 5 Mbps en un 90% no pasa saturado, mientras que se generan picos periódicos aproximadamente a las 6:00 AM, 8:30 AM, de 10:30 a 11:30, 12:20 pm y a las 17:10. Estos picos no son permanentes y generalmente se producen al momento de prender y actualizar los sistemas. Solo en el rango descrito, se tiene una saturación mayor pero esto debido a que en este horario, se tiene el mayor número de computadores conectados y la mayoría de ellos, se conectan a Internet.

[11] Es un cifrado por desplazamiento, en el que una letra en el texto original es reemplazada por otra letra que se encuentra en una posición que está un número determinado de espacios más adelante en el alfabeto. En caso del alfabeto español, pueden ser hasta 26 posiciones.

Como conclusión, la red no está saturada, tiene una amplia gama de expansión y el canal de Internet es lo suficientemente grande como satisfacer las actuales conexiones sin implicar, que el sistema se vuelva lento con la ampliación de la red de datos actual. Esta saturación descrita, no implicará problemas en la expansión o aumento del número de computadores, pero hay que estar alerta, si el rango descrito aumenta tanto en periodicidad como en el rango del tiempo que permanece el canal saturado.

2.7. COMUNICACIONES DE VOZ EN LA UTEQ

La universidad cuenta con una PBX marca *Definity* para realizar las conexiones telefónicas entre los distintos departamentos de la UTEQ, con capacidad para 95 anexos. Pero este dispositivo no satisface todas las necesidades de comunicaciones, existen áreas que no poseen extensiones, tienen números convencionales, e incluso otras donde no se tiene teléfonos. La falta de comunicación provoca que el personal en ciertas ocasiones deba movilizarse para realizar alguna gestión, lo que provoca una pérdida de tiempo.

2.8. SOFTWARE Y APLICACIONES UTILIZADAS EN LA RED DE DATOS DE LA UTEQ

Las computadoras de la mayoría de usuarios de la red utilizan el Sistema Operativo Windows XP.

En lo que se refiere a los servidores de la red, estos tienen instalados los siguientes sistemas operativos: Windows Server 2003 en el Servidor del SIU, en el de RRHH y el de Evaluación a Docentes. El servidor del área Financiera tiene instalado Windows Server 2000. Los servidores Proxy 1 y 2 trabajan con el sistema operativo Linux Fedora 8 y finalmente, los servidores del Proxy dedicado a Dial-Up y el servidor para el Web/Mail con Linux Red Hat 9.

Los usuarios de la red de la UTEQ, también tienen instalados en sus equipos el software Zone Alarm Pro para que ellos puedan determinar a los usuarios que puedan tener acceso a la información compartida de cada uno.

En el departamento Financiero utilizan un sistema OLIMPO, el cual es una plataforma que permite desarrollar aplicaciones personalizadas para el área financiera y de contabilidad.

2.9. DIAGNÓSTICO DE LA RED DE DATOS DE LA UTEQ

De la información antes presentada sobre la situación de la red, se ha obtenido el siguiente diagnóstico:

- Los equipos de conmutación cuentan con las capacidades adecuadas para manejar el tráfico de información de la red.
- Actualmente, no se cuenta con un equipo específico dedicado exclusivamente para el manejo de las seguridades de la red.
- No se disponen de adecuadas políticas de administración y seguridad.
- Solo se dispone de las herramientas estándares que vienen incluidas en los equipos de red para su administración y monitoreo.
- No se cuenta con un software especializado para la gestión y administración global de la red de datos.
- Falta mayor automatización de los procesos de la red, como en la asignación de IPs.
- Ausencia de un software de antivirus corporativo.
- No se cuenta con un sistema de comunicaciones de voz adecuado que soporte a todas las oficinas del personal administrativo.

2.10. REQUERIMIENTOS DE LA RED DE DATOS DE LA UTEQ

Del diagnóstico realizado al analizar la información recopilada sobre la infraestructura tecnológica de la UTEQ, se tiene que los requerimientos de la red universitaria son:

- Desarrollar políticas de administración y seguridad para la red de datos de la UTEQ.
- Contar con un equipo dedicado exclusivamente para la seguridad de la red.
- Implementar herramientas para la gestión y monitoreo de la red, adicionales a las que vienen por defecto en los equipos.
- Contar con un sistema completo de administración de red especializada para el manejo global de la red de datos de la UTEQ.
- Conseguir una mayor automatización en los procesos de la red.
- Instalar un antivirus corporativo.
- Implementar un mecanismo de comunicación de voz más eficiente para el personal administrativo de la universidad.
- Mejorar las comunicaciones entre los diferentes campus que posee la universidad.
- Mejorar el acceso a la intranet y a Internet a los estudiantes dentro de los diferentes campus.
- Definir un método de uso de reportes, así como su esquema y su forma de administrarlo.
- Tener información suficiente sobre el rendimiento de todos los equipos de la red, para poder verificar equipos sobre utilizados, subutilizados, enlaces saturados y enlaces caídos.
- Llevar una contabilidad de toda la red de la UTEQ para controlar todo acto indebido que atente contra las políticas establecidas y así preservar la confiabilidad de la red.

BIBLIOGRAFÍA DEL CAPÍTULO II

[1] Tríptico sobre el departamento UNIAGRO, UTEQ 2008.

CAPÍTULO III
DESARROLLO DEL MODELO DE GESTIÓN Y ADMINISTRACIÓN DE RED

3.1 INTRODUCCIÓN

El uso de la tecnología ha sido muy grande y continúa creciendo, en especial dentro del campo de la investigación y educación. La necesidad de las instituciones por mayores anchos de banda y mejores formas de acceso a los recursos IT (*Information Tecnologhy*) es indispensable. Además, la globalización del uso de las tecnologías en especial del Internet, ha hecho que las instituciones educativas, como la UTEQ se vea inmersa en ambientes agresivos donde el saboteo de la información se ha vuelto algo común. De ahí la importancia de que la Intranet Universitaria sea más segura y gestione de mejor manera sus recursos de red y esté preparada para acoger y solventar estas necesidades, de tal forma que ofrezca una satisfactoria experiencia con sus servicios a los usuarios de la red.

Como se ha podido observar en capítulos anteriores, el manejo de la infraestructura actual de la universidad no es suficiente para satisfacer las demandas de los usuarios. Por eso, es necesario establecer ciertos parámetros que permitirán al administrador de la red solventar estas demandas.

Estos parámetros se los establecerá en las Políticas de Seguridad y Administración propuestas por este trabajo, las cuales deben ser reflejadas mediante la configuración, monitoreo y administración de los recursos IT, que se detallan dentro de las diferentes capas del Modelo de Gestión de Red escogido.

La estructura interna típica de un Intranet se puede separar lógicamente en dos zonas importantes, una zona dedicada a los servicios y otra dedicada a la administración. La zona dedicada a los servicios es la más frágil desde el punto de vista de la seguridad, puesto que está expuesta a todos los usuarios de la

Internet que quieran acceder o utilizan un servicio determinado. En cambio, la zona de administración debe ser la más protegida, para no recibir ataques. Y también, es precisamente esta zona de administración la que acogerá el modelo que se desarrolla en el presente capítulo.

3.2 OBJETIVOS DEL DESARROLLO DEL MODELO DE GESTIÓN

3.2.1 OBJETIVOS GENERALES

- Brindar las pautas para implementar un modelo de gestión y administración que satisfaga los requerimientos expuestos en el capítulo anterior.
- Incrementar las seguridades físicas y lógicas dentro de la red de la universidad.
- Crear las condiciones para poder gestionar el crecimiento de la red de datos de la UTEQ.

3.2.2 OBJETIVOS ESPECÍFICOS

- Asegurar que los usuarios de la red reciban los servicios de la intranet con niveles de calidad de servicio aceptables internacionalmente.
- Ayudar al administrador de la red a enfrentar las complejidades de la red y asegurar que la información se mueva a través de ella con la máxima eficiencia y transparencia para los usuarios.
- Mejorar la disponibilidad de la red.
- Mejorar el rendimiento de la red.
- Ofrecer mayor flexibilidad y escalabilidad en el manejo de la red.
- Tener una administración global de la red.
- Dar mayor automatización a la red.
- Mejorar las comunicaciones de voz, y la calidad de los servicios ofrecidos sobre la red de la universidad.
- Controlar los costes de ancho de banda de tráfico de internet sobre la red.

Todos los objetivos mencionados anteriormente, se pretenden cumplir mediante el desarrollo del sistema de gestión y administración de la red que se desarrollará en este capítulo.

3.3 POLÍTICAS DE SEGURIDAD

Una política fundamental de seguridad nace de la amenaza latente de la exposición de la red y sus servidores a ataques desde el Internet y la Intranet, por tal motivo es necesario implementar mecanismos de seguridad para protegerlos, tales como normas de seguridad internas y externas para los empleados y usuarios; así también la instalación de equipos de seguridad para prevenir ataques desde el exterior de la red.

Considerando que la Intranet Universitaria es susceptible a ataques desde el interior, así como desde el exterior de la misma, entonces se definirá una política interna y una política externa de seguridad dentro del Modelo de Gestión que se propondrá en el presente capítulo.

3.3.1 POLÍTICA INTERNA DE SEGURIDAD

Una red debe ser segura desde su interior, debiendo esta seguridad ser reflejada hacia el exterior, para generar mayor confianza a los usuarios que la utilizan; se considera la siguiente política interna de seguridad para la Intranet universitaria:

- Normar el acceso a los servicios e infraestructura de la red desde el interior de la Intranet; esta normalización permitirá organizar la red para evitar ataques desde el interior de la misma y garantizar la confidencialidad de la información generada internamente.

3.3.2 POLÍTICA EXTERNA DE SEGURIDAD

La mayor cantidad de datos que cursa por la infraestructura de Intranet universitaria es exterior a la misma y es generada por los usuarios. Las políticas que garantizarán la transmisión correcta de estos datos son:

- Normar un modelo que detalle cómo se ubicarán, clasificarán y denominarán los equipos de la infraestructura de red.
- Normar el acceso a la información que contiene la infraestructura de red, para garantizar la transmisión de datos generados por los usuarios que acceden a Internet a través de dicha infraestructura.
- Brindar seguridad perimetral y garantizar que la seguridad de la Intranet se extienda hacia el usuario.
- Ofrecer niveles de seguridad aceptable mediante la configuración de acceso y administración de las plataformas de servicio que posee la universidad.
- Ofrecer seguridad contra ataques que denieguen los servicios ofertados por la Intranet; normándose el uso y configuración de servicios e infraestructura.

3.4 SELECCIÓN DEL MODELO DE GESTIÓN Y ADMINISTRACIÓN DE RED

Los modelos de Gestión de Redes son muchas veces criticados de ser complejos. Pero en muchas ocasiones eso se debe al poco entendimiento sobre lo que en realidad significan estos modelos en sí.

Un modelo referencial de gestión de redes, debe entenderse como algo conceptual, que permite dividir el problema de manera abstracta. En realidad, un modelo de referencia no se lo sigue literalmente al pie de la letra, este simplemente proporciona el marco general para dar la solución a una necesidad.

Para el presente trabajo se han estudiado los modelos de gestión de redes de telecomunicaciones como TMN y e-TOM y modelos de gestión de redes de computadoras como son el modelo OSI y el SNMP (o Modelo Internet). Debido a que estos son los modelos de gestión de redes más difundidos en la actualidad.

Para la selección del Modelo de Gestión a seguir dentro del presente trabajo se tomaron en cuenta las siguientes comparaciones:

- TMN y el modelo OSI guardan mucha relación. La arquitectura funcional de TMN puede ser explicada en términos de conceptos del modelo OSI. Además, ambos utilizan la ayuda del modelo FCAPS para definir ciertas áreas funcionales dentro de sus propios modelos.[2]

- En cambio, TMN y el modelo de Internet (SNMP), guardan una gran diferencia en sus enfoques al presentar los modelos. Por ejemplo TMN se enfoca principalmente en especificaciones para las arquitecturas de gestión, y el modelo de Internet se concentra en la implementación de protocolos de gestión. Y como resultado de esto, en el mercado son limitados los productos para trabajar con TMN, mientras que el dominio de productos para trabajar con SNMP son mucho más difundidos.

- TMN en sus especificaciones sugiere una separación conceptual entre la red que es administrada o gestionada y la red sobre la cual se transfiere la información gestionada. En cambio en el modelo de Internet o SNMP esto lo toma desde otra perspectiva, este prefiere el uso de los mismos componentes para la red que es gestionada y la red sobre la cual se transfiere la información acerca de la red administrada. [2]

Luego de ser analizados los modelos, se decidió optar por un modelo híbrido de gestión de red. Con el fin de aprovechar las características más relevantes de cada uno de ellos, para satisfacer al desempeño de la red y a los objetivos planteados.

Los modelos de gestión estandarizados a ser tomados en cuenta, son el modelo TMN y el SNMP o modelo de Internet.

TMN se propone como la arquitectura de referencia para el intercambio de información de gestión entre los diferentes sistemas y/o equipos. Siguiendo una conexión gestor-agente, donde el sistema de gestión (consola de monitoreo) no

envía las órdenes directamente a los recursos, sino a través de agentes localizados más cerca de los mismos.

TMN también proporcionará el *aspecto funcional* del modelo que se propone en este trabajo, definiendo las actividades que hay que realizar y la organización de las mismas (modelo FCAPS).

SNMP en cambio proporcionará el *aspecto de la comunicación*, ya que será el protocolo sobre el cual se basará el modelo híbrido propuesto en el presente capítulo. Con él especificamos el lenguaje utilizado por los sistemas para el intercambio de la información. Su objetivo será permitir la transferencia e interpretación correcta de la información de gestión.

Otro aspecto importante al utilizar el modelo SNMP como nuestro protocolo para gestionar los recursos, es que permite usar una misma infraestructura de red sobre la cual se transfieran los datos gestionados, y con esto permite ahorrar costos, ya que no es necesario adquirir nuevos equipos para implementar una red independiente para la transferencia de la información de gestión. El modelo de Internet o SNMP puede hacer esto porque las redes de datos proveen el mismo tipo de servicio (asincrónico, es decir, orientado a paquetes) que se requiere para la transferencia de la información de gestión. [2]

Es decir, se va a utilizar el concepto más valioso del modelo TMN como es la Arquitectura Lógica de Capas (*LLA: Logical Layered Architecture*).

LLA indica como las funciones de gestión se organizan en una estructura jerárquica de niveles que cubren todos los aspectos de la administración de una red que se deben abarcar en una institución, como la del presente trabajo y clasifica las funciones que se deben realizar en cada nivel según criterios de responsabilidad.

La arquitectura de capas de TMN hace distinciones entre la gestión de un elemento, de una red, de un servicio y de un negocio, a diferencia de SNMP que

tradicionalmente se enfoca en la gestión de elementos y de la red. Es por esta razón, que viendo la necesidad de extender el enfoque de SNMP que se propone una combinación de ambos modelos. [3]

3.5 METODOLOGÍA PARA LA IMPLEMENTACIÓN DEL MODELO DE GESTIÓN Y ADMINISTRACIÓN EN LA RED DE LA UTEQ

En esta parte se presentará la metodología propuesta para la implementación de un modelo de gestión y administración de la red de datos de la UTEQ.

3.5.1 PLAN PARA EL DESARROLLO DE LA METODOLOGÍA

La figura 3.1 muestra de manera general todas las etapas necesarias para el mejoramiento del sistema de administración y gestión de la red de datos de la UTEQ, incluyendo la etapa “metodología para la implementación del modelo” de gestión que es la razón del desarrollo del presente capítulo.

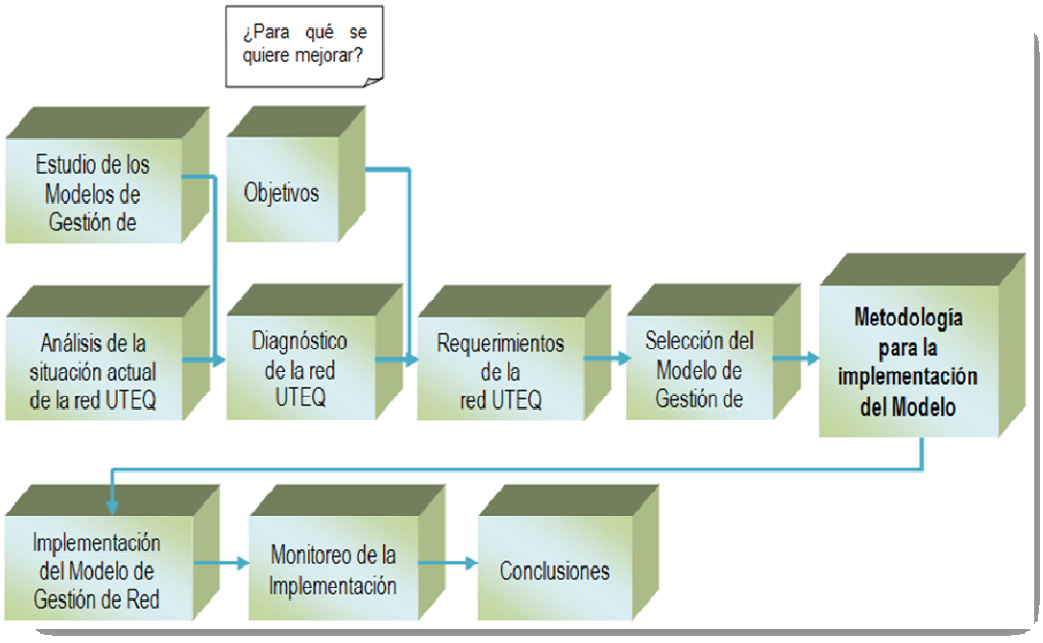


Figura 3.1 Etapas para el mejoramiento de la Gestión y Administración de la Red de Comunicaciones

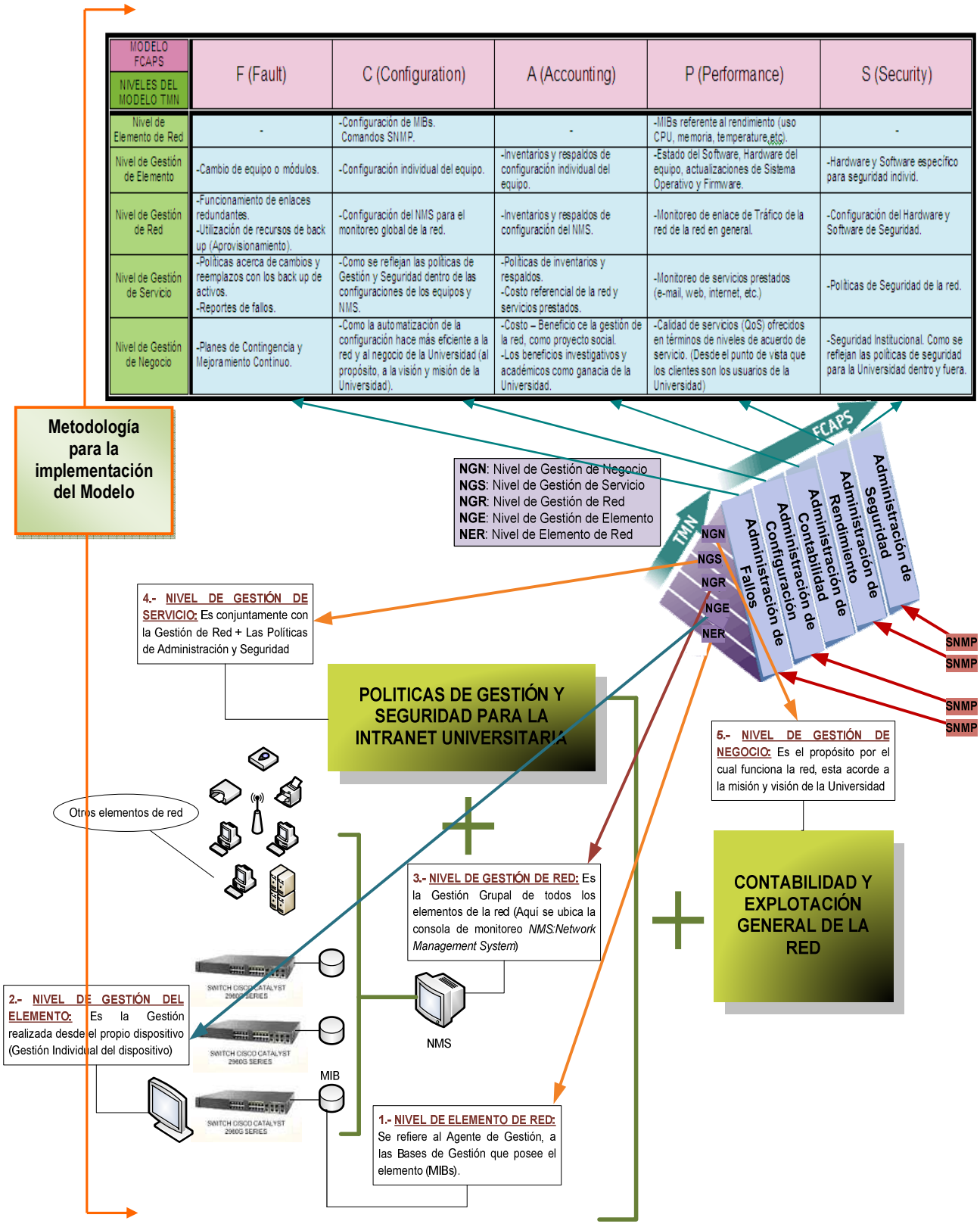


Figura 3.2 Desarrollo Esquemático de la Metodología de la Implementación del Modelo de Gestión y Administración de Red para la UTEQ

El presente capítulo como se mencionó, se centrará en la Metodología para la Implementación del Modelo de Gestión.

Se toma en cuenta que anteriormente en este mismo trabajo, en capítulos previos se han desarrollado varias de las etapas señaladas dentro del esquema general (Estudio de los modelos de Gestión de Redes/Capítulo 1, Análisis de la situación actual de la red UTEQ/Capítulo 2, Diagnóstico de la red/Capítulo 2, Requerimientos de la red UTEQ/Capítulo 2) mostrado en la figura 3.1.

El alcance del trabajo sólo llega hasta el desarrollo de esta metodología (Ver figura 3.2), más no incluye las etapas de implementación. Se tomará como referencia la dimensión funcional del modelo TMN redefinida con *FCAPS* (Figura 3.3).

MODELO FCAPS / NIVELES DEL MODELO TMN	F (Fault)	C (Configuration)	A (Accounting)	P (Performance)	S (Security)
Nivel de Elemento de Red	-	-Configuración de MIBs. Comandos SNMP.	-	-MIBs referente al rendimiento (uso CPU, memoria, temperature,etc).	-
Nivel de Gestión de Elemento	-Cambio de equipo o módulos.	-Configuración individual del equipo.	-Inventarios y respaldos de configuración individual del equipo.	-Estado del Software, Hardware del equipo, actualizaciones de Sistema Operativo y Firmware.	-Hardware y Software específico para seguridad individ.
Nivel de Gestión de Red	-Funcionamiento de enlaces redundantes. -Utilización de recursos de back up (Aprovisionamiento).	-Configuración del NMS para el monitoreo global de la red.	-Inventarios y respaldos de configuración del NMS.	-Monitoreo de enlace de Tráfico de la red de la red en general.	-Configuración del Hardware y Software de Seguridad.
Nivel de Gestión de Servicio	-Políticas acerca de cambios y reemplazos con los back up de activos. -Reportes de fallos.	-Como se reflejan las políticas de Gestión y Seguridad dentro de las configuraciones de los equipos y NMS.	-Políticas de inventarios y respaldos. -Costo referencial de la red y servicios prestados.	-Monitoreo de servicios prestados (e-mail, web, internet, etc.)	-Políticas de Seguridad de la red.
Nivel de Gestión de Negocio	-Planes de Contingencia y Mejoramiento Continuo.	-Como la automatización de la configuración hace más eficiente a la red y al negocio de la Universidad (al propósito, a la visión y misión de la Universidad).	-Costo – Beneficio ce la gestión de la red, como proyecto social. -Los beneficios investigativos y académicos como ganacia de la Universidad.	-Calidad de servicios (QoS) ofrecidos en términos de niveles de acuerdo de servicio. (Desde el punto de vista que los clientes son los usuarios de la Universidad)	-Seguridad Institucional. Como se reflejan las políticas de seguridad para la Universidad dentro y fuera.

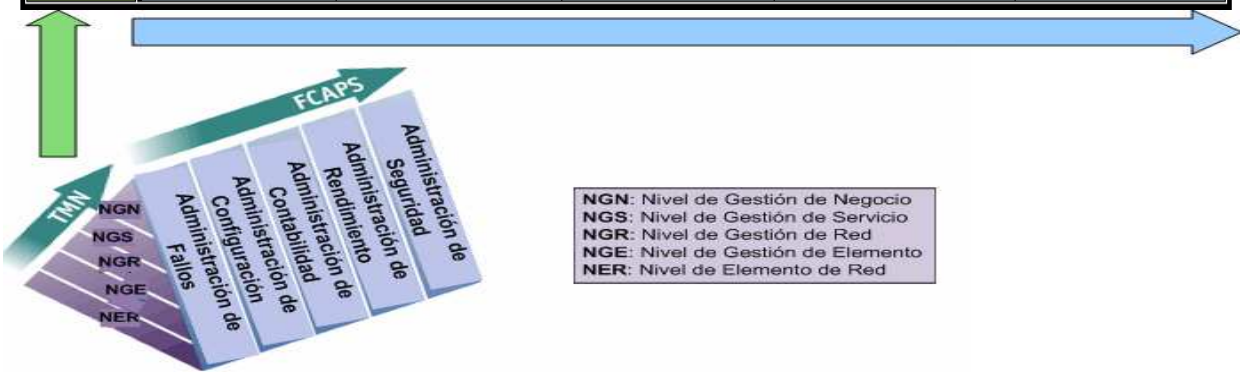


Figura 3.3 Modelo TMN y las actividades definidas para dentro de FCAPS

Se dividirá las funciones de la gestión y administración de la red en cinco categorías, como son la administración de la configuración, la administración del rendimiento, la administración de fallas, la administración de la contabilidad y la administración de la seguridad. Esta categorización será incluida dentro del modelo lógico de capas de TMN (*LLA*). Siendo SNMP el protocolo utilizado en los diferentes niveles de gestión.

3.5.2 ADMINISTRACIÓN DE LA CONFIGURACIÓN

Esta área funcional de la administración comprende el conjunto de actividades y funciones cuyo objetivo es proporcionar los servicios solicitados por los usuarios de la red. [3]

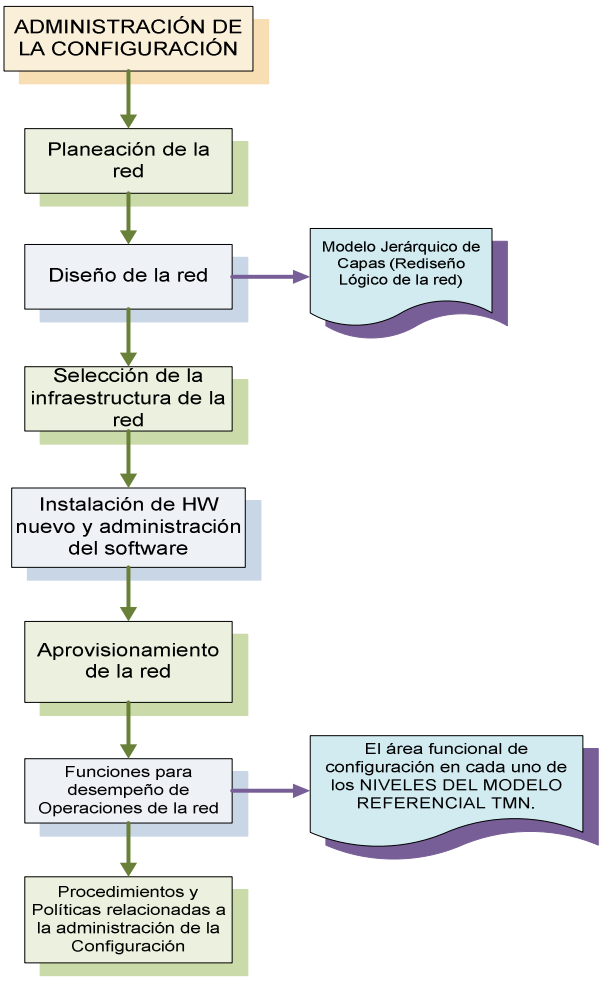


Figura 3.4 Etapas para llevar a cabo la Administración de la Configuración

La administración de configuración como primer paso abarca las actividades de planeación y diseño de la red; continuando con la selección de la infraestructura de la misma, la instalación de hardware, administración del software y el aprovisionamiento. También, hace referencia a las funciones para desempeñar operaciones que modifiquen las configuraciones de los equipos de la red. Por último, se tienen los procedimientos y políticas que pueden significar una ayuda para el desarrollo de esta área de la gestión de la red. [5]

3.5.2.1 Planeación de la Red

La meta de esta actividad es satisfacer los requerimientos inmediatos y futuros de la red, reflejarlos en su diseño hasta llegar a su implementación. La planeación de la red tiene varias etapas. La primera es reunir las necesidades específicas o generales de la red, lo cual se planteó como los objetivos en el presente capítulo.

Para satisfacer estos requerimientos muchas veces sólo es necesaria una adecuación en el diseño de la red (rediseño lógico de la red), y no requiere un rediseño completo.

Sólo en casos particulares de querer implementar completamente una nueva tecnología o cambiar los protocolos de ruteo interno, se crea la necesidad de un cambio total de la red, para el caso en específico esto no será necesario.

Las siguientes etapas abarcan, el diseño de la topología de la red, determinar y seleccionar la infraestructura de la red basándose en los objetivos y la topología propuestas. Y como último paso una vez satisfechas las etapas anteriores, pasar a la implementación, que para el presente proyecto no se encuentra dentro de su alcance.

3.5.2.2 Diseño de la red

Para lograr reflejar todos los objetivos que se quieren conseguir con la red de datos, se realizará un rediseño de la infraestructura de la misma, en el cual más

que ser un rediseño físico, será una reestructuración lógica jerárquica de los componentes de la red.

Para realizar tal rediseño nos ayudaremos del modelo de capas de CISCO, que a breves rasgos será descrito a continuación:

3.5.2.2.1 Modelo Jerárquico de Capas [6]

El modelo jerárquico de capas es un esquema que ayuda a los diseñadores y administradores de redes a tener una mejor visión de la red, desde varios puntos de vista principalmente tecnológicos y funcionales; además es un modelo didáctico que permite detallar las características y funciones que deben tener cada una de las capas de las cuales se conforma.

Las capas y características de cada una de ellas se detallan a continuación.

a. Capa de Acceso

La capa de acceso es el punto en el que cada usuario se conecta a la red. Ésta es la razón por la cual la capa de acceso se denomina a veces capa de puesto de trabajo, capa de escritorio o de usuario. Los usuarios así como los recursos a los que éstos necesitan acceder con más frecuencia, están disponibles a nivel local. El tráfico hacia y desde recursos locales está confinado entre los recursos, *switches* y usuarios finales.

En la capa de acceso se puede encontrar múltiples grupos de usuarios con sus correspondientes recursos. En muchas redes no es posible proporcionar a los usuarios un acceso local a todos los servicios, como archivos de bases de datos, almacenamiento centralizado, etc. En estos casos, el tráfico de usuarios que demandan estos servicios se desvía a la siguiente capa del modelo (capa de distribución).

En éste caso en particular, la universidad tiene una capa de acceso, que comprende los equipos como el router del proveedor y la infraestructura LAN

utilizada por personal administrativo y demás usuarios. Así como la red inalámbrica que permite el acceso de los campus secundarios a la red principal.

b. Capa de Distribución

La capa de distribución marca el punto medio entre la capa de acceso y los servicios principales de la red. La función primordial de esta capa es realizar funciones tales como enrutamiento, filtrado y acceso WAN.

En el entorno como el de la red de la universidad, la capa de distribución abarca una gran diversidad de funciones, entre las que figuran las siguientes:

- Servir como punto de concentración para acceder a los dispositivos de la capa de acceso.
- Enrutar el tráfico para proporcionar acceso a los departamentos o grupos de trabajo.
- Segmentar la red en múltiples dominios de difusión/multidifusión.
- Proporcionar niveles de seguridad y filtrado.

La capa de distribución puede resumirse como la capa que proporciona una conectividad basada en una determinada política, dado que determina cuándo y cómo los paquetes pueden acceder a los servicios principales de la red.

La capa de distribución determina la forma más rápida para que la petición de un usuario (como un acceso al servidor de archivos) pueda ser remitida al servidor. Una vez que la capa de distribución ha elegido la ruta, envía la petición a la capa de núcleo. La capa de núcleo podrá entonces transportar la petición al servicio apropiado.

c. Capa Núcleo

La capa del núcleo, principal o *Core* se encarga de enviar el tráfico lo más rápidamente posible hacia los servicios apropiados. Normalmente, el tráfico transportado se dirige o proviene de servicios comunes a todos los usuarios.

Estos servicios se conocen como servicios globales, algunos de estos servicios pueden ser: *e-mail*, acceso a Internet o videoconferencia.

Cuando un usuario necesita acceder a un servicio global, la petición se procesa al nivel de la capa de distribución. El dispositivo de la capa de distribución envía la petición del usuario al núcleo, este se limita a proporcionar un transporte rápido hasta el servicio global solicitado. El dispositivo de la capa de distribución se encarga de proporcionar un acceso controlado a la capa de núcleo.

El modelo jerárquico de capas permite dividir una red de información en módulos autónomos de funcionalidades bien definidas. De este modo se puede separar el problema del diseño de la red en sub-problemas con mayor facilidad de solución. [7]

3.5.2.2.2 Propuesta Esquemática del Rediseño Lógico de la Red de Comunicaciones de la UTEQ

Siguiendo el Modelo Jerárquico de Capas, en la Figura 3.5 se muestra la estructura interna de la red de la universidad que se quiere conseguir; se pueden identificar además varias zonas, que se enlazan a las distintas capas del sistema: la zona de usuarios, zona de servicios, zona de administración y zona Internet.

La capa de núcleo está formada por un sistema de conmutación, que es el *switch* del Área de Redes del Instituto de Informática, que posee la capacidad suficiente para manejar el tráfico que pasa por él.

Para el caso particular de la red UTEQ consideraremos como parte de la capa de distribución al core de *switches* Cisco 2960 que dispone la universidad. Los cuales se encuentran conectados en una topología estrella con redundancia al *switch* del Departamento de Informática, donde se concentran los servicios proporcionados por la red.

La capa de acceso está formada por el enlace a Internet, y las diferentes infraestructuras LAN que utilizan los usuarios.

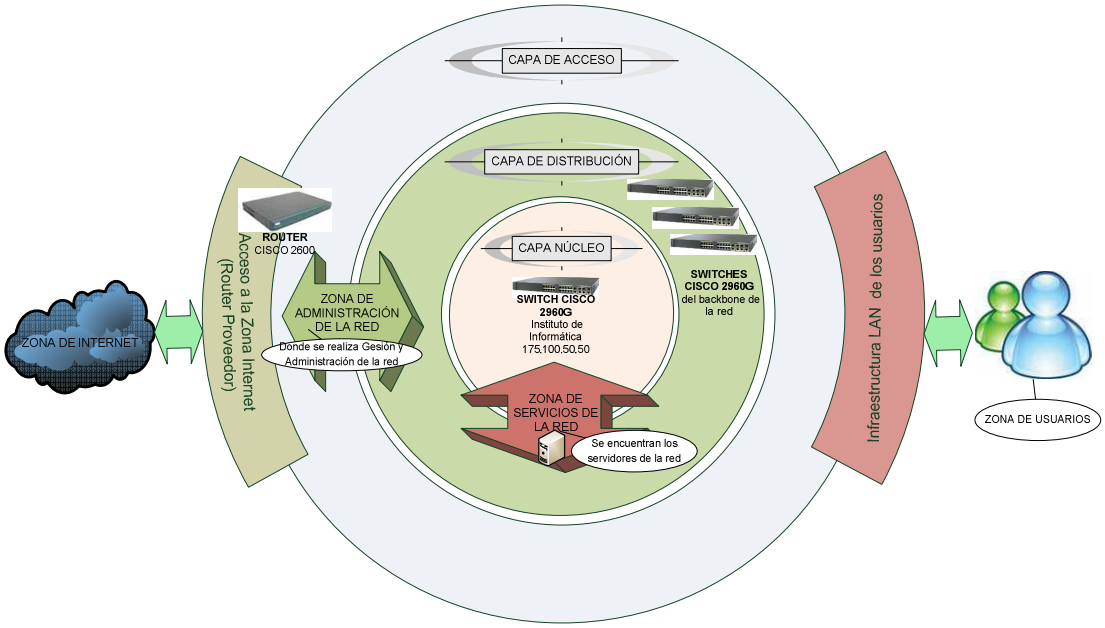


Figura 3.5 Propuesta Esquemática del Rediseño Lógico de la Red de Datos de la UTEQ

La zona de servicios alberga a los servicios básicos de red públicamente disponibles (DHCP, DNS, Correo Electrónico, entre otros.).

La zona de administración contiene los sistemas necesarios para la administración y gestión de la red de la universidad en general, así como los sistemas que soportan las operaciones de la misma. Esta zona es de principal interés, ya que la implementación del modelo de administración se ubicaría aquí.

La zona Internet incorpora la funcionalidad para conectarse con los proveedores de servicios para tener presencia y acceso a Internet.

La zona de usuarios permite el acceso a usuarios del personal administrativo, docente y estudiantes a la red de la institución; está formada por los equipos terminales de usuario.

El rediseño lógico de la red se realizará de forma modular, de acuerdo con los parámetros de diseño y requisitos antes descritos.

3.5.2.3 Selección de la Infraestructura de la red

Para el presente caso, se reutilizará la infraestructura de la red con la que cuenta la universidad actualmente, mejorándola en caso de ser necesario para que cumpla con los objetivos propuestos por el modelo de gestión.

Criterios de reutilización:

La UTEQ cuenta con una red de Tecnología Fast Ethernet con capacidad de transmisión de hasta 100 Mbps[12] en todos los puntos donde existen usuarios finales, su infraestructura LAN utiliza cableado estructurado UTP Cat5e, el mismo que ofrece la capacidad de canal óptimo para la transmisión de datos necesaria y suficiente para el trabajo de la red paralela de gestión que se sugiere implementar en esta tesis.

Para mayor detalle sobre las capacidades que tiene la red para soportar el tráfico del nuevo modelo de gestión, se monitoreo el tráfico total de la red interna de la Universidad en el Switch de Core que se encuentra en el Instituto de Informática.

El monitoreo del tráfico que actualmente cursa el equipo principal de Backbone de la UTEQ, se lo realizó en una semana considerada pico como es la semana final de clases y exámenes, donde se realiza mayor uso de los aplicativos de la institución. El monitoreo se realizó en el puerto de Backbone de Fibra que tiene la UTEQ. Se analizó la entrada (*Downstream*) de tráfico al equipo donde se están considerando las peticiones de los clientes (Figura 3.6) y también se analizó el tráfico de salida (*Upstream*) donde se consideraron las respuestas generadas por los servidores a estas peticiones. (Figura 3.6)

Con el monitoreo realizado, se pudo notar que el mismo no supera en promedio los 16 Mbps totales.

[12] En el presente trabajo se asociará el término Ancho de Banda al concepto de Capacidad de Canal cuyas unidades se dan en bits por segundo (bps).

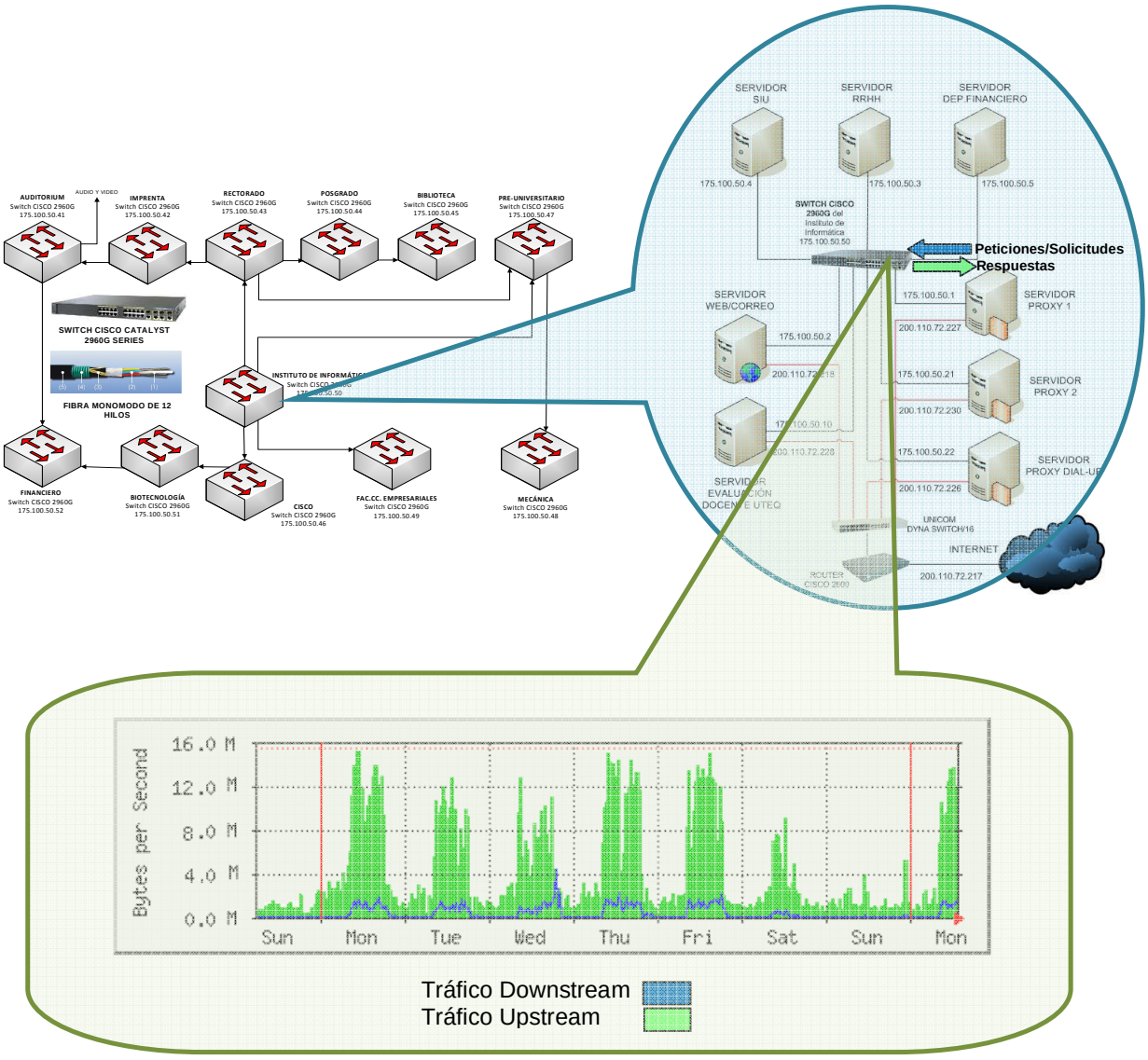


Figura 3.6 Monitoreo del tráfico en el puerto fibra óptica del Switch de Informática de la UTEQ

Calcular el tráfico promedio que se generaría con la implementación de la red de gestión depende de muchos factores, entre los cuales se menciona: las configuraciones del protocolo SNMP, refiriéndose especialmente a los tiempos de poleo y del número de estaciones que se van a monitorear. Como criterio de diseño utilizado en este trabajo, se asumirá el peor caso en donde el tráfico de gestión representará un incremento del 100% del valor promedio actual de

utilización de la red, con lo cual este no se llegaría a valores críticos de uso para la infraestructura de la red Universitaria, como se demuestra a continuación:

Tráfico de Red Actual + Tráfico de Red de Gestión = Tráfico Total

Tráfico de Red Actual + Tráfico de Red Actual = Tráfico Total

16 Mbps + 16 Mbps = **32 Mbps < 100 Mbps**

Después del análisis de la situación actual de la red Universitaria, se ha encontrado 2 puntos que pueden generar cuellos de botella en el funcionamiento de la red:

1. En la salida de tráfico de Internet, el cual es un servicio contratado y tiene un valor según su capacidad, el mismo que en la actualidad es de 5 MB.

2. Son los cuellos de botella que se podrían generar en los Servidores de la UTEQ, ya sea por aplicaciones y/o concurrencia de usuarios del servicio. Pero este tipo de dificultad podría revisarse en un redimensionamiento de servidores, lo cual excede el alcance del presente trabajo.

Tomando en cuenta estos puntos críticos se verifica que estos no se generan por la red interna en sí, ni su infraestructura, la misma que es robusta y soportaría muy bien el modelo planteado en esta tesis.

Otro criterio para la reutilización de la infraestructura son los equipos del backbone y demás equipos de conmutación, los mismos que son equipos actuales y cuentan con las capacidades suficientes para soportar los niveles de información que se necesitaría manejar sobre la red. Este criterio se lo obtiene de la información del monitoreo de procesos realizado a los equipos de conmutación, donde se analizó sus estadísticas de uso de CPU (ANEXO F) y memoria, los cuales reflejaron que actualmente los equipos no trabajan ni siquiera la mitad de sus capacidades reales, muchos de los cuales mostraron un máximo de 15 % de utilización de su capacidad total.

Las actuales características de la infraestructura de red por los criterios antes mencionados, satisfacen el rediseño lógico de jerarquías de capas necesario para facilitar la comprensión de la metodología para la implementación del modelo de gestión para la red de la UTEQ.

Para el caso, en el que fuese necesario adquirir nuevos equipos, estos deberían cumplir con la mayoría de las necesidades técnicas y es recomendable que previamente hayan pasado por un plan de pruebas.

3.5.2.4 Instalaciones del Hardware y Administraciones del Software

La finalidad de esta actividad es conseguir un manejo adecuado de los recursos de hardware y software dentro de la red.

3.5.2.4.1 Instalaciones de Hardware [5]

Las tareas de instalación de hardware contemplan, tanto la agregación como la sustitución de equipamiento de la red de la UTEQ, y pueden abarcar, ya sea un dispositivo completo, como un switch o un router; o solo una parte de los mismos, como una tarjeta de red, tarjeta procesadora, un módulo, etc. El proceso de instalación consiste de las siguientes etapas:

- Realizar un estudio previo para asegurar que la parte que será instalada es compatible con los componentes ya existentes.
- Definir la fecha de ejecución y hacer un estimado sobre el tiempo de duración de cada paso de la instalación.
- Notificar anticipadamente a los usuarios sobre algún cambio en la red.
- Generalmente, a toda instalación de hardware corresponde una instalación o configuración en la parte de software, entonces es necesario coordinar esta configuración.
- Generar un plan alterno por si la instalación provoca problemas de funcionalidad a la red.

- Realizar la instalación procurando cumplir con los límites de tiempo previamente establecidos.
- Documentar los cambios realizados en el equipamiento para futuras referencias.

3.5.2.4.2 Administraciones del Software [5]

Esta es la actividad responsable de la instalación, desinstalación y actualización de una aplicación, sistema operativo o funcionalidad en los dispositivos de la red. Además, de mantener un control sobre los programas que son creados para obtener información específica en los dispositivos.

Antes de realizar una instalación, se debe tomar en cuenta lo siguiente.

- Que las cantidades de memoria y almacenamiento sean suficientes para la nueva entidad de software.
- Asegurar que no exista conflicto alguno, entre las versiones actuales y las que se pretenden instalar.

Otra actividad importante es el respaldo frecuente de las configuraciones de los equipos de red ya que son un elemento importante que requiere especial cuidado.

Estos respaldos son de mucha utilidad cuando un equipo se daña y tiene que ser reemplazado, ya que no es necesario realizar la configuración nuevamente, lo que se hace es cargar la configuración al dispositivo mediante un servidor de tftp.

3.5.2.5 Aprovisionamiento de la red

Esta actividad tiene la función de asegurar la redundancia de los elementos de software y hardware más importantes de la red. Esto se lo puede llevar a cabo a nivel de la red global o a nivel de un elemento en particular. Esta etapa es la responsable de abastecer de los recursos necesarios para que la red funcione, entre los que se encuentran los elementos físicos como conectores, cables,

multiplexores, tarjetas, módulos, y los elementos de software como versiones de sistema operativo, parches y aplicaciones. La etapa de aprovisionamiento permite asegurar que recursos tanto de hardware como de software, siempre se encuentren disponibles ante cualquier eventualidad que se pueda producirse en la red. Algunos de los elementos de hardware más importantes con los que siempre se debe contar son tarjetas de procesadores, fuentes de poder, módulos de repuesto, equipos para sustitución y un respaldo de cada uno de ellos.

3.5.2.6 Funciones para el Desempeño de Operaciones de la Red [8]

El objetivo de esta actividad es permitir modificaciones a las configuraciones de los equipos de la red.

3.5.2.6.1 Configuración de los Recursos Gestionados

En el núcleo de la gestión de configuración están las actividades y operaciones usadas para configurar los elementos de red que están siendo gestionados. Esto incluye el envío de comandos a los equipos de la red para cambiar sus configuraciones. En algunos casos, puede tratarse solo de aislar la configuración de una interfase en un puerto en un dispositivo de red.

La gestión de configuración también incluye las funciones para realizar las configuraciones que son necesarias para que la red pueda brindar un servicio al usuario final.

Cabe recalcar que la administración de la configuración participa en cada uno de los niveles del marco referencial TMN utilizado para este trabajo. A continuación se detalla como la configuración se involucra en cada uno de los niveles:

En el *Nivel de Elemento de Red (NER)* se realiza las configuraciones de las MIBs en los elementos de la red para poder tener acceso a toda la información gestionable de los mismos. Las MIBs que soportan los equipos o elementos principales de interconexión de red de la Universidad se encuentran en el ANEXO G. [40]

A *Nivel de Gestión del Elemento (NGE)* se realiza las configuraciones individuales de de cada uno de los equipos, se habilitan las versiones del Protocolo SNMP que soporta cada equipo respectivamente. Los equipos de la red de la UTEQ según sus características técnicas soportan las siguientes versiones SNMP:

EQUIPO	Versión SNMP	Otras Aplicaciones para Gestión del equipo
DWL-2100AP	Soporta SNMP v.3	Web-Based-Internet Explorer V6 o superior, Netscape Navigator V6 o superior
DWL-3200AP	Soporta SNMP v.3	Web Browser (HTTP,HTTPS), Telnet, AP Manager II
WAP54G	-	Web Browser (HTTP)
Switch CISCO Catalyst 2960G	Soporta SNMP v.3	Cisco Works LMS (LAN Management Solution)
ORINOCO OR 1100	Soporta SNMP	OR Manager
Router CISCO 2600	Soporta SNMP	Cisco Works, Cisco View
Switch Baseline 2824	-	No administrable
UNICOM DYNA Switch/16	-	No administrable

3.1. Tabla con principales equipos de interconexión y aplicaciones para ser gestionados y administrados

En el *Nivel de Gestión de Red* se configura la consola que realizará el monitoreo global de la red. Más adelante en el desarrollo del capítulo se ofrecen varias alternativas de sistemas de gestión de red global.

En el *Nivel de Gestión del Servicio,* tiene que ver con los criterios de políticas de seguridad y gestión tomados en cuenta al llevar a cabo las configuraciones en los niveles anteriores.

En el *Nivel de Gestión de Negocio* se reflejan en cambio las consecuencias de una buena configuración en los niveles anteriores de TMN, que brindan una mayor automatización de la red en general, y esto a su vez mayor eficiencia en los procesos dentro de la institución.

3.5.2.6.2 Auditoría de la Red

Con auditar la red, se refiere a la capacidad del administrador para pedir a la red que encuentre lo que está actualmente configurado en ella. En este caso la auditoría de la red tiene que ver con comandos para leer mucho más que con escribir.

Con la auditoría de la red se pone en conocimiento del estado de la red y se puede tener una mejor idea sobre la configuración y crecimiento de la misma. Nos proporciona un análisis de la arquitectura existente, infraestructura lógica y física, problemas, rendimiento y utilización.

Con la auditoría de la red de la UTEQ, lo que se quiere lograr es:

- Una evaluación y revisión de la arquitectura de la red.
- Un chequeo básico de la red LAN.
- Tener un informe final del estado de la red.
- Tener una base para recomendaciones y posibles soluciones.

Para la auditoría de la red, la misma que se aconseja se realice una o dos veces en el año, va a necesitar de un grupo dedicado a esta tarea. Con ello se logrará uniformidad en los informes y reportes presentados, el grupo al ser externo, analizará a profundidad cualquier detalle y se dedicará al 100% a auditar toda la red.

3.5.2.6.3 Respaldo de la Información [9]

El respaldo es una parte muy importante para la protección de los datos. En una red institucional como la UTEQ que desarrolla distintos Proyectos de Investigación, es importante contar con el respaldo automático de la información (Figura 3.7).

Como sistema de respaldo se propone un sistema centralizado de storage para almacenar la información sensible de la universidad. Información crítica para el desempeño de la red como configuraciones de los elementos y respaldo de

información de servidores. Otra información crítica es la información institucional, como la del personal administrativo, la del financiero, docente y estudiantil. También se encuentra la información digital del Área de Diseño Gráfico como aquella utilizada para hacer los trípticos, carnets estudiantiles, etc., que debería ser respaldada.

En la Unidad de Informática Agropecuaria trabajan en la digitalización de mapas, tienen bases de datos climatológicas del Ecuador, así como cartografía e imágenes de fotografías aéreas de grandes volúmenes de datos que necesitan ser respaldadas para garantizar el trabajo de la Institución en diferentes proyectos en los que trabajan actualmente.

Los riesgos para los datos pueden ser de distinto tipo. El más común es la falla en discos duros, pero hay otras maneras en las que los datos corren un riesgo inminente, algunas de ellas son: falla del hardware, falla del software, corrupción del sistema de archivos, borrado accidental, infección por virus, desastre natural, robo del equipo, sabotaje, etc. Debido a los riesgos antes mencionados, la necesidad de un respaldo confiable y la recuperación de datos tienen un nivel de importancia crítico para una institución como la UTEQ, la cual entiende las ventajas de salvar y acceder grandes volúmenes de datos.

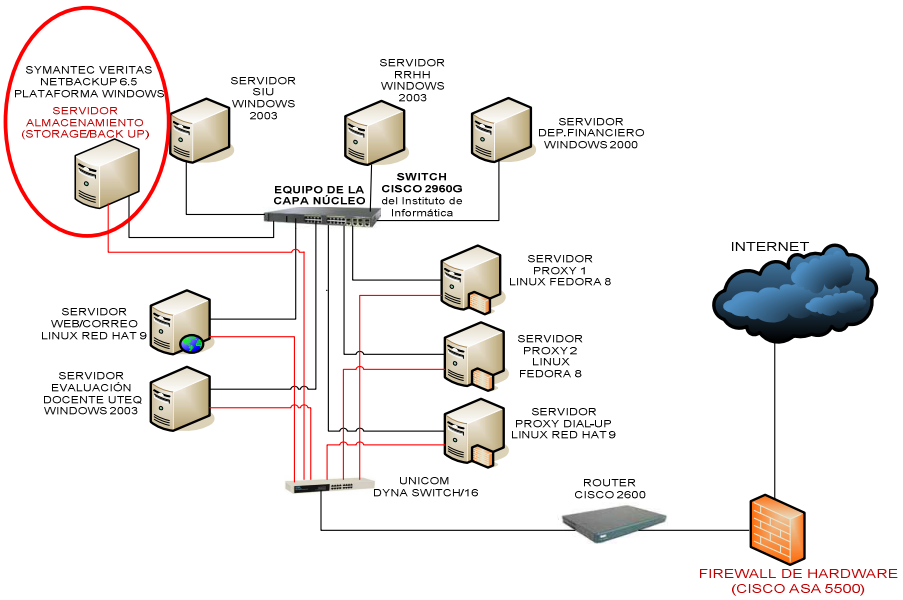


Figura 3.7 Ubicación del servidor redundante de almacenamiento

Servidor	Tipo	Procesador	RAM	Disco Duro
BackUp	HP Proliant ML370 G4	Intel QUAD Xeon 3.4 GHz.	4 GBytes	2 discos de 146 GBytes

Tabla 3.2 Servidor de Respaldo

General	
Tipo	Servidor
Uso recomendado	Empresa
Factor de forma del producto	Torre - 5U
Cantidad de compartimentos de intercambio rápido (hot-swap)	8
Procesador	
Tipo	Intel Xeon 3.4 GHz
Características principales del procesador	Hyper-Threading Technology
Placa principal	
Tipo conjunto de chips	Intel E7520
Velocidad bus de datos	800 MHz
Memoria RAM/Disco	
Tamaño instalado	2 GB / 4 GB (máx.)
Nivel RAID	RAID 0, RAID 1, RAID 5, RAID 10
Tamaño de búfer	128 MB
Disco duro	2 x 146 GB - intercambio rápido (hot swap)
Conexión de redes	
Conexión de redes	Adaptador de red - PCI-X / 133 MHz - integrado
Protocolo de interconexión de datos	Ethernet, Fast Ethernet, Gigabit Ethernet
Cumplimiento de normas	IEEE 802.3, IEEE 802.3u, IEEE 802.3ab
Sistemas operativos / Software	
OS proporcionado	Microsoft Windows Storage Server 2003
Software	Controladores y utilidades
Garantía del fabricante	
Servicio y mantenimiento	3 años de garantía

Tabla 3.3 Características Servidor HP Proliant ML370 G4

Cabe mencionar que existen distintos tipos de respaldo que pueden ser implementados, dependiendo de la característica del respaldo, que pueden ser:

capacidad, automatización, expansión, confiabilidad, simplicidad, universalidad y/o rendimiento.

En el caso de la Universidad las características de automatización y confiabilidad se consideran primordiales al momento de elegir el mecanismo para los respaldos. Es decir, se busca que los respaldos sean programados y la recuperación de datos sea predecible, confiable, segura y rápida.

En el mercado actualmente se utiliza tecnología de respaldo digital. En el caso de la red de la UTEQ, se propone la implementación del servidor dedicado para respaldo de datos, que se detalla en la tabla 3.2. Equipo que se encargaría de salvaguardar los datos más sensibles de todos los servidores de la UTEQ. Junto a este servidor se contaría con el software de automatización de las tareas programadas de respaldos proporcionado por el proveedor del equipo.

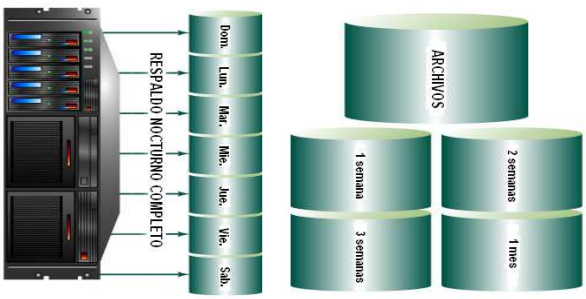


Figura 3.8 Automatización del Respaldo de la Información [9]

El servidor de almacenamiento tendrá plataforma de Windows y en lo que se refiere a aplicaciones de software, se utilizará Symantec Veritas NetBackup 6.5, un popular y completo sistema de almacenado y restauración de información.

3.5.2.6.4 Gestión de Imágenes de Software [8]

Este tipo de gestión es muy necesaria, para que el administrador esté en capacidad de seguir el rastro sobre cuales imágenes de software están instaladas en cuales equipos de la red, y tener los mecanismos para enviar nuevas

imágenes a aquellos dispositivos de la red que necesiten ser actualizados, y realizar toda la instalación sin interrumpir el servicio.

3.5.2.7 Procedimientos y Políticas relacionadas con el Área de Configuración[2]

En esta etapa se encuentran los procedimientos y políticas sugeridas para el desarrollo de la parte de gestión de configuración dentro del modelo de gestión de red:

3.5.2.7.1 Procedimientos de instalación de aplicaciones más utilizadas

El siguiente es un procedimiento sugerido para la instalación de las aplicaciones más utilizadas en los equipos que conforman la red de la UTEQ:

- Comprobar si el equipo en el cual se va instalar la aplicación dispone de una serie de requisitos técnicos mínimos, necesarios para el correcto funcionamiento del mismo.
- Realizar una prueba preliminar para verificar que la aplicación no provoque conflictos con el resto de aplicaciones instaladas previamente en los equipos.
- Definir las fechas de ejecución de las instalaciones y un estimado del tiempo de duración de la misma.
- Notificar anticipadamente a los usuarios de los equipos sobre los trabajos de instalación de las aplicaciones.
- Respetar los plazos de tiempo establecidos para las instalaciones.
- Realizar pruebas con las nuevas aplicaciones instaladas.
- Documentar los cambios realizados en los equipos para futuras referencias.

3.5.2.7.2 Política de respaldo de configuraciones

La política de *respaldo* de configuraciones, tiene algunos aspectos para cumplir que son:

- Definir la periodicidad del *respaldo* (diario, cada x días, semanal, quincenal, mensual).
- Definir el tipo de *respaldo* (Diferencial o completo)**.**
- Definir donde se almacenará (Otro disco duro, medio removible, servidor de archivos).
- Definir el método de *respaldo* (manual o automático).
- Definir el responsable del *respaldo*.

3.5.2.7.3 Procedimientos de instalación de una nueva versión de Sistema Operativo

- Realizar el respaldo de la información más importante del equipo, previa actualización del sistema operativo.
- Definir las fechas de ejecución de las instalaciones y un estimado del tiempo de duración de la misma.
- Notificar anticipadamente a los usuarios de los equipos sobre los trabajos de actualización del sistema operativo.
- Respetar los plazos de tiempo establecidos para las instalaciones.
- Realizar pruebas con las nuevas aplicaciones instaladas.

3.5.3 ADMINISTRACIÓN DEL RENDIMIENTO [2]

Esta área de la administración incluye las actividades que hacen posible que los servicios, redes o elementos de la red funcionen correctamente, mediante mediciones de parámetros y acciones correctivas necesarias en caso de situaciones anormales dentro de la red.

Esta área de gestión tiene como objetivo recolectar y analizar el tráfico que circula por la red para determinar su comportamiento en diversos aspectos, ya sea en un momento en particular (tiempo real) o en un intervalo de tiempo.

A continuación se muestran las etapas necesarias para realizar la administración del rendimiento de la red de la UTEQ:

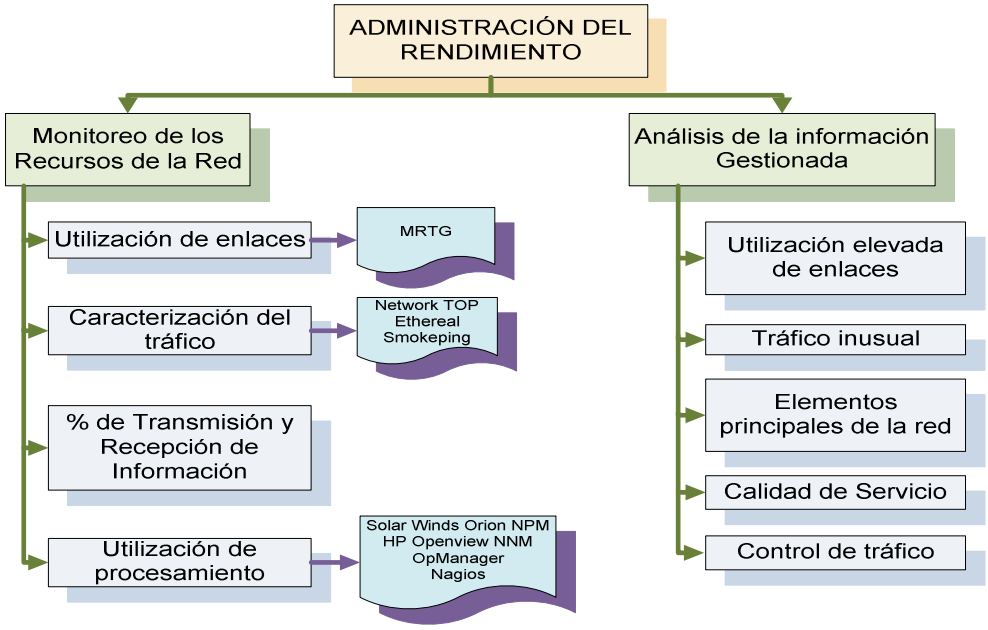


Figura 3.9 Etapas para la Administración del Rendimiento

3.5.3.1 Monitoreo de los recursos de la red

Al realizar un monitoreo constante sobre la disponibilidad y funcionalidad de los dispositivos y recursos informáticos de la UTEQ, se permite lograr un óptimo rendimiento de la red.

Las áreas funcionales de la administración muchas veces trabajan unas con otras, como en este caso, en la que el área de administración de rendimiento necesita de las demás áreas de administración para el correcto funcionamiento de la red.

El detectar las fallas en la red de manera oportuna, dar seguimiento a cualquier eventualidad ocurrida en los dispositivos de comunicaciones y servidores internos de la red, es de vital importancia cuando se trata del desempeño de una red institucional como la UTEQ. [11]

Actualmente, como ya se mencionó en el capítulo 2, el monitoreo de la red es básico y se lo realiza con un software proporcionado desde el router del proveedor, SQUINT y con herramientas propietarias incluidas en los equipos de

interconexión de los equipos CISCO como el Administrador de Dispositivos, la cual es una herramienta gráfica de gestión de dispositivos que entrega vistas en tiempo real de la configuración y condiciones de desempeño del switch de manera individual.

Con un monitoreo adecuado el administrador de la red de la UTEQ podrá observar y recolectar la información referente al comportamiento de la red con respecto a las siguientes situaciones:

3.5.3.1.1 Utilización de enlaces

En este caso, el administrador de la red podrá saber las cantidades ancho de banda utilizada por cada uno de los enlaces de área local (Ethernet, FastEthernet, GigabitEthernet, etc) de la universidad, ya sea de un dispositivo o de toda la red.

En este trabajo se proponen herramientas adicionales para monitorear los recursos de la red, que deberán instalarse en el servidor WEB Linux de la UTEQ. Esto debido a que es donde más libertades tienen los programas para correr y monitorear los ordenadores y equipos de la red evitando que cualquier intruso afecte a los servidores más sensibles (como bases de datos). De esta manera, se establece como ambiente de implementación al servidor HTTP APACHE para las aplicaciones de gestión que se proponen a continuación.

a. MRTG (Multi Router Traffic Graph) [12]

MRTG es una herramienta que sirve para generar gráficos estadísticos de los recursos gestionados de la red (Ver figura 3.10). Con ella se puede monitorear la carga de tráfico en los enlaces de la red de la universidad, carga de procesador de los servidores internos, temperatura de los dispositivos de red. Este software permite representar prácticamente cualquier dato que se desee analizar en la red.

MRTG se basa en Perl, el lenguaje C y funciona bajo los sistemas operativos UNIX y Windows NT. MRTG captura los datos de dos maneras: mediante SNMP y

mediante scripts de usuario. El protocolo del modelo de gestión planteado en este trabajo se basa en el protocolo SNMP, es por esta razón que se recomienda trabajar con este software.

El método utilizado para la captura de datos será mediante el protocolo snmp, por lo que las configuraciones se deben realizar para este método. Aunque, si se decide hacerlo mediante scripts, cabe mencionar que existen scripts que se pueden descargar de Internet y están listos para usar, según las necesidades.

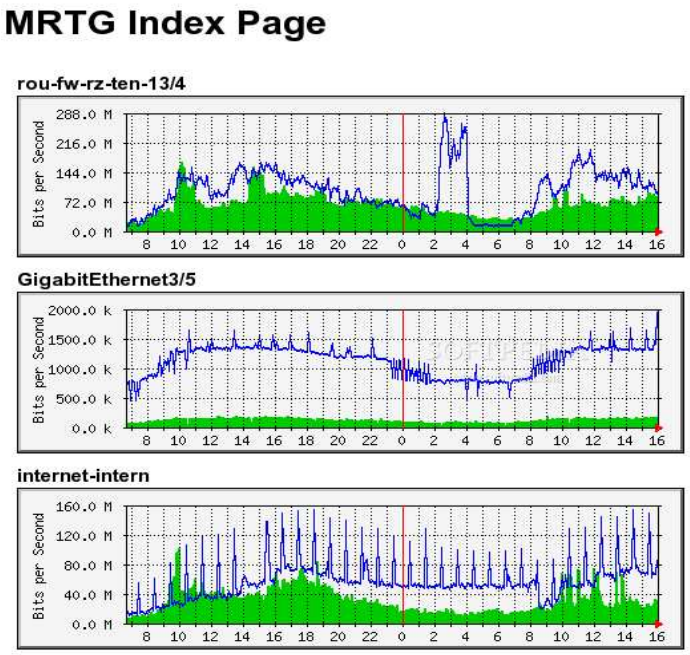


Figura 3.10 Ejemplo de gráfica generada por MRTG sobre consumo de ancho de banda [10]

MRTG puede ser integrado a una consola de administración global de la red (NMS: *Network Management System*) como NAGIOS, para trabajar en conjunto. Más adelante en el desarrollo del capítulo, se especifica cómo puede trabajar con un NMS.

3.5.3.1.2 Caracterización del tráfico

Tiene que ver con la tarea de detectar los diferentes tipos de tráfico que circulan por la red, con el fin de obtener datos sobre los servicios de red, como http, ftp, que son más utilizados. Además, esto también permite establecer un patrón en cuanto al uso de la red.

Como se mencionó en el punto del rediseño, dentro de la red se incluirán cierto tipo de servidores que permitirán la implementación del Sistema de Gestión y Administración. Además, se pretende mejorar y aumentar el número de servicios que presta la red, estos servicios y servidores adicionales aumentarán de hecho el tráfico dentro de la intranet de la UTEQ.

Los enlaces que se maneja dentro de la red de la Universidad son de tipo FastEthernet (100Mbps) para la red interna y de GigabitEthernet (1000Mbps) para los enlaces del backbone. Debido a esto no es una preocupación el ancho de banda dentro de la intranet para el desarrollo de este trabajo y por ende cuellos de botella dentro de la red de la UTEQ.

Para realizar una caracterización del tráfico existe una gran variedad de soluciones que van desde productos propietarios hasta soluciones gratuitas y de código abierto comúnmente utilizadas bajo sistemas Linux-UNIX.

Entre las herramientas para caracterizar el tipo de tráfico, proponemos las siguientes:

a. Network Top (NTOP) [15]

Ntop es una herramienta de gestión de red que muestra el uso de la red discriminando protocolos, puertos y aplicaciones. Está basada en la librería de captura de paquetes “pcap” y bajo sistemas *UNIX* se le conoce como TCPDump. [14]

En el presente caso, con este software el administrador de la red podrá ver lo que circula por la red de la universidad, generando una lista de las estaciones que están utilizando actualmente recursos de la red y mostrar la información referente al tráfico *IP* (*IP: Internet Protocol*) generado por cada estación.

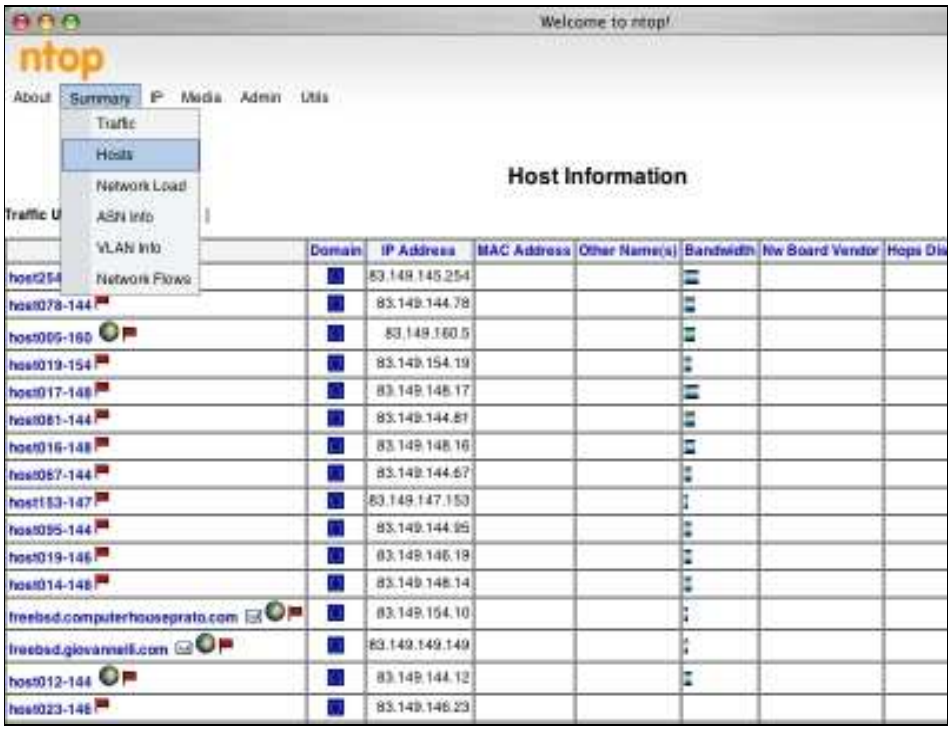


Figura 3.11 Ejemplo de monitoreo de características del tráfico con Ntop [13]

El tráfico de la lista estará clasificado según la estación y el protocolo. Entre las ventajas de usar esta herramienta están, el bajo consume memoria y recursos de CPU, y el ofrecer una configuración y administración vía web.

Entre los protocolos que es capaz de monitorear están: TCP, UDP, ICMP, ARP, IPX, DLC, Decnet, AppleTalk, Netbios, y ya dentro de TCP/UDP es capaz de agruparlos por FTP, HTTP, DNS, Telnet, SMTP/POP/IMAP, SNMP, NFS, X11, etc.

b. Ethereal [16]

Esta herramienta es un potente analizador de protocolos de redes, al igual que Ntop sus bases residen en la librería “pcap” diseñado para máquinas con sistema operativo Linux-Unix y Windows.

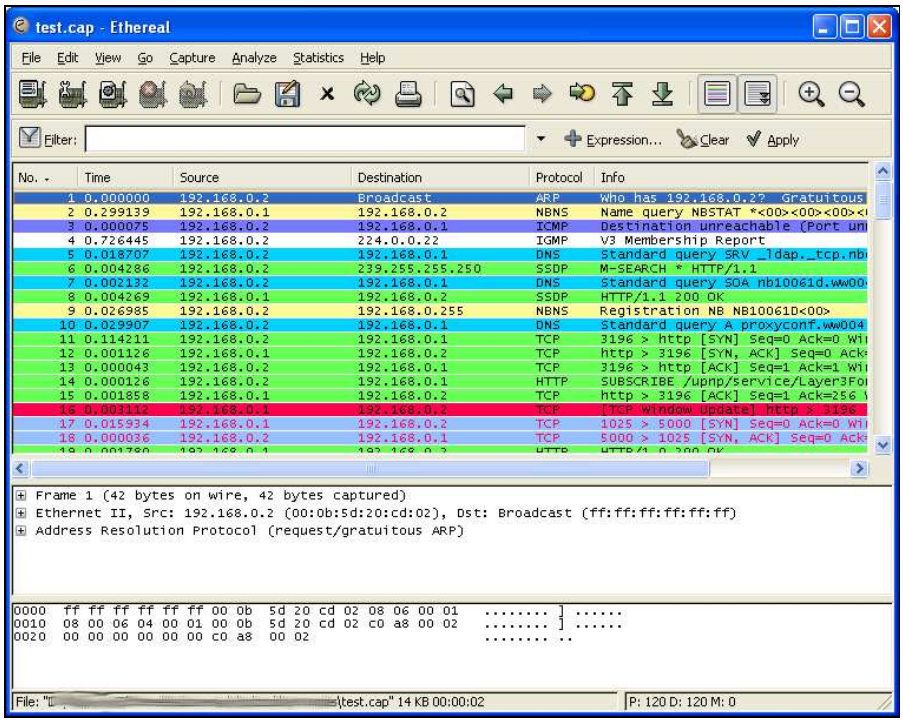


Figura 3.12 Ejemplo de monitoreo de características del tráfico con Ethereal [17]

Permite capturar los datos directamente de una red (tiempo real) o analizar la información a partir de una captura en disco (puede leer más de 20 tipos de formato distintos). Destaca también por su impresionante soporte de más de 300 protocolos.

c. Smokeping [18] [19]

Con la herramienta SmokePing el administrador de la red puede medir la latencia o retardos en la red. Con esta aplicación puede obtener información de retardo de paquetes ICMP y varios servicios más como: HTTP, DNS, SMTP, SSH, LDAP,

etc. Además permite definir rangos estadísticos para generar alarmas. Entre las utilidades están: medir, almacenar y mostrar latencias y paquetes perdidos. SmokePing se basa en RDDTool para mantener durante mayor tiempo los datos almacenados y generar de forma gráfica la información del estado actual de la red en cada cierto intervalo de tiempo para cada uno de los enlaces de la Intranet de la institución.

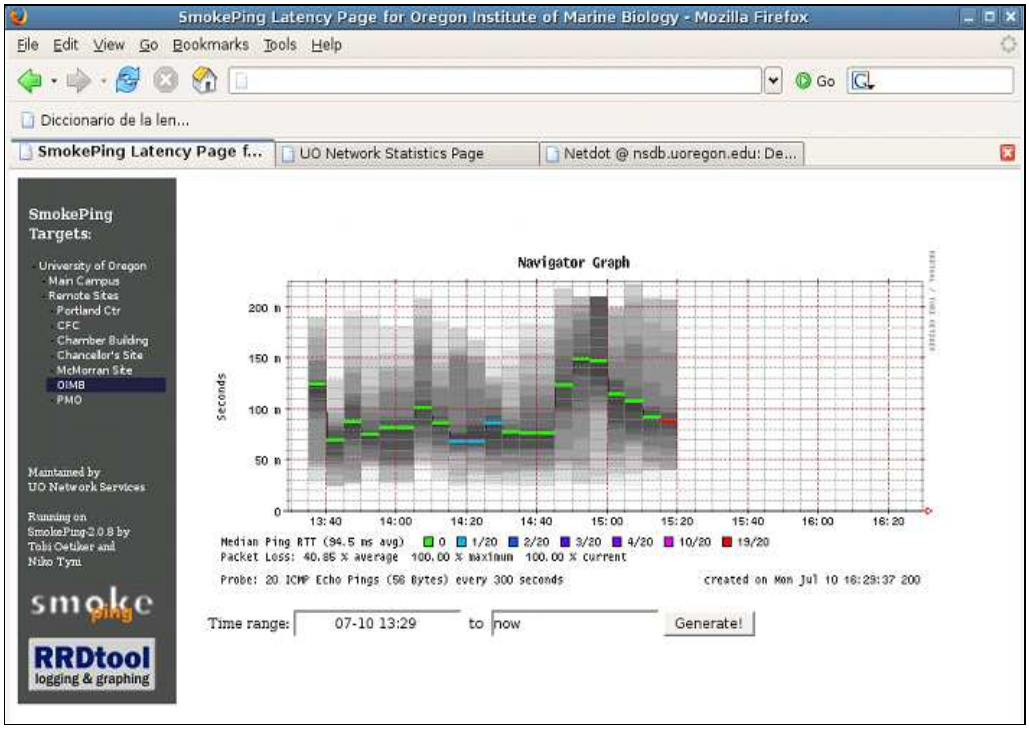


Figura 3.13 Ejemplo de monitoreo de características del tráfico con SmokePing [19]

3.5.3.1.3 Porcentaje de transmisión y recepción de información

Este tipo de información permite encontrar los elementos de la red que más solicitudes hacen y atienden, como servidores, estaciones de trabajo, dispositivos de interconexión, puertos y servicios. La herramienta Network Top (NTOP) mencionada en el literal anterior, también nos permite obtener este tipo de información para el caso la red de la Universidad.

3.5.3.1.4 Utilización de procesamiento

Otro aspecto importante dentro de la gestión de rendimiento de la red, está el monitorear la utilización de procesamiento. Es decir, es importante que el administrador conozca la cantidad de procesador que un servidor está consumiendo para atender una aplicación.

Este proyecto considera importante un sistema de gestión de red centralizado (NMS Sistema de Monitoreo Global de Red) que permita la recolección de datos en un lugar estratégico mencionado anteriormente dentro de la reestructuración lógica de la red de la universidad. El cual puede ser desde una solución comercial como SolarWinds NPM, OpManager, HP OpenView hasta una solución integrada con productos de software libre como Nagios, MRTG.

a. Sistemas de Monitoreo Global de la Red

a.1 SolarWinds Orion NPM [20] [21]

SolarWinds Orion Network Performance Monitor es un sistema de gestión que permite administrar ancho de banda y fallos en la red en tiempo real directamente desde su navegador. Orion Network Performance Monitor, monitoriza y recoge datos de routers, switches, servidores, y cualquier otro dispositivo de red con capacidad SNMP. Adicionalmente, monitoriza la carga de CPU, utilización de Memoria, y espacio en disco disponible. Orion NPM es altamente escalable, capaz de monitorizar desde 10 hasta más de 10.000 nodos.

Entre los vendedores soportados por esta consola de administración se incluyen: equipos Cisco®, Foundry®, Extreme Networks®, Motorola®, ARRIS®, Linux, Solaris®, HP-UX®, AIX®, Windows® 2000, Windows 2003, y Windows XP. Esta consola de administración permite la recolección de datos estadísticos de la red de datos y la generación de alertas que potencialmente podrían causar una degradación de la red. Esta consola de monitoreo ya incluye una base de datos

de MIB que cubre la gran mayoría de dispositivos de la red. Pero para el resto de dispositivos permite recolectar información detallada de las MIBs.

Solarwinds Orion NPM Versión 9 cuenta con la herramienta Universal Device Poller, que facilita la creación de pollers a medida para monitorear cualquier dispositivo SNMP compatible que incluye MIBs. Con esto es capaz de monitorear la temperatura de un switch, el status de una batería en una UPS, etc.

La última versión de la consola de administración también permite monitorear servers e instancias de máquinas virtuales. Realizar seguimiento de la disponibilidad y rendimiento de las máquinas virtuales, incluyendo métricas de CPU, memoria y ancho de banda. Automáticamente descubre, identifica máquinas virtuales agregadas.

Con su característica de administrar los nodos de la red vía web, permite al administrador a través de la consola web:

- Agregar, borrar y modificar nodos e interfases.
- Administrar múltiples nodos simultáneamente.
- Delegar acceso a la consola web de administración.
- Asignar propiedades configurables a nodos e interfases.

Entre sus características principales están:

- Herramientas para la administración de fallos y disponibilidad.
- Monitorización de CPU, Memoria, y Espacio de disco.
- Mapas de la red.
- Eventos y Herramientas de administración de Alertas.
- Generador de informes.

Adicionalmente, la consola de administración es escalable y puede integrar los siguientes módulos, dependiendo de las necesidades o servicios que vayan surgiendo dentro de la red.

La herramienta *Solarwinds Orion NetFlow Traffic Analizer*, que le permite al administrador ver el tráfico y comportamiento de la red. Aprovechando el protocolo NetFlow de Cisco para extraer datos de equipos CISCO. Y así saber que usuarios y que aplicaciones están consumiendo el mayor ancho de banda.

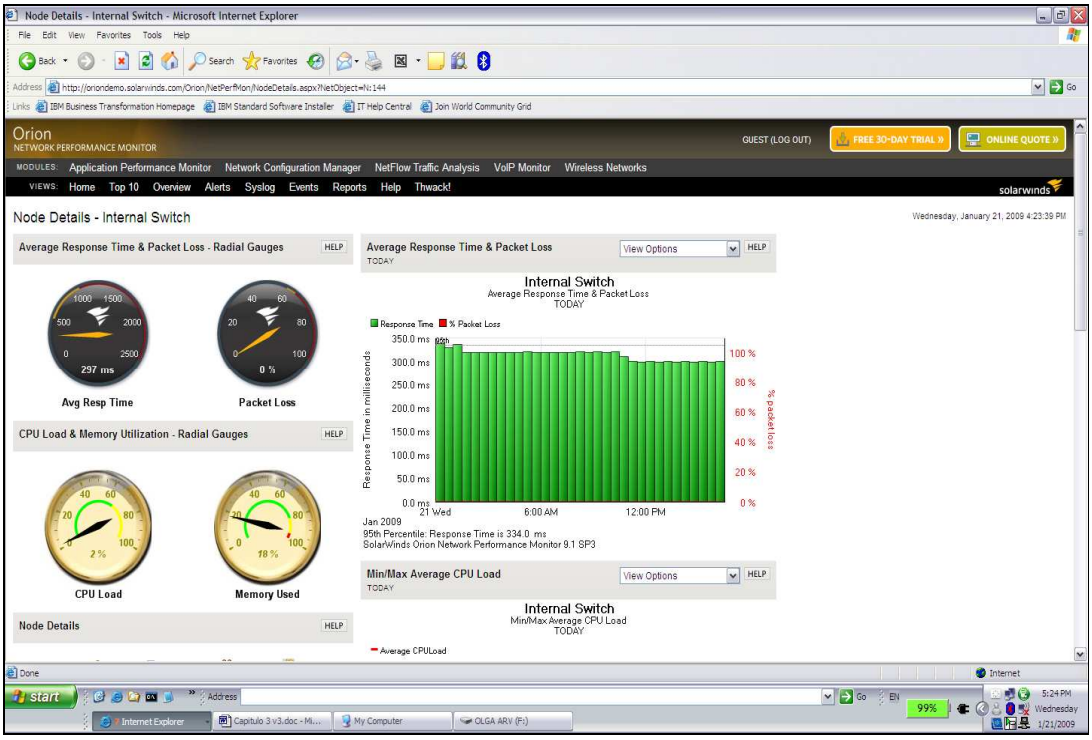


Figura 3.14 Ejemplo de monitoreo de procesos con SolarWinds Orion NPM [22]

El *Solarwinds Orion Wireless Network Monitor*, el cual es un módulo adicional para monitoreo a las redes inalámbricas.

Con el módulo *Solarwinds VoIP Monitor* permite analizar la calidad VoIP a través de los enlaces de la red, así como monitorear los sistemas y protocolos que utiliza el ambiente VoIP.

Solarwinds Orion Application Monitor es un módulo que permite extender las capacidades de monitoreo respecto a las aplicaciones, servidores y servicios.

Con el módulo Solarwinds Orion Hot Standby Engine se puede chequear constantemente la disponibilidad del sistema primario. En caso de falla, este asumirá automáticamente la función del monitoreo. Y cuando el sistema caído se recupere, "devuelve" las tareas de monitoreo al sistema original.

a.1.1 Requisitos del Sistema dependiendo de la cantidad de dispositivos

Equipo	**SL100 a SL500**	**SL200**	**SLX**
CPU	2.0 GHz	2.4 GHz	3.0 GHz
Memoria	1 GB	2 GB	2 GB
Disco Duro	1 GB	2 GB	10 GB
Software	Requerimientos mínimos		
Sistema Operativo	Windows 2003 Server (32-bit o 64-bit) incluyendo R2, con IIS instalado		
.Net Framework	.NET 3.5 Framework		
Base de Datos	SQL Server 2000 SP4 Standard o Enterprise/ SQL Server 2005 Express, Standard,/ Enterprise		

Tabla 3.4 Requerimientos mínimos del Sistema para SolarWinds Orion NPM [23]

a.2 HP Openview Network Node Manager [24] [25]

HP Openview NetWork Node Manager, proporciona un mapa de la red donde se muestra el estado de los elementos y ofrece diversas herramientas para gestionarlos.

Sus características principales son:

- Autodescubrimiento de la red.
- Visualización topológica de la red descubierta.
- Interfaz grafico de usuario.
- Gestión de eventos.
- Servicio de correlación de eventos.
- Actualización automática de estados en el mapa.
- Colecciones de datos SNMP.
- Visualización grafica de datos SNMP.

- Herramientas de gestión de fallos.
- Gestión distribuida mediante Estaciones colectoras y estaciones gestoras.
- Consolas de gestión.
- Interfaz web de usuario.

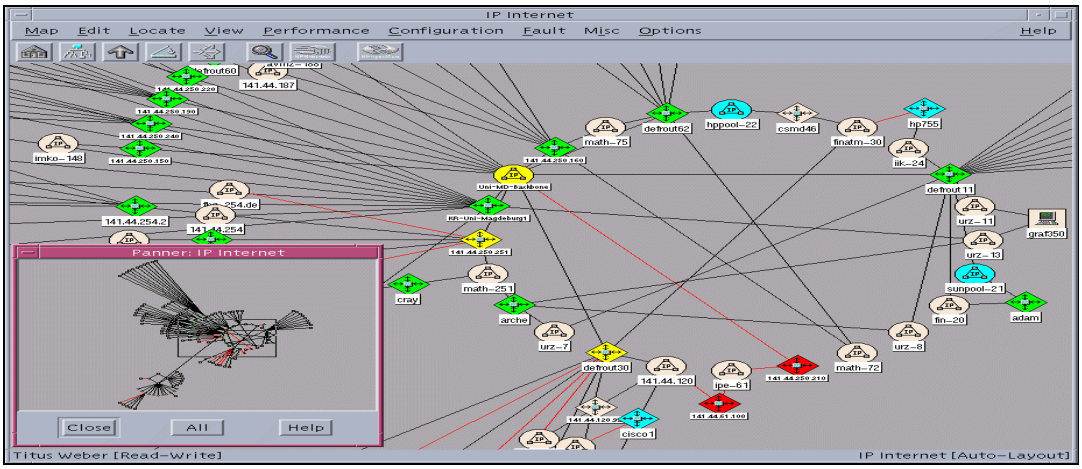


Figura 3.15 Ejemplo de monitoreo de una red con HP OpenView Network Node Manager [26]

a.2.1 Requerimientos mínimos del sistema para el software HP OpenView Network Node Manager Advanced Edition 7.5

Sistemas HP	Sistemas Sun	Sistemas Windows 2000, XP and 2003
• Servidores HP 9000 y estaciones de trabajo, incluyendo multiprocesadores HP-UX 11.0, 11i. • RAM: 1 GB. • Bit-mapped display o X-terminal. • Color graphics: 1024x768 • Resolución mínima recomendada (1280x1024). • Espacio libre en disco: 500 MB más 1 GB de Espacio swap. • LAN/Link para HP 9000. • ARPA services/9000.	• Servidores SunSPARC y estaciones de trabajo, incluyendo multiprocesadores Sun Solaris 8 y 9. • RAM: 1 GB • Bit-mapped display o X-terminal. • Color graphics: 1024x768 Resolución mínima recomendada (1280x1024. • Espacio libre en disco: 800 MB más 512 MB de Espacio swap.	• Procesador Intel® Pentium, 333 MHz o mayor. • Microsoft® Windows 2000 o XP Professional o 2003 Server system. • TCP/IP networking instalado y configurado. • RAM: 1 GB • Monitor 800x600 con tarjeta gráfica SVGA. • Espacio libre en disco: 400 MB más 512 MB espacio de archivo de paging libre. • Tarjeta adaptadora de red.

Tabla 3.5 Requerimientos mínimos del sistema para el software HP OpenView Network Node Manager Advanced Edition 7.5 [33]

a.3 OpManager [27]

Es una completa y eficiente consola de monitoreo de redes que ofrece herramientas de control y gestión combinada de redes LAN y WAN, servidores, aplicaciones, gestión de activos y análisis del tráfico de la red. Este software le permite al administrador automatizar diversas tareas de monitoreo de la red y eliminar la complejidad asociada con su administración. OpManager puede controlar en forma automática toda la red, agrupar dispositivos en mapas intuitivos, monitorear los dispositivos en tiempo real, alertar al instante sobre fallas, proporcionar informes y gráficos globales de la red.

Esta herramienta ofrece soporte para Windows y Linux. Otorga auditorias de gestión de inventario (tanto de software como hardware) de red planificado, muestra el software nuevo y el que falta, posee capacidad de adjuntar activos a las estaciones de trabajo analizadas y la capacidad de añadir manualmente el software que falta.

Con esta herramienta el administrador está en capacidad de monitorear equipos WAN como routers, y optimizar los enlaces de la red. Permite una mejor asignación de ancho de banda, resolver problemas en la red, así como planificar la capacidad para crecimientos futuros. Además de minimizar los costos de enlaces, identificar las fuentes de mucho tráfico, utilización o saturación de los mismos.

Dentro de la LAN, esta herramienta ofrece una identificación automática de los switches, su monitoreo y disponibilidad junto con sus puertos. Permite monitorear el tráfico a nivel de puerto, la asignación de los puertos del switch. Además trabaja con una herramienta a través de un árbol de expansión de cada puerto (STP: Spanning Tree Protocol), para detectar aquellos puertos que están bloqueados en el switch.

La red de la universidad está compuesta principalmente por equipos CISCO como switch de la Serie 2960, por eso es importante destacar que OpManager se

integra estrechamente con NetFlow Analyzer, un producto que ofrece supervisión de ancho de banda en base a la tecnología NetFlow de Cisco. Al utilizar ambos programas, se pueden ver automáticamente informes detallados del tráfico de interfaz de NetFlow Analyzer desde OpManager.

Con respecto al monitoreo de servidores, esta herramienta permite la visibilidad necesaria sobre la disponibilidad y rendimiento de estos equipos. Además de monitorear los servidores, se puede monitorear aplicaciones, servicios, registro de eventos, utilización de la CPU, memoria y disco, tiempo de respuestas de servidores y servicios, dispositivos no SNMP y generar amplios informes históricos de esta variada gama de monitoreos que ofrece el servicio. Entre los principales servicios que monitorea esta herramienta están: DNS, IMAP, SMTP, Echo, LDAP, Telnet, FTP, NNTP, Web, Finger, POP, WebLogic y HTTPS.

a.3.1 Requerimientos del Sistema

# de dispositivos	Procesador	RAM	Disco Duro	Sistemas Operativos Soportados
Hasta 50	1.7 GHz	1GB	20GB	Windows: 2003 Server, 2000 professional SP4, XP Professional Linux: RedHat 7.x y superiores, Debian 3.0
50-150	2.4 GHz	2GB		
150-300	3.4 GHz	2GB		
300-500	2*3.4 GHz	4GB		
501 y más	4*3.4GHz	4GB		

Tabla 3.6 Requerimientos del Sistema para la Consola de Monitoreo OpManager [28]

Figura 3.16 Ejemplo de monitoreo de los datos estadísticos del funcionamiento de un servidor con OpManager [29]

a.4 Nagios [30] [31]

Esta herramienta de software libre, escrita en C, originalmente fue diseñada para ejecutarse bajo el sistema operativo Linux. Nagios se caracteriza por su alto rendimiento y flexibilidad, además es adaptable a necesidades específicas de administración de una red.

La consola de monitoreo Nagios, permite dar seguimiento a los equipos y servicios de la red, alertando cuando existe algún evento de falla y cuando estos se solucionan. Entre sus características principales están:

- Monitorización de servicios de red: SMTP, POP3, HTTP, NTTP, ICMP, SNMP, etc.
- Monitorización de los recursos de un host: carga del procesador, uso de los discos, utilización de memoria, logs del sistema. Incluso en varios sistemas operativos, como Microsoft Windows con el plugin NRPE_NT.
- Monitorización remota a través de túneles SSL cifrados o SSH.
- Diseño simple de plugins, que permiten a los usuarios desarrollar sus propios chequeos de servicios dependiendo de sus necesidades, usando sus herramientas preferidas (Bash, C++, Perl, Ruby, Python, PHP, C#, etc.).
- Chequeo de servicios paralizados.
- Posibilidad de definir la jerarquía de la red, permitiendo distinguir entre host caídos y host inaccesibles.
- Notificaciones a los contactos cuando ocurren problemas en servicios o hosts, y cuando son resueltos (Vía email, SMS, o cualquier método definido por el usuario junto con su correspondiente complemento).
- Posibilidad de definir manejadores de eventos que se ejecuten al ocurrir algún problema en cualquier servicio o host para tener respuestas proactivas ante cualquier evento.
- Soporte para implementar hosts de monitores redundantes.
- Consola web para observar el estado de la red actual, notificaciones, historial de problemas, archivos de registros, etc.

- Soporte para bases de datos para el almacenamiento de datos externos.

La instalación y configuración completa de esta herramienta no es tan fácil, requiere un poco de aprendizaje. Pero Nagios cuenta con una documentación extensa y detallada. Con la consola web de monitorización de Nagios se puede:

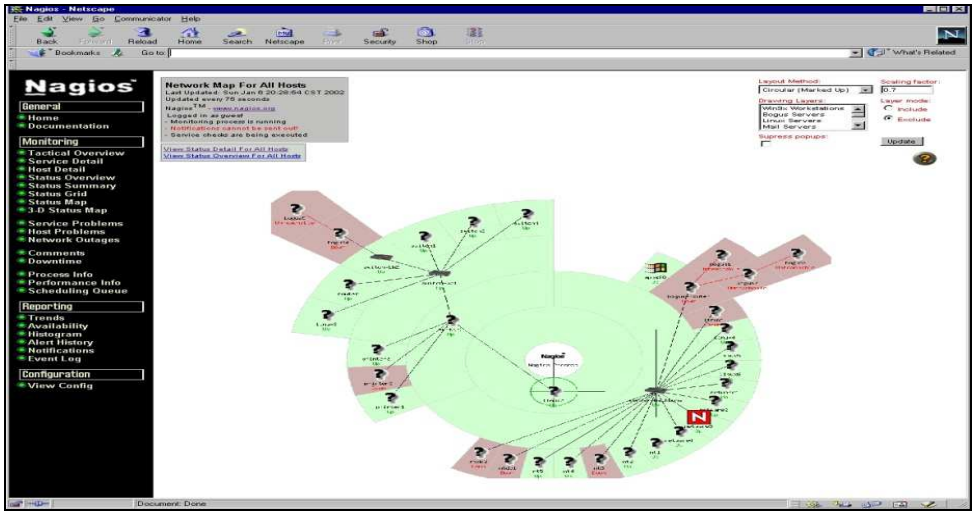


Figura 3.17 Ejemplo del estado de una red con la Consola de monitoreo Nagios [32]

- Acceder a la documentación online de Nagios.
- Obtener un resumen general del estado del sistema.
- Conocer el estado actual de todos los servicios y hosts chequeados.
- Visualizar un mapa de estado con todos los hosts.
- Visualizar un mapa en 3D.
- Obtener un resumen de todos los problemas.
- Añadir comentarios a diferentes situaciones, hosts y servicios.
- Obtener estadísticas de disponibilidad y estado de los diferentes hosts y servicios.
- Obtener listados del histórico de alertas.
- Obtener listados de notificaciones enviadas.
- Ver los ficheros de configuración y el log de eventos.
- Deshabilitar los chequeos que se crean oportunos.

- Deshabilitar los manejadores de eventos.
- Solicitar chequeo inmediato de un servicio o host.
- Planificar paradas de servicio.

a.4.1 Requerimientos del sistema para la instalación de la herramienta Nagios

Requisitos del Sistema
Máquina ejecutando el sistema operativo GNU/Linux y un compilador de C
Un web server, preferentemente Apache
Librerías gráficas GD, JPEG y PNG
SNMP (net_snmp), MySQL o PostgreSQL

Tabla 3.7 Requerimientos del Sistema para la Consola de Monitoreo Nagios

Cabe mencionar que Nagios y MRTG trabajan muy bien en conjunto. Nagios se puede utilizar para recolectar datos estadísticos de la red y MRTG para graficarlos y monitorear el desempeño de la red.

a.5 Comparación entre los Sistemas de Monitoreo Global de Red

La evaluación según un criterio propio, califica de 1 a 3 puntos, considerando a 3 como mejores características y desempeño. Esta evaluación se la ha realizado, de acuerdo al análisis de cada uno de los software, así mismo, se ha caracterizado cada uno de acuerdo a las necesidades de la UTEQ.

Consola de Monitoreo	Escalabilidad	Flexibilidad	Rendimiento	Uso de Recursos	SO	Costo
SolarWinds Orion NPM	3	3	3	2	Windows	Privado
HP OpenView NNM	3	2	2	2	Linux/ windows	Privado
OpManager	2	2	2	2	Linux/ windows	Privado
Nagios	3	3	3	3	Linux	Gratuito

Tabla 3.8 Comparación entre las Consolas de Monitoreo Global de Red

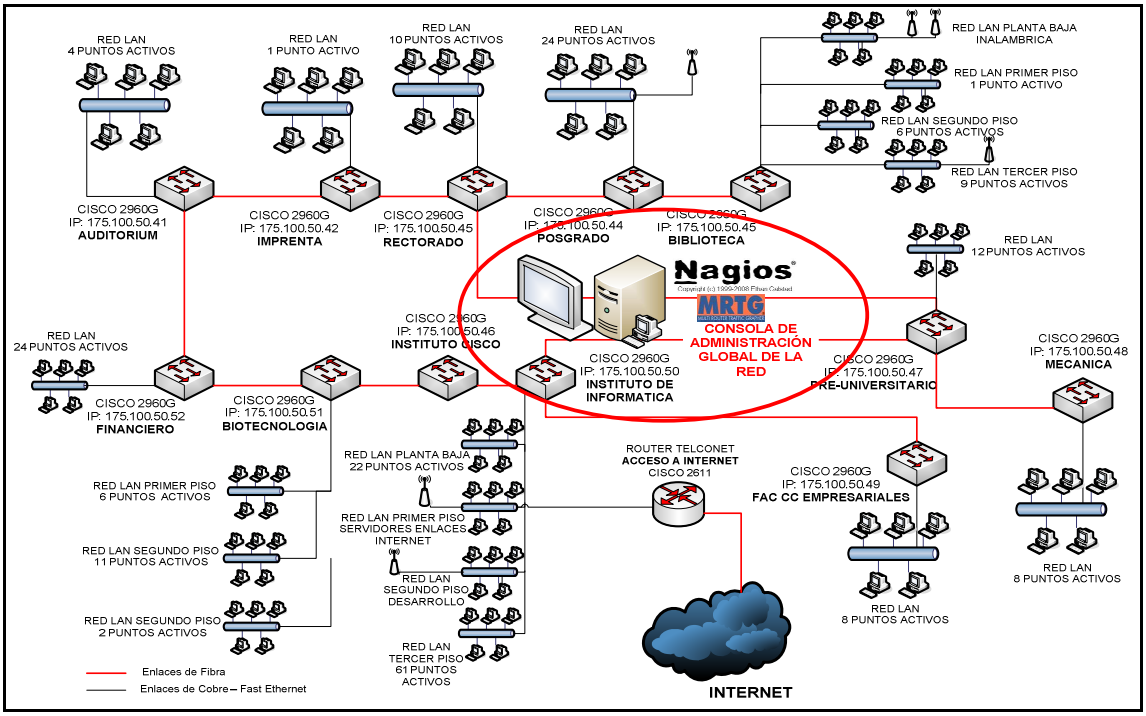


Figura 3.18 Ubicación de la Consola de Monitoreo Global de Red dentro del esquema general de la red de la UTEQ

De las características evaluadas en la tabla 3.8, se seleccionó a Nagios como la consola de monitoreo global para ser instalada en el servidor de administración y monitoreo, para trabajar en conjunto con otras herramientas de uso libre como Mrtg.

3.5.3.2 Análisis de la Información Gestionada

Una vez recolectada la información mediante la actividad de monitoreo, es necesario interpretarla para determinar el comportamiento de la red y tomar decisiones adecuadas que ayuden a mejorar su desempeño.

En el proceso de análisis se pueden detectar comportamientos relacionados con lo siguiente:

3.5.3.2.1 Utilización elevada de enlaces

Al analizar este parámetro de utilización elevada de enlaces, se puede tomar la decisión de incrementar el ancho de banda o de agregar otro enlace para balancear las cargas de tráfico. También, el incremento en la utilización, puede reflejarse como resultado de la saturación por tráfico generado maliciosamente, en este caso de debería contar con un plan de respuesta a incidentes de seguridad.

3.5.3.2.2 Tráfico inusual

El tráfico inusual, se refiere aquel que sale fuera de los patrones de aplicaciones normales que circulan por la red. Detectar este tipo de tráfico aporta elementos importantes para la resolución de problemas que pueden afectar el rendimiento de la red de la Universidad.

3.5.3.2.3 Elementos principales de la red

Los elementos principales de la red, son aquellos que transmiten y reciben más información dentro de la misma. Y por lo tanto son los que se recomienda deben ser monitoreados de manera más constante. La universidad debe ubicar cuales son los equipos más importantes de su red, porque así si se detecta un elemento que generalmente no se encuentra dentro del patrón de los equipos con más actividad, puede ayudar a la detección de posibles ataques a la seguridad de dicho equipo y de la red.

3.5.3.2.4 Calidad de servicio

Otro aspecto, es la Calidad de Servicio o QoS, es decir, garantizar, mediante ciertos mecanismos, las condiciones necesarias, como ancho de banda, retardo, a aplicaciones que requieren de un trato especial, como lo son la voz o el video.

Los switches CISCO Catalyst 2960G tanto de la capa núcleo como de la capa de distribución que componen la red de la UTEQ, cuentan con características para implementar QoS en la red. Los switches permiten una clasificación y priorización del tráfico.

3.5.3.2.5 Control de tráfico

El control de tráfico permite ver cuando el tráfico debe ser reenviado o ruteado por otro lado. Esto se debe hacer cuando se detecte saturación por un enlace, o al detectar que se encuentra fuera de servicio. En general, esto se realiza de manera automática si es que se cuenta con enlaces redundantes, como es el caso de la UTEQ, que posee un enlace redundante entre los switches del Rectorado y el Pre-Universitario.

En caso de que las acciones tomadas no sean suficientes, éstas se deben reforzar para que lo sean, es decir, se debe estar revisando y actualizando constantemente.

3.5.4 ADMINISTRACIÓN DE FALLAS [2]

Esta área de la administración agrupa las actividades necesarias para garantizar que tanto la red de la UTEQ como los equipos que la forman estén en las condiciones idóneas para prestar los servicios a los que están asignados.
Esta parte de la administración tiene como objetivo la detección y resolución oportuna de situaciones anormales en la red.

En la administración de fallos, primero, una falla debe ser detectada y reportada de manera inmediata. Una vez que la falla ha sido notificada se debe determinar el origen de la misma para así considerar las decisiones a tomar. Las pruebas de diagnóstico son, algunas veces, la manera de localizar el origen de una falla. Una vez que el origen ha sido detectado, se deben tomar las medidas correctivas para restablecer la situación o minimizar el impacto de la falla.

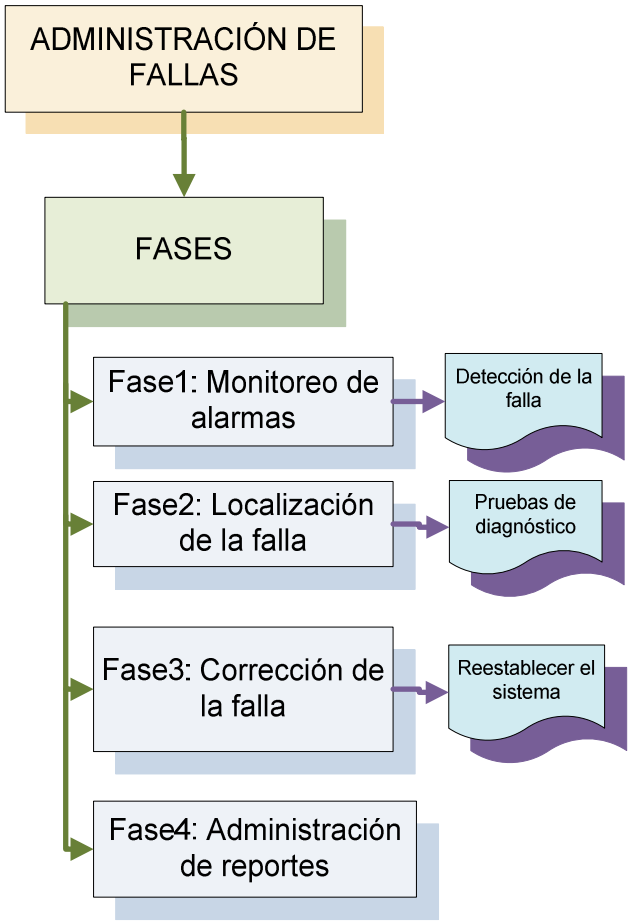


Figura 3.19 Etapas para llevar a cabo la Administración de Fallas

El proceso de la administración de fallas consiste de distintas fases. Las que se mencionan a continuación:

3.5.4.1 Fase 1: Monitoreo de Alarmas

Las alarmas son un elemento importante para la detección de problemas en la red. Es por eso que se propone contar con un sistema de alarmas, el cual es una herramienta con la que el administrador se auxilia para conocer que existe un problema en la red de la UTEQ.

Las alarmas tratan de un mecanismo que permite notificar que ha ocurrido un problema en la red. Esta propuesta se basa en la utilización de herramientas

basadas en el protocolo estándar de monitoreo SNMP, ya que este protocolo es utilizado por todos los fabricantes de equipos de red de la UTEQ.

Cuando una alarma se genera, ésta debe ser detectada en el instante de haber sido emitida para que el administrador de la red pueda atender el problema de una forma inmediata de manera proactiva, incluso antes de que los usuarios de los servicios de la red universitaria puedan percibirlo.

Las alarmas consideradas para la red de la UTEQ son caracterizadas desde dos perspectivas, su tipo y su severidad.

3.5.4.1.1 Tipo de las alarmas para la red de la UTEQ

- *Alarmas en las comunicaciones.* Son las asociadas con el transporte de la información, como las pérdidas de señal. Esta alarma se aplica para todos los elementos físicos que enlazan la red UTEQ (enlaces de fibra, de cobre e inalámbricos).
- *Alarmas de procesos.* Son las asociadas con las fallas en el software o los procesos, por ejemplo cuando el procesador de un equipo excede su porcentaje normal de utilización. Estas alarmas se aplican a los procesos que se ejecutan para los servicios que prestan los servidores y sus aplicaciones.
- *Alarmas de equipos.* Como su nombre lo indica, son las asociadas con los equipos. Una falla de una fuente de poder, un puerto, etc. Estas alarmas se activan para los equipos de interconexión de la red como el router CISCO 2600, los switches CISCO 2960G y servidores de la UTEQ.
- *Alarmas ambientales.* Son las asociadas con las condiciones ambientales en las que los equipos de la universidad operan, como las alarmas de altas temperaturas.
- *Alarmas en el servicio.* Relacionadas con la degradación del servicio en cuanto a límites predeterminados dentro de los acuerdos de servicio que plantea la institución, como excesos en la utilización del ancho de banda, peticiones abundantes de icmp.

3.5.4.1.2 Severidad de las alarmas establecidas para la red de la UTEQ

- *Crítica.* Indica que un evento severo ha ocurrido en la red universitaria, el cual requiere de atención urgente.
- *Inmediata*. Se relaciona con las fallas que afectan el funcionamiento global de la red, como un enlace importante (Ejemplo: Backbone principal de fibra) fuera de servicio. Casos que necesitan un restablecimiento inmediato por parte del personal que administra la red de la universidad.
- *Mayor.* Indica que un servicio ha sido afectado y se requiere su inmediato restablecimiento. No es tan severo como el crítico, ya que el servicio se sigue ofreciendo aunque su calidad no sea la óptima.
- *Menor.* Indica la existencia de una condición que no afecta el servicio que ofrece la red de la UTEQ pero que deben ser tomadas las acciones pertinentes para prevenir una situación mayor. Por ejemplo, cuando se alcanza cierto límite en la utilización de un enlace de la red universitaria, no indica que el servicio sea afectado, pero lo puede ser si se permite que siga avanzando.

A continuación para el caso en estudio, se utilizará el sistema de códigos descrito en la Tabla 3.9 para identificar los posibles tipos de alarmas y su severidad dentro de la red de la universidad, utilizando solo los niveles de severidad menor, mayor y crítica.

TIPOS / SEVERIDAD	AC	AP	AE	AA	AS
C	AC-C	AP-C	AE-C	AA-C	AS-C
M	AC-M	AP-M	AE-C	AA-M	AS-M
m	AC-m	AP-m	AE-m	AA-m	AS-m

AC	ALARMA EN LAS COMUNICACIONES
AP	ALARMAS DE PROCESOS
AE	ALARMA DE EQUIPOS
AA	ALARMA AMBIENTALES
AS	ALARMA EN LOS SERVICIOS

C	CRÍTICA
M	MAYOR
m	MENOR

Tabla 3.9 Sistema de Codificación Tipo de Alarma – Severidad

Este tipo de codificación gráfica basada en iniciales y colores permite al administrador de red identificar de una manera más rápida y simple el posible problema que se esté suscitando dentro de la red y la severidad del mismo. Lo cual posibilita una acción más oportuna para la solución del problema. Este sistema debe estar ligado a una comunicación con todo el personal de UTEQ para que este informado sobre la apertura y cierre de cualquier evento.

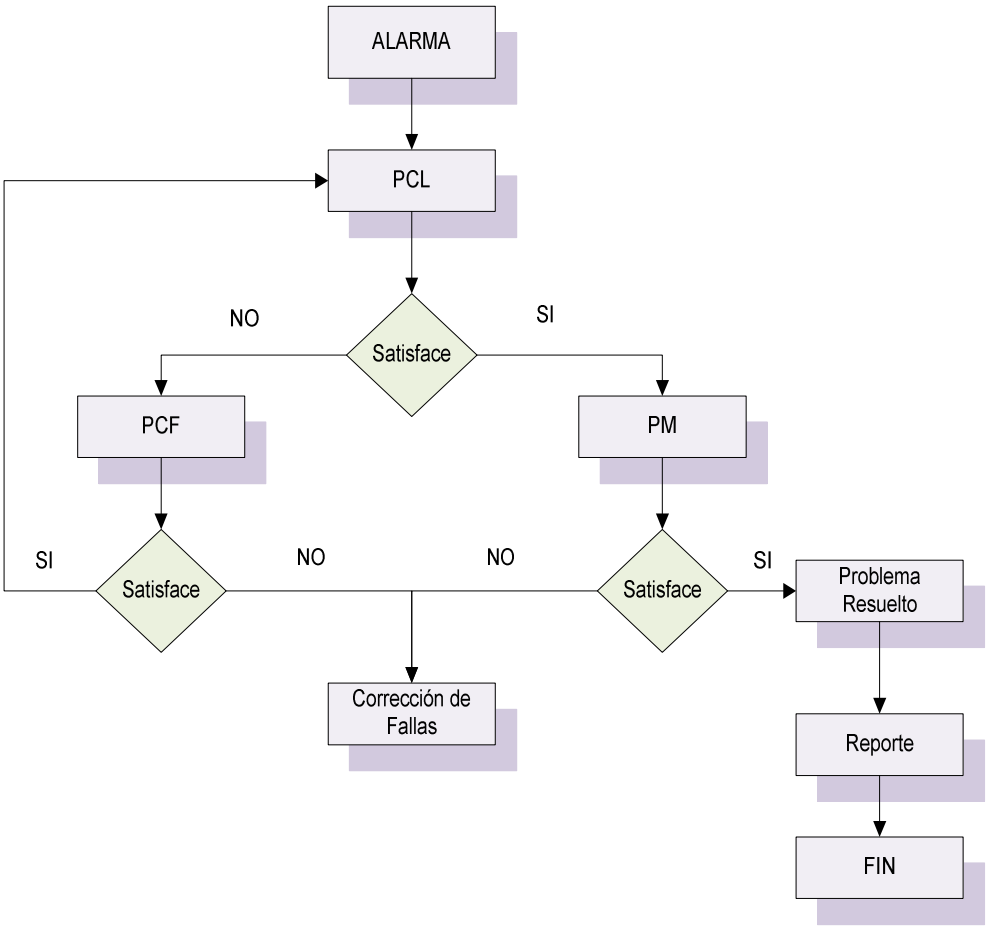
3.5.4.2 Fase 2: Localización de Fallas

Este segundo elemento de la administración de fallas es importante para identificar las causas que han originado una falla. La alarma indica el lugar del problema, pero las pruebas de diagnóstico adicionales son las que ayudan a determinar el origen de la misma. Una vez identificado el origen, se tienen que tomar las acciones suficientes para reparar el daño.

3.5.4.2.1 Pruebas de diagnóstico

Las pruebas de diagnóstico son medios importantes para determinar el origen de una falla. Algunas de estas pruebas de diagnóstico que se pueden realizar son:

- *Pruebas de Conectividad Física (PCF).* Son pruebas que se realizan para verificar que los medios de transmisión se encuentran en servicio, si se detecta lo contrario, tal vez el problema es el mismo medio.
- *Pruebas de Conectividad Lógica (PCL).* Son pruebas que ofrecen una gran variedad, ya que pueden ser punto a punto, o salto por salto. Las pruebas punto a punto se realizan entre entidades finales, y las salto por salto se realizan entre la entidad origen y cada elemento intermedio en la comunicación. Los comandos usualmente utilizados son “ping” y “traceroute”.
- *Pruebas de Medición (PM). Esta prueba va de la mano con la anterior, donde, además de revisar la conectividad, se prueban los tiempos de respuesta en ambos sentidos de la comunicación, la pérdida de paquetes, la ruta que sigue la información.*



PCL: Pruebas de Conectividad Física
PCF: Pruebas de Conectividad Lógica
PM: Pruebas de Medición

Figura 3.20 Flujo de aplicación de las Pruebas de Diagnóstico

Las pruebas de diagnóstico en primera instancia verifican las tres primeras capas del modelo OSI. El proceso lógico de implementación y desarrollo de las pruebas de diagnóstico que se propone en este trabajo es el descrito en la figura 3.20.

3.5.4.3 Fase 3: Corrección de Fallas

En esta etapa es donde se recuperan las fallas, las cuales dependen de la tecnología de red. En esta propuesta sólo se mencionan las prácticas referentes a las fallas a nivel de la red que pueden presentarse.

Entre los mecanismos más recurridos, y que en una red basada en switches, como la del presente estudio, están los siguientes:

- *Reemplazo de recursos dañados. Hay equipos de red* que permiten cambiar módulos en lugar de cambiar totalmente el equipo. Dentro de los equipos más sensibles del caso en estudio se encuentran los switches CISCO de la Serie 2960 que conforman el Backbone y la capa de Distribución de la red de la universidad. Por cuestiones de disponibilidad el presente trabajo considera la adquisición de un switch adicional para mantenerlo en estado de back-up pasivo dentro de las instalaciones de la universidad. De esta manera este equipo adicional puede asumir las funciones de cualquiera de los equipos críticos que pudiera fallar dentro de la red. También es importante considerar los módulos de comunicación de estos equipos como son los Ethernet y Seriales (tarjetas WIC), este proyecto también considera la adquisición de un módulo adicional de cada tipo.
- *Aislamiento del problema.* Aislar el recurso que se encuentra dañado y que, además, afecta a otros recursos es factible cuando se puede asegurar que el resto de los elementos de la red pueden seguir funcionando.
- *Redundancia.* Si se cuenta con un recurso redundante, el servicio se cambia hacia este elemento. En este punto, el diseño de la red de la universidad contempla la existencia de enlaces redundantes activos para el backbone de comunicaciones, garantizando de esta manera la comunicación entre los diferentes equipos de la Capa de Distribución y la Capa Núcleo en caso de que ocurra una caída de enlaces principales.
- *Recarga del sistema.* Muchos sistemas se estabilizan si son reiniciados.
- *Instalación de software.* Sea una nueva versión de sistema operativo, una actualización, un parche que solucione un problema específico, etc. Es importante contar con actualizaciones de los sistemas operativos y parches de seguridad de los equipos sensibles de la red.
- *Cambios en la configuración.* También es algo muy usual cambiar algún parámetro en la configuración del elemento de la red.

3.5.4.4 Fase 4: Administración de Reportes

Es la etapa de documentación de las fallas. Cuando un problema es detectado o reportado, se le debe asignar un número de reporte para su debido seguimiento, desde ese momento un reporte queda abierto hasta que es corregido.
Este es un medio para que los usuarios del servicio puedan conocer el estado actual de la falla que reportaron. La administración de reportes se divide en cuatro áreas, como las siguientes:

3.5.4.4.1 Creación de reportes

Un reporte es creado después de haber recibido una notificación sobre la existencia de un problema en la red, ya sea por una alarma, una llamada telefónica de un usuario, por correo electrónico o por otros medios. Cuando se crea un reporte debe contener al menos la siguiente información:

- El nombre de la persona que reportó el problema.
- El nombre de la persona que atendió el problema o que creó el reporte del mismo.
- Información técnica para ubicar el área del problema.
- Comentarios acerca de la problemática.
- Fecha y hora del reporte.

3.5.4.4.2 Seguimiento de reportes

La administración de reportes permite al administrador de la red de la UTEQ dar seguimiento de cada acción tomada para solucionar el problema sufrido en la red, y conocer el estado histórico y actual del reporte.

Para cada reporte debe mantenerse un registro de toda la información relacionada al mismo: pruebas de diagnóstico, como fue solucionado el problema, tiempo que llevó la solución, etc, y ésta debe poder ser consultada en cualquier momento por el administrador.

3.5.4.4.3 Manejo de reportes

El administrador de la red debe ser capaz de tomar ciertas acciones cuando un reporte está en curso, como escalar el reporte, solicitar que sea cancelado un reporte que no ha sido cerrado aún, poder hacer cambios en los atributos del reporte, como lo es el teléfono de algún contacto, poder solicitar hora y fecha de la creación o finalización de un reporte, etc.

3.5.4.4.4 Finalización de reportes

Una vez que el problema reportado ha sido solucionado, la persona responsable del sistema de reportes, debe dar por cerrado el reporte. Una práctica importante, es que antes de cerrar un reporte el administrador debe asegurarse que efectivamente el problema reportado ha sido debidamente corregido.

Para el presente caso de estudio se ha desarrollado el siguiente esquema de reporte manual para el manejo de fallas dentro de la red de la universidad, aunque también puede ser implementada una aplicación en software donde se registre toda la información referente a la falla.

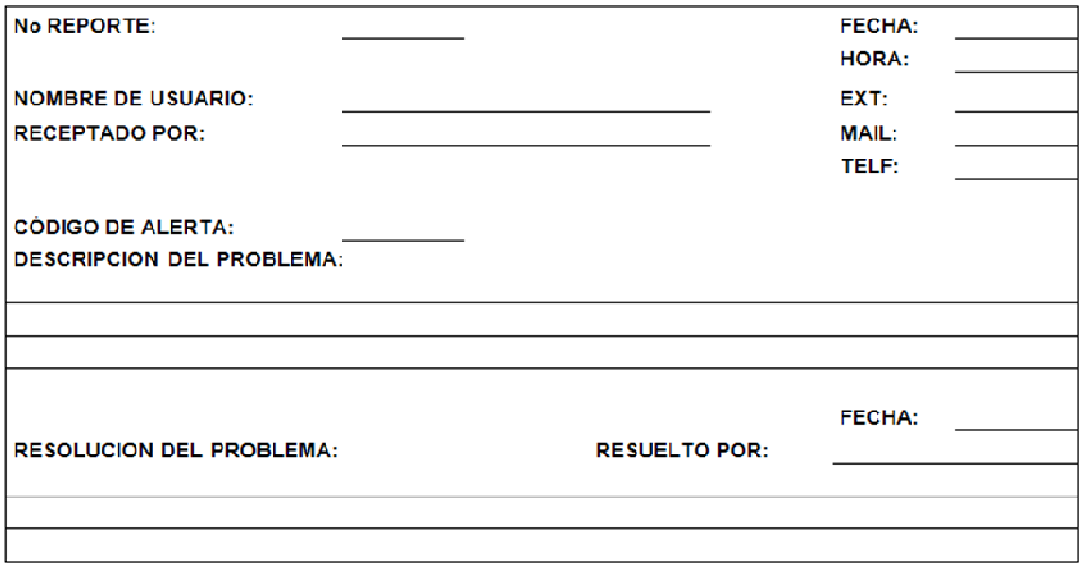


Figura 3.21 Esquema del modelo de reporte

Para finalizar este punto se presenta el esquema completo de Administración de Fallas propuesto por el Sistema de Gestión y Administración de la red en la figura 3.22.

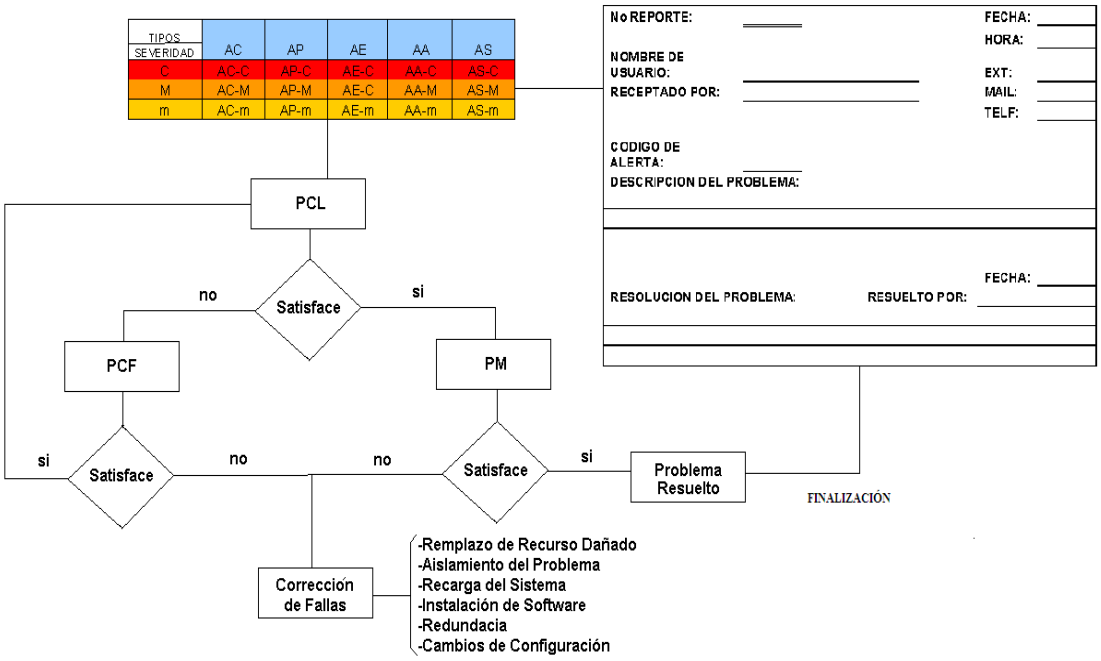


Figura 3.22 Esquema de Administración de Fallas

3.5.4.5 Políticas para instalación de los equipos de Back Up

La política, será que la instalación de equipos o elementos de red de back up sea lo más transparente posible para las actividades normales de la Universidad. El procedimiento para implementar esta política debe ser:

- Realizar respaldo de información crítica, si existe algún riesgo que esta se pierda al realizar cambios de elementos sobre un equipo.
- Definir las fechas de ejecución de las instalaciones y un estimado del tiempo de duración de la misma.
- Notificar a los usuarios de la red sobre los trabajos de instalación de los equipos de recuperación o back up.

- En lo posible respetar los plazos de tiempo establecidos para las instalaciones.
- Realizar pruebas de configuración, conectividad y funcionalidad con los nuevos equipos o elementos reemplazados.

3.5.5 ADMINISTRACIÓN DE CONTABILIDAD

Esta área agrupa las funciones y actividades para cuantificar el uso de los recursos utilizados en la prestación de los servicios, para obtener el retorno de la inversión.

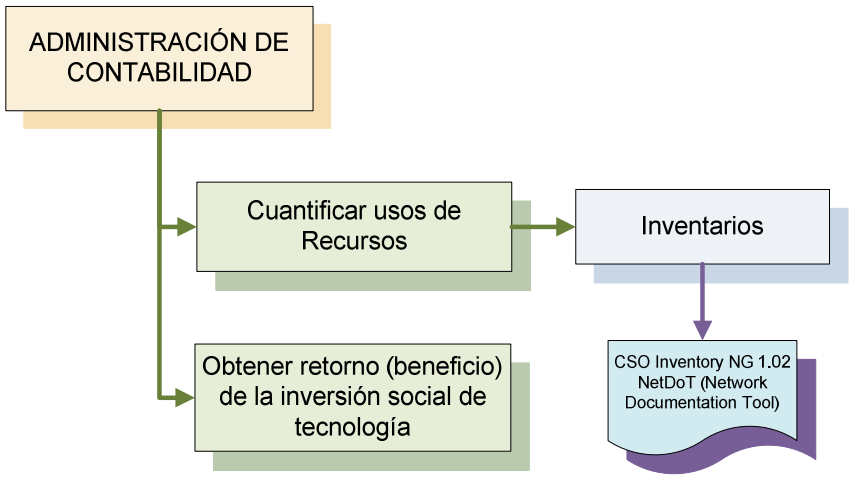


Figura 3.23 Etapas para llevar a cabo la Administración de Contabilidad

Incluye el proceso de recolección de información de los recursos utilizados por los elementos de la red, desde equipos de interconexión hasta usuarios finales. Información referente a las características de los equipos (Tipo, Modelo, Serie, Procesador, Memoria, etc.) y configuraciones de los mismos. [2]

Esto se hace con el objetivo de realizar los cobros correspondientes a los clientes del servicio mediante tarifas establecidas. Este proceso, también llamado tarificación, es muy común en los proveedores de servicio de Internet o ISP. Pero para el caso del presente proyecto, esto no es totalmente aplicable ya que la universidad tiene una finalidad y misión diferente a la de los proveedores de

servicio. Por lo que se puede tratar al mismo como un proyecto social, el cual tiene como objetivo contribuir con la visión y misión de la universidad, que son:

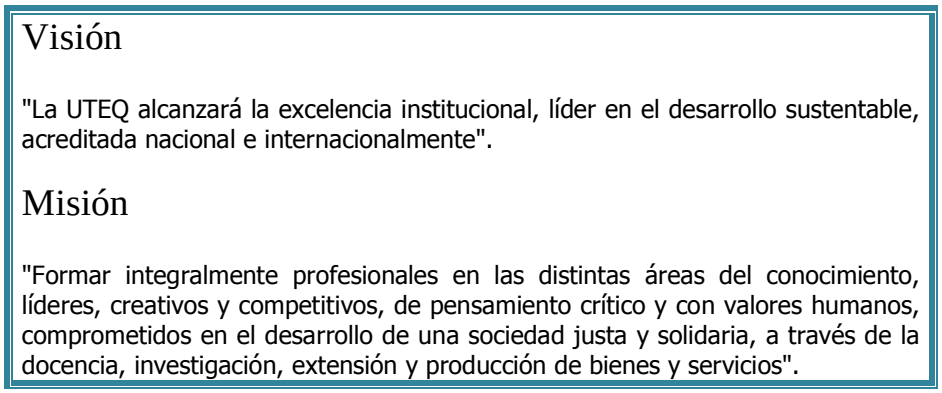


Figura 3.24 Visión y Misión de la UTEQ [34]

Por las razones explicadas anteriormente, dentro de este punto se tomará, por una parte, los costos referenciales para el funcionamiento óptimo de la red. Todo esto se detallará en el siguiente capítulo, donde se realizará un análisis de costos del proyecto para la universidad, tomando en cuenta los beneficios para la sociedad universitaria al realizar este tipo de inversión. Por otra parte, en esta área de la administración también se topa el tema de inventarios. Teniendo base en las políticas de seguridad y administración generales propuestas por el proyecto.

3.5.5.1 Inventarios [35]

Para esta actividad, se propone el uso de herramientas de software que se encargan automáticamente de inventariar en un instante los recursos informáticos de la red, ya sea este hardware o software.

Aplicar una automatización en los inventarios disminuye el coste de la obtención de información. Además, los datos sobre el nivel de uso de las aplicaciones permiten decidir sobre compras de licencias o renovación de mantenimientos.

Respetando las políticas para la seguridad de la red que se mencionan en el área de administración de seguridad, los inventarios facilitan la detección de configuraciones inadecuadas, antivirus sin actualizar o programas no autorizados, minimizando los huecos de seguridad y asegurando la conformidad del parque frente a posibles auditorías. Además, este tipo de herramientas le permite al administrador de la red y al personal técnico aumentar su eficacia al evitar desplazamientos innecesarios, e interrupciones a los usuarios.

A nivel de la institución, le permite aumentar su productividad**,** ya que los usuarios de la red ven cómo se minimizan el número de incidencias y el tiempo medio de resolución de las mismas.

Los inventarios permiten tener documentada toda la información detallada de la red de datos; información tal como: topología, esquemas de direccionamiento, contactos de proveedores, contactos de técnicos y reportes.

Una herramienta que facilita el proceso de documentar la red es NetDoT (*Network Documentation Tool*), que conforma un utilitario más de la lista de aplicaciones de código abierto para plataformas UNIX. [36]

Otra herramienta también de uso gratuito es *OCS Inventory NG 1.02 (Open Computer and Software Inventory Next Generation)*, la cual permite al administrador tener un seguimiento de todo el hardware y software instalados en la red. Esta aplicación detecta todos los dispositivos de red como switch, router, impresoras, etc, tomando datos de MAC y direcciones IP y permitir al administrador clasificarlos si lo desea. Para más detalles sobre el tipo de información que recolecta esta herramienta referirse al ANEXO H. [37]

Para la administración de la red de la UTEQ se propone un sólo un equipo dedicado, donde se instalarán el software de gestión recomendados. Este equipo, tiene las siguientes características:

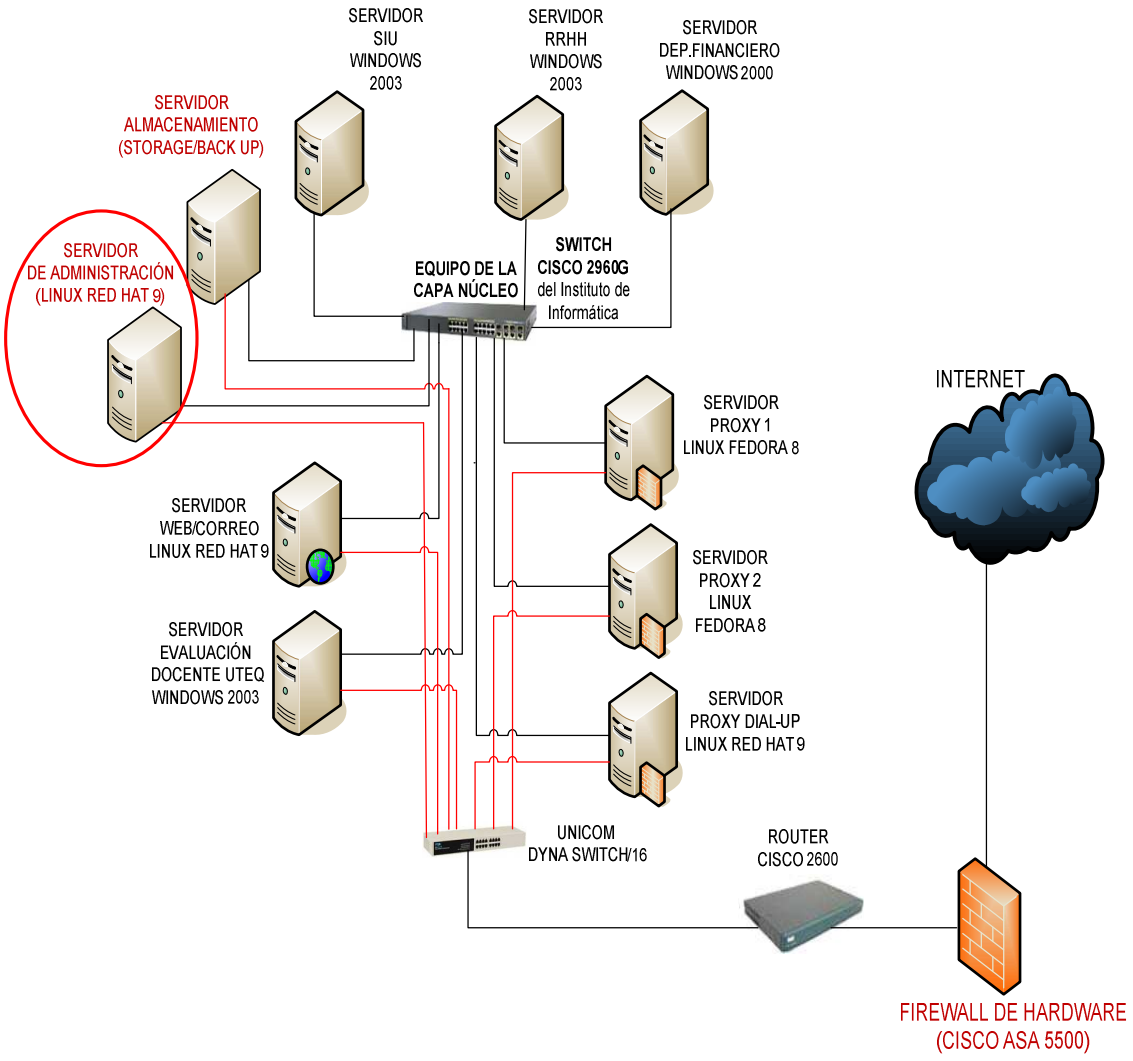


Figura 3.25 Ubicación del Servidor de Gestión

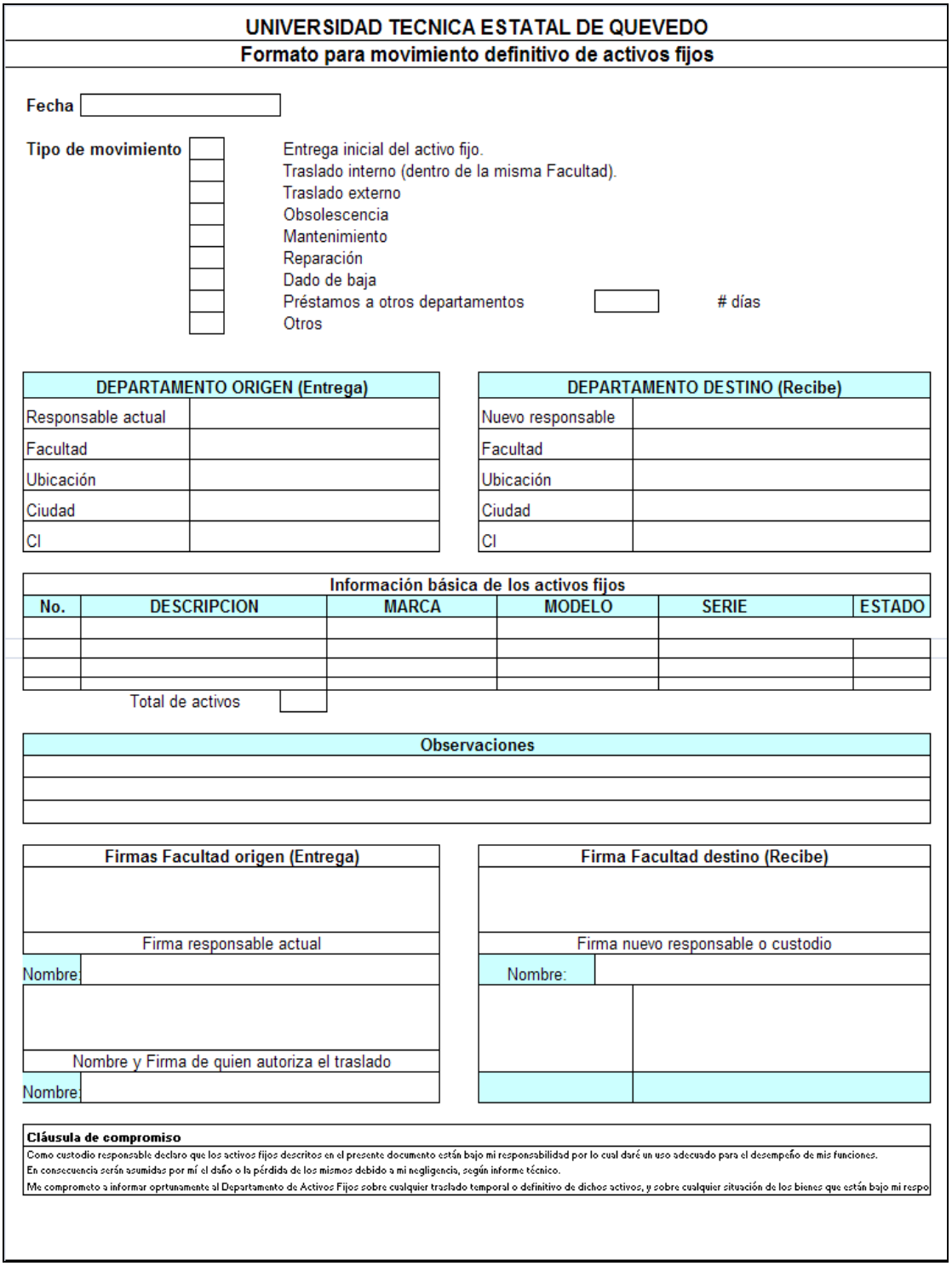
Servidor	Tipo	Procesador	RAM	Disco Duro
Gestión y Administración	CLON	INTEL CORE 2 QUAD Q8200 2.33GHZ	4 GBytes	1 disco de 500 GBytes

Tabla 3.10 Característica del Servidor de Gestión de Red

CARACTERÍSTICAS DEL SERVIDOR DE GESTIÓN	
Case	CASE ALTEK 5805 COMBO
Motherboard	INTEL DG41TY C2Q,1333GHZ,DDR2,V,S,R
Procesador	INTEL CORE 2 QUAD Q8200 2.33GHZ
Memorias	KINGSTON 2GB PC-667
Disco Duro	500GB SAMSUNG SATA 7200RPM
Teclado/mouse	TECL. GENIUS TTLM PRO + MOUSE MET
Periféricos	GENIUS SW 2.1 850 FLAT BLACK
Monitor	AOC 19" 913FW LCD
Unidad CD/DVD	Unidad DVD - CD ROOM LG negro

Tabla 3.11 Servidor de Gestión de Red

Dentro de los inventarios, además del software y hardware se propone formatos que son muy útiles para el apoyo de los sistemas y del trabajo del administrador para tener un control y seguimiento del parque informático de la Universidad.



UNIVERSIDAD TECNICA ESTATAL DE QUEVEDO

Formato para movimiento definitivo de activos fijos

Fecha

Tipo de movimiento

- Entrega inicial del activo fijo.
- Traslado interno (dentro de la misma Facultad).
- Traslado externo
- Obsolescencia
- Mantenimiento
- Reparación
- Dado de baja
- Préstamos a otros departamentos # días
- Otros

DEPARTAMENTO ORIGEN (Entrega)	
Responsable actual	
Facultad	
Ubicación	
Ciudad	
CI	

DEPARTAMENTO DESTINO (Recibe)	
Nuevo responsable	
Facultad	
Ubicación	
Ciudad	
CI	

Información básica de los activos fijos

No.	DESCRIPCION	MARCA	MODELO	SERIE	ESTADO

Total de activos

Observaciones

Firmas Facultad origen (Entrega)
Firma responsable actual
Nombre
Nombre y Firma de quien autoriza el traslado
Nombre

Firma Facultad destino (Recibe)	
Firma nuevo responsable o custodio	
Nombre:	

Cláusula de compromiso

Como custodio responsable declaro que los activos fijos descritos en el presente documento están bajo mi responsabilidad por lo cual daré un uso adecuado para el desempeño de mis funciones.
En consecuencia serán asumidas por mí el daño o la pérdida de los mismos debido a mi negligencia, según informe técnico.
Me comprometo a informar oprtunamente al Departamento de Activos Fijos sobre cualquier traslado temporal o definitivo de dichos activos, y sobre cualquier situación de los bienes que están bajo mi respo

Figura 3.26 Formato de Movimientos de Activos

Instituto de Informática

SOLICITUD DE ACCESOS A LA RED INTERNA DE DATOS Y SISTEMAS

Fecha de la Solicitud: _____ Solicitud No: _____

LLENAR TODOS LOS DATOS DEL USUARIO

Nombres Completos: _____ Campus: _____

Apellidos Completos: _____ Cargo Actual: _____

Facultad _____ Cédula de Identidad: _____

LLENAR SOLO SI NECESITA USUARIO DE RED, CORREO ELECTRONICO E INTERNET

1. Usuario de Red. ☐ 4. Acceso a Internet ☐

2. Correo Electrónico Interno ☐ 5. Acceso a MSM Messenger ☐

3. Correo Electrónico Externo ☐ 6. Acceso para VPN ☐

PERFIL

Indicar Perfil/es _____

AUTORIZACIONES

_____ _____

Rector de la Facultad Solicitante **Usuario Solicitante**

DATOS DE USO INTERNO PARA LA ADMINISTRACION DE SISTEMAS

Fecha de cumplimiento: ☐☐☐

Login para Acceso : _____ Nombre de Usuario: _____

_____

Administrador del Departamento de IT

Figura 3.27 Formato de Solicitud de Acceso

UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO

FORMATO PARA INVENTARIO DE ACTIVOS DE LA RED

Información Personal

NOMBRES:	APELLIDOS:	# DE EMPLEADO:	STATUS LOGÍSTICO:	PAÍS:
_____	_____	_____	_____	_____

Información del Activo

TIPO DE MÁQUINA:	MODELO DE MÁQUINA:	SERIE DE LA MÁQUINA:	DESCRIPCIÓN DEL ACTIVO:	TIPO DE USO:
_____	_____	_____	_____	_____

LOCALIDAD DEL ACTIVO: _____

TIPO DE EQUIPO: _____

NOTA DE ENTREGA: _____

CONDICIÓN DEL ACTIVO: _____

Información de Configuración de Hardware

PROCESADOR DE PC:	VELOCIDAD DE PC:	MEMORIA DE PC:	NÚMERO DE SERIE FDD:
_____	_____	_____	_____

Drive 1: ESPACIO TOTAL:	ESPACIO DISPONIBLE:	HDD Parte #:	HDD NÚMERO DE SERIE:
_____	_____	_____	_____

CD-ROM Parte #:	CD-ROM Serial #:	DIRECCIÓN ADAPTADOR DE Ethernet:
_____	_____	_____

DIRECCIÓN FÍSICA DEL EQUIPO: _____

Información de Configuración de Software

SISTEMA OPERATIVO: _____

PLATAFORMA: _____

SOFTWARE PRINCIPAL: _____

NIVELES DEL SOFTWARE: _____

Stacked (Y/N): _____

LICENCIA DE LA MÁQUINA: _____

Figura 3.28 Formato de Inventario

3.5.6 ADMINISTRACIÓN DE SEGURIDAD [38]

La administración de seguridad, se vuelve cada día más importante en el fin de salvaguardar la confidencialidad y la privacidad de la información de una institución.

Los métodos para garantizar la seguridad son variados que van desde diversos programas, hasta hardware especializados que de alguna manera cubren los huecos de seguridad que se pueden generar en una red. Por eso es necesaria una buena gestión de la seguridad de la red para reducir las vulnerabilidades del sistema y poder estar prevenidos ante eventuales ataques.

La UTEQ debe de entrelazar dos aspectos importantes con respecto a la seguridad: permitir libertad para experimentar procesos sobre redes y, salvaguardar toda la información crítica de la misma.

Para esto, las políticas de seguridad tanto para prevención y respuesta ante ataques, se deben diseñar sectorizando y discriminando posibles escenarios y las necesidades de incrementar o disminuir la seguridad. Sin olvidar los objetivos básicos de la seguridad en redes, esto es: Integridad, confidencialidad y disponibilidad de la información.

En la parte inicial de este capítulo se proclamó de manera global la Política de Seguridad que se va a seguir, ahora es indispensable definir la misma, que esencialmente es el conjunto formal de reglas que resumen cómo el administrador protegerá la Intranet y sistemas de la universidad, para brindar a sus usuarios confiabilidad y disponibilidad.

La figura 3.29 muestra el perímetro de seguridad que se establece para la Intranet.

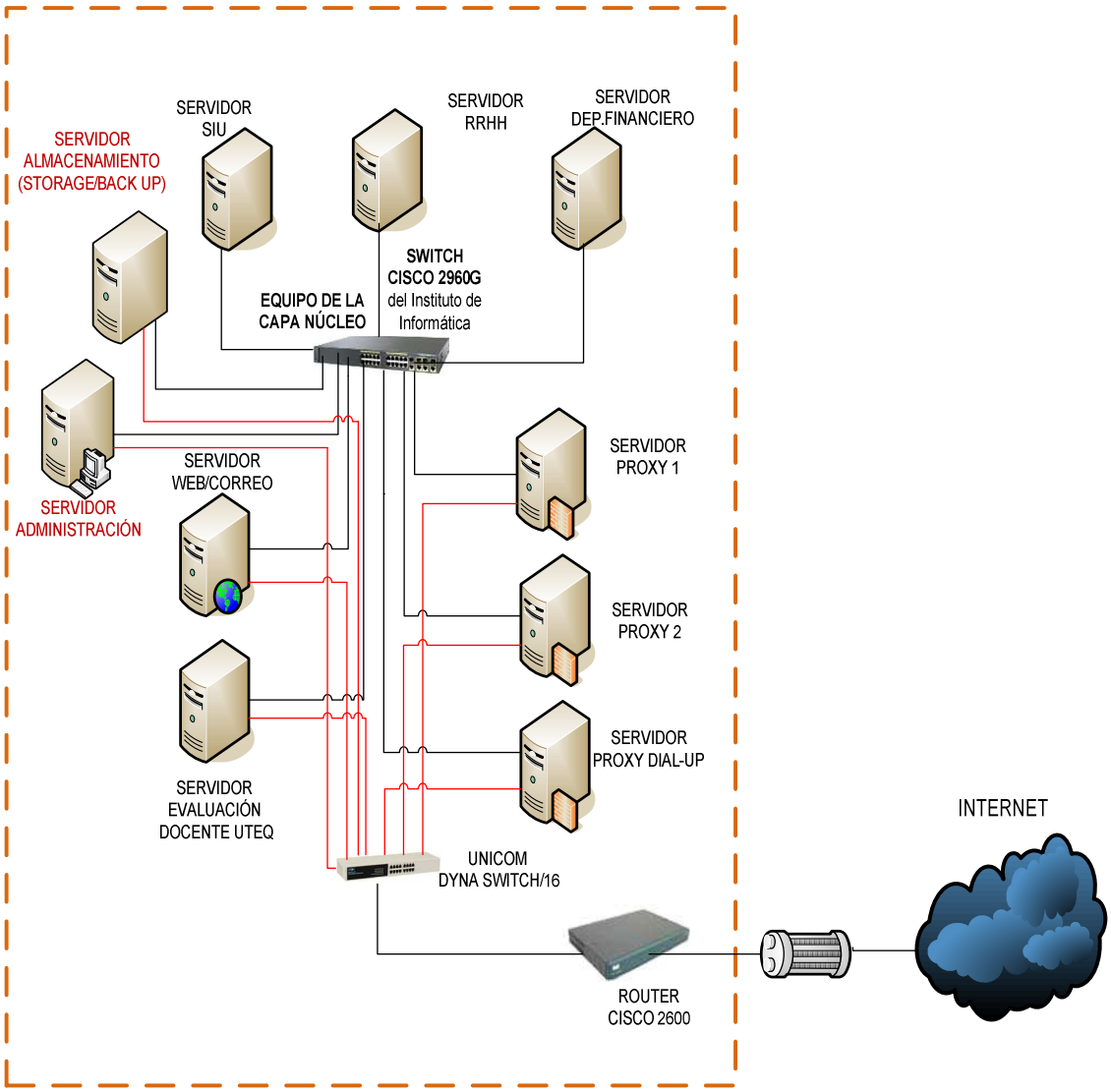


Figura 3.29 Perímetro de Seguridad de la Intranet

El perímetro de seguridad que se muestra en la figura 3.29 se basa en los tipos de ataques que pueden sucederse; estos ataques pueden generarse tanto en el interior como en el exterior de la red.

En función del perímetro de seguridad se definen dos tipos de políticas: Política Interna y Política Externa.

3.5.6.1 Definición de la Política Interna de Seguridad para la UTEQ

Política: **"**Organización de la Intranet Universitaria para evitar ataques internos".
Propósito: Evitar ataques por parte de los usuarios internos de la red, estos ataques pueden ser: DoS (Denegación de Servicio), trap-door (Puerta Trasera), Spoof (engaño), PoD (Ping de la Muerte), inundación SYN, etc. Todos estos ataques provocan la "negación de servicio" de los servidores y recursos de la red que ofrecen el servicio de acceso.
Cobertura: Esta política se aplicará sobre los usuarios internos de la red y dispositivos presentes al interior del perímetro de seguridad.
Cumplimiento: Se considera el cumplimiento de la política interna en el uso adecuado de los recursos de la red por parte de los usuarios internos de la red, el tráfico interno será monitoreado por el administrador de red.
Procedimiento: Las políticas internas de seguridad se cumplirán mediante la organización adecuada de personal interno de la institución y dispositivos de la Intranet y mecanismos de seguridad.

- *Organización del Personal Interno:* Es indispensable capacitar a los usuarios internos de la red en el uso de las tecnologías de información; se deberá asegurar que todos los usuarios de la Intranet conozcan los riesgos de seguridad y las consecuencias de no respetar la política de seguridad.

  Cada usuario debe conocer los riesgos por confidencialidad de la información propia de la Intranet, definición de responsabilidades, reconocimiento de áreas, servicios y aplicaciones restringidas (tráfico P2P, páginas Web permitidas, etc.), conocimiento de los requisitos de seguridad organizacional, responsabilidades legales y correcto uso de las instalaciones.

  El personal de administración de la red es el responsable en la creación de las cuentas de acceso al sistema (*user name-password*) en servidores, configuración de acceso en sus respectivas estaciones de trabajo,

respaldo de información generada por usuario retirado y eliminación de esas cuentas.

- *Organización de los Dispositivos:* Esta organización tiene que ver con el aspecto de la seguridad física de la red, que comprende el acceso físico a los racks de comunicaciones, servidores, consola de trabajo, etc.

  En el laboratorio de informática, donde se encuentran todos los equipos de core y servidores deben tener acceso restringido; deben ser protegidos en cuanto a acceso (dispositivos de autenticación en la puerta) y respetar las condiciones a favor de los equipos (temperatura, humedad, etc.), instalaciones y respaldos de energía eléctrica. Además debe definirse celosamente los lugares donde se guardarán los respaldos de la información.

  Todos los servidores y dispositivos de red deben estar dentro de un solo cuarto al cual se lo denominará “cuarto de telecomunicaciones”, a excepción de los equipos de la red inalámbrica, que necesariamente deben estar en instalaciones exteriores protegidas. Esto se aplica para todas las facultades de la UTEQ.

- *Organización Lógica de la Seguridad Interna:* En esta parte, en primer lugar se aprovecharán las configuraciones de seguridad presentes en las características de los equipos.

La tabla 3.12 muestra los parámetros a configurarse en cada elemento de la infraestructura de red, adicionalmente se indica la ventaja que se obtiene al configurar tales características.

Elemento	Configurar:	Ventajas
Switches de Capa Distribución	✓ IDS (Sistema de detección de Intrusos) ✓ Segmentación de la red en VLANs. ✓ Métodos de autenticación. ✓ Tecnologías de encriptación de datos y NAC (*Network Admisssion Control*: Control de Admisión a la Red) basada en usuarios, puertos y deirecciones MAC.	✓ El uso de ACL (Lista de Control de Acceso) con filtrado por direcciones MAC, direcciones IP o puertos TCP/UDP.
Switch de Capa Núcleo	✓ IDS (Sistema de detección de Intrusos) ✓ Segmentación de la red en VLANs. ✓ Métodos de autenticación. ✓ Tecnologías de encriptación de datos y NAC (*Network Admisssion Control*: Control de Admisión a la Red) basada en usuarios, puertos y deirecciones MAC.	✓ El uso de ACL (Lista de Control de Acceso) con filtrado por direcciones MAC, direcciones IP o puertos TCP/UDP.
Servidores	✓ Se hace un control a nivel de aplicación, mediante la gestión de usuarios y acceso remoto. ✓ Casos particulares como: encriptación Web (SSL, SHTTP, certificados digitales) en Web-Hosting si lo requiere; seguridad e-mail (PEM, PGP, MIME-certificados, etc).	✓ Dar acceso al servidor de administración para los supervisores técnicos desde sus estaciones de trabajo.

Tabla 3.12 Configuraciones de seguridad

3.5.6.2 Definición de la Política Externa de Seguridad para la UTEQ

Política: **“**Controlar el tráfico entrante desde Internet y de los usuarios externos para evitar ataques externos”.

Propósito: Evitar ataques externos tales como: ping de la muerte, virus, gusanos, caballos de Troya, spoof (engaño), spam, etc. que pueden provocar la “negación de servicio” de servidores y recursos de la red.

Cobertura: Esta política se aplicará en el borde del perímetro de seguridad.

Cumplimiento: Se considera como cumplimiento de la política externa el efectivo monitoreo y notificación de ataques; estas notificaciones serán generadas por el dispositivo de seguridad presente en el borde del perímetro.

Procedimiento: Las políticas externas de seguridad se cumplirán mediante la configuración adecuada de un dispositivo de seguridad en el borde del perímetro.

Los dispositivos de seguridad en los bordes suelen ser a nivel de hardware y software. Se considera mejor un dispositivo a nivel de hardware para evitar introducir mayores retardos en la red.

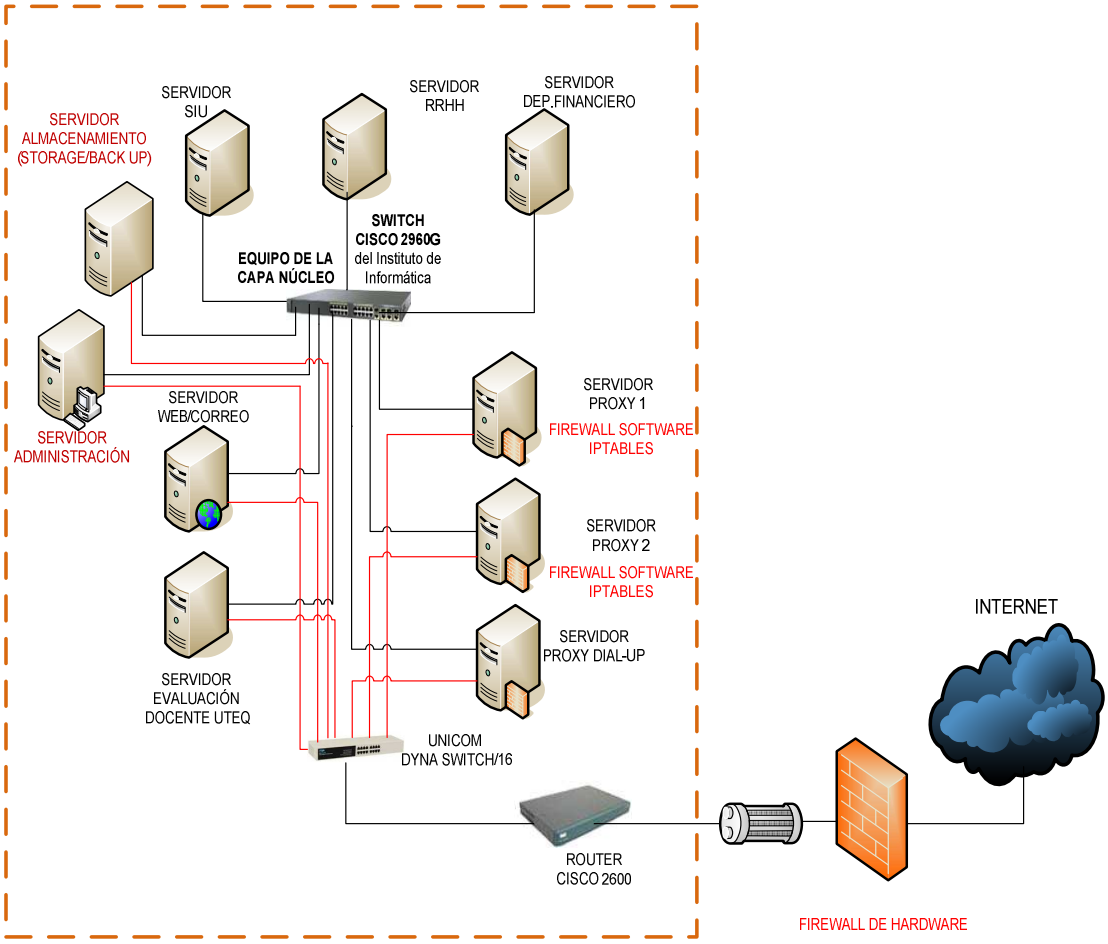


Figura 3.30 Esquema de seguridad de borde

El dispositivo, a nivel de hardware, debe poseer características de *firewall* para que permita bloquear puertos claves como:

- Puertos DNS (53/udp) en servidores que no son DNS.
- Transferencias de zonas DNS (53/tcp) excepto para DNSs secundarios.

- LDAP (389/tcp y 389/udp).
- Los puertos SMTP (25/tcp).
- POP (109/tcp y 110/tcp) e IMAP (143/tcp) en máquinas que no son servidores de correo.
- FTP (21/tcp), HTTP (80/tcp) y SSL (443/tcp), etc.

3.5.6.3 Mecanismos de Seguridad

Al momento, la UTEQ cuenta con un filtraje de direcciones a través de IPTable. Los demás son seguridades básicas. El filtraje IPTable se debe mantener a pesar de que los mecanismos recomendados sean implantados, este trabajará como un Firewall de software para dar redundancia y que no exista punto de fallo, como se muestra en la Figura 3.30.

3.5.6.3.1 Mecanismos de seguridad recomendados

Dada la infraestructura montada sobre la universidad, estandarizada equipos de acceso y distribución CISCO, se aconseja mantener esta línea y los equipos que se recomiendan se instalen serán de esta compañía. Como agregado al diseño, se va a recomendar la utilización de un software de seguridad corporativo.

a. Hardware

Los mecanismos físicos se vuelven importantes cuando los servidores dedicados tienen demasiados servicios corriendo y por ende el sistema se vuelve lento. Ante un ataque y eventual caída de este servidor, se perdería la protección del resto de la red, por tal motivo siempre es necesario mantener la seguridad con un equipo exclusivo dedicado y adicionalmente a esto, la vigilancia a través de un software especializado. Aquí se presentan 3 opciones de firewall para ser implementadas.

Características	CheckPoint Nokia IP390	CISCO ASA 5520 Adaptive Security Appliance	FortiGate-300A
Imagen			
Marca	NOKIA	CISCO	FORTINET
Usuarios	Sin restricciones	Sin restricciones	Sin restricciones
Funcionalidad	✓ FW (FireWall) ✓ VPN(Virtual Private Network) ✓ IPS(Intrusion Prevention System) ✓ AV(AntiVirus) ✓ TS(Traffic Shaping)	✓ FW (FireWall) ✓ VPN(Virtual Private Network) ✓ IPS(Intrusion Prevention System) ✓ AV(AntiVirus) ✓ WF(Web Filtering) & AS(AntiSpam) ✓ TS(Traffic Shaping)	✓ FW (FireWall) ✓ VPN(Virtual Private Network) ✓ IPS(Intrusion Prevention System) ✓ AV(AntiVirus) ✓ WF(Web Filtering) & AS(AntiSpam) ✓ TS(Traffic Shaping)
Interfaces de Hardware	4 10/100/1000 más 4 opcionales 10/100/1000	4 10/100/1000 y 1 10/100 Ethernet	4 10/100 y 2 10/100/1000 Ethernet
Sesiones concurrentes	N/A	280,000	400,000
Túneles VPN	N/A	750	1500
Rendimiento (IPSec,3DES)	600 Mbps	225 Mbps	120 Mbps
Rendimiento de Firewall	3 Gbps	450 Mbps	400 Mbps
Precio de lista (USD)	$ 6,995	$ 7,995	$6,495

Tabla 3.13 Comparación de firewalls de hardware [39]

De las 3 opciones presentadas anteriormente, se escogió la de CISCO, porque cumple todos las funcionalidades de seguridad que busca la red de la UTEQ y con buenas características de rendimiento en cuanto a velocidades de Firewall y además continua con la línea de equipos de core y distribución que posee la universidad en la actualidad. De esta manera, se va a recomendar el siguiente equipo:

a.1 Cisco ASA 5520 Adaptive Security Appliance

Cisco ASA 5520 Adaptive Security Appliance, que es un Firewall basado completamente en hardware, que incluye un sistema operativo propietario de Cisco, con el cual se segmenta la red interna para aislar los equipos con características y requerimientos de seguridad diferentes como es el caso de los servidores de Internet e Intranet.

Este equipo, que se detalla en el ANEXO B9, se colocará como protección en el acceso a la Intranet. Así se tendrá protección ante eventuales ataques desde fuera del perímetro de la red de la UTEQ. Con este equipo, nos enfocamos sobre las conexiones que se hacen desde el Internet, así podemos bloquear intensiones de acceso, repudio, fraude, suplantación de identidad, etc. Este equipo será instalado tal como se detalla en la figura 3.31. Este equipo se ha escogido por tres razones fundamentales:

- El convenio con la Academia CISCO la cual proveerá el soporte necesario para cualquier problema que presente el equipo.
- Todos los equipos de core y distribución de la red, son de la línea CISCO y se prefiere mantener la misma línea para tener uniformidad en los equipos y en la administración de la red.
- Se necesita un equipo que soporte Gigabyte Ethernet para los enlaces de fibra, y este equipo se adapta fácilmente a estos requerimientos.

Por lo demás, este equipo cuenta con las características necesarias que un equipo de mediana empresa debe tener, los cuales son:

- Formación de VPNs[13] y hardware acelerador de servicios.
- Inspección de protocolos (DNS, ICMP, SNMP, FTP, http, etc.).
- Ofrece Servicios Anti-X contra amenazas y realiza un control de contenidos de Internet con las completas funciones antivirus, antispyware, bloqueo de

[13] VPN. Redes Privadas Virtuales. Son túneles que se forman en el Internet, permitiendo proteger información de datos que están circulando por redes públicas.

archivos, antispam, antiphishing, bloqueo y filtrado de URL y filtrado de contenidos.

- Provee servicios de firewall para las capas del 2 al 7 del modelo OSI.
- Ofrece características de calidad de servicio.
- Ofrece completos servicios de administración y supervisión de dispositivos.
- Ofrece menores costos de instalación y operación.

b. Software

Primero, se presenta una tabla comparativa de los antivirus corporativos más seguros según la red mundial Internet, con su respectiva valoración (Tabla 3.14). La evaluación en la valoración según un criterio propio, califica de 1 a 10 puntos, considerando a 10 como el antivirus con mejores características y funcionalidades para ser propuesto en la implementación del presente proyecto.

Para complementar la acción del equipo de seguridad CISCO ASA 5520, se debe tener una herramienta en software que nos permitan un control centralizado, en tiempo real y que garantice la prevención y eliminación de cualquier tipo de amenaza que sea compatible con las versiones de Linux que maneja la UTEQ.

Por este motivo y según el cuadro de evaluación de la tabla 3.14 se ha escogido al antivirus McAfee LinuxShield, este antivirus ofrece una interfaz remota simple, con bajo consumo de memoria en las estaciones de trabajo, tiene un potente detector de acceso en tiempo real y su costo nos favorece para la implantación de licencias en todo los equipos de la red.

Este antivirus debe ser instalado en el servidor PROXY de la red de la UTEQ, para mantener una estructura lógica adecuada y organizada, separando servicios de las herramientas de monitoreo y prevención.

Antivirus	Protección	Número de licencias	Tiempo de duración	Costo	Valoración
AVG Network Edition	✓ Antivirus. ✓ Antispyware. ✓ AntiRootkit[14]. ✓ Protección contra sitios Web maliciosos. ✓ Firewall por maquina.	200	2 años	$ 4993	8
Symantec Business Pack	✓ Tratamiento proactivo a detección de intrusos. ✓ Antivirus. ✓ Detección de intrusos. ✓ Firewall. ✓ Control de aplicaciones y dispositivos. ✓ Administrada por un solo agente y una sola consola remota. ✓ Control de acceso a la red.	25	2 años	$ 818	**7**
MCAFEE Linux Shield	✓ Control de acceso en tiempo real contra intrusos. ✓ Proveo un escaneo Heurístico basadas en reglas que permiten detectar variantes de virus o intrusos. ✓ Provee escaneo ✓ Detección y bloqueo de amenazas escondidas en archivos. ✓ Provee protección independientemente de la plataforma e SO que esté operando sobre la red. ✓ Compatible con casi todas la versiones de Linux.	300	2 años	$ 6600	9

Tabla 3.14 Tabla comparativa de Antivirus

[14] Controla amenazas escondidas en archivos. Procesos ocultos.

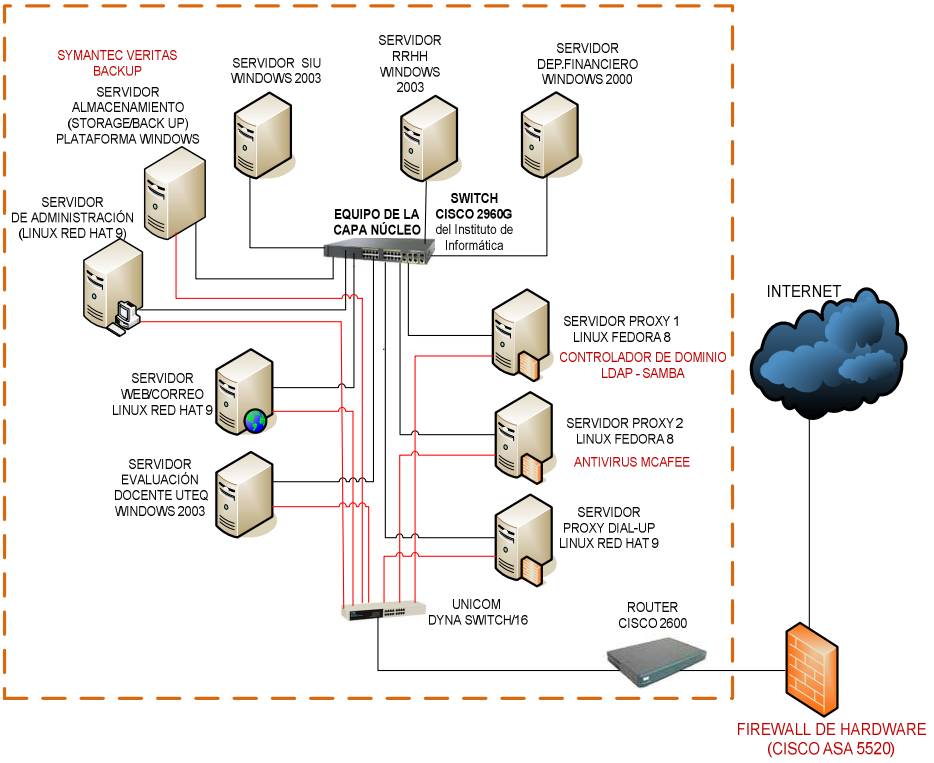


Figura 3.31 Software de Seguridad y autenticación de la UTEQ

c. Herramientas de autenticación

Es necesario tener el control de los usuarios que están permitidos el ingreso a la intranet de la Universidad, así como los permisos de acceso a cada uno de los recursos de la red incluyendo servicios como el Internet.

La UTEQ debe centralizar el acceso a los recursos utilizando un controlador de dominio instalado en los PROXYs de la red. Este controlador estaría conformado por el software LDAP y SAMBA que autenticaría tanto a las máquinas que trabajen con Windows y con LINUX.

Con esto se podrá establecer políticas de acceso a todos los equipos que estén accediendo a la red, se tendrá sectorizado los permisos de acceso a recursos y carpetas compartidas, se tendrá definido que tipo de software debe tener cada facultad, obteniendo con esto un menor número de infiltraciones o instalaciones

de software espías que compliquen el rendimiento de la red y obteniendo un control sobre la asignación de IPs dinámicas y diferenciando cada facultad con una subred especifica.

Así también, estas mismas herramientas se pueden implementar sobre los servidores Linux, teniendo en cuenta que el software es gratuito pero la administración y mantenimiento requiere conocimientos sólidos sobre este sistema operativo.

3.6 PLAN DE CONTENCIÓN ANTE DESASTRES

La Figura 3.32 muestra en forma condensada el Plan de Acción frente a un posible desastre que pudiera enfrentar la Universidad, y que a su vez pudiera afectar el funcionamiento de la Infraestructura IT Universitaria.

El mismo se basa en un monitoreo constante de la infraestructura IT para poder tomar la acción más oportuna y eficaz según el esquema de Administración de Fallas mostrado en apartados anteriores en este capítulo.

Determinado que la función de Administración de Fallas no está posibilitada para resolver tal falla, se pasa al siguiente nivel, que es tomar a la falla como desastre.

Estableciendo como los más posibles escenarios de desastres que podría enfrentar la Universidad a los siguientes:

- *Falla:* Se refiere a una posible falla en algunos de los suministros externos a la Infraestructura Universitaria (Energía, Agua, etc.) ó a una falla humana en el manejo de los mismos.
- *Social:* Se refiere a posibles disturbios, altercados, movimientos, manifestaciones o eventos sociales que puedan modificar o afectar la Infraestructura Universitaria y con ello a la Infraestructura IT.
- *Ambiental:* Se refiere a posibles desastres naturales (inundaciones, terremotos, etc.) que de alguna manera puedan alterar la Infraestructura Universitaria y con ello a la Infraestructura IT.

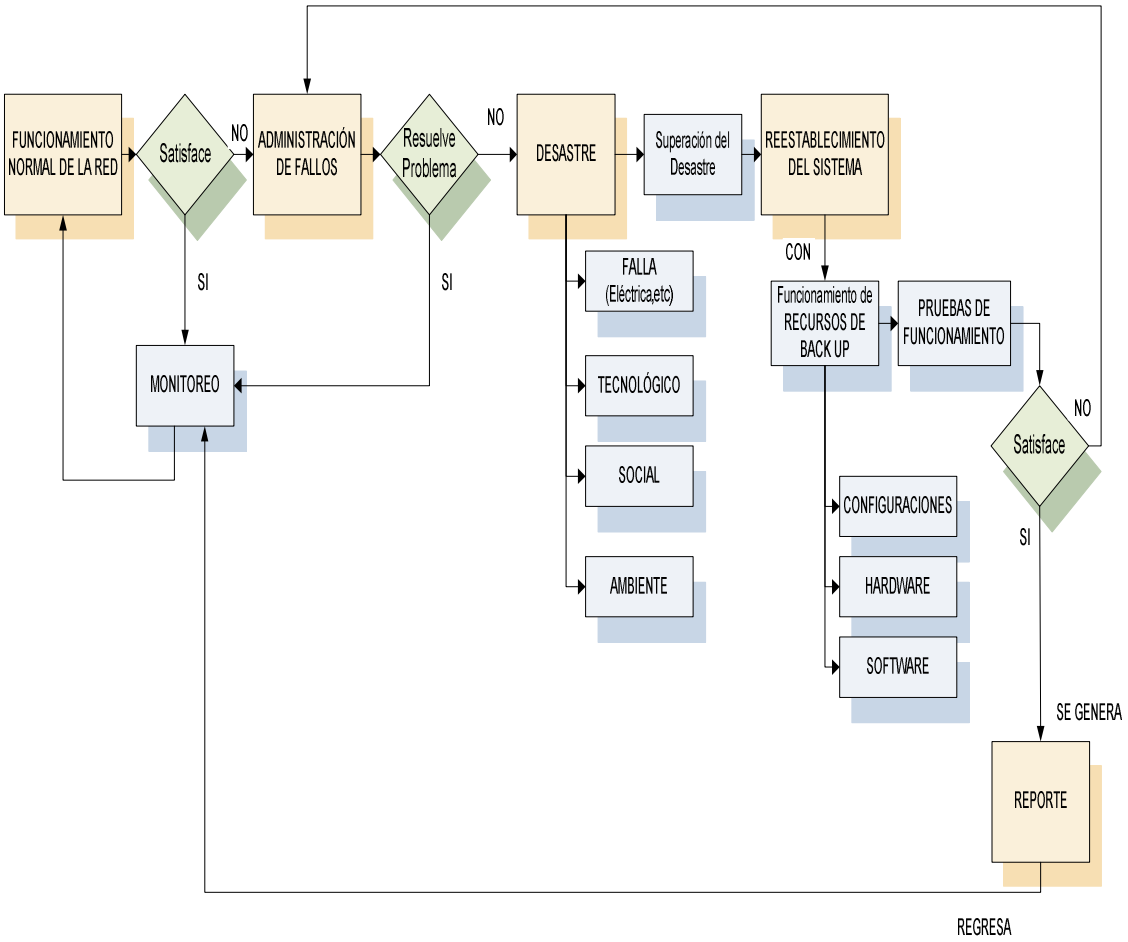


Figura 3.32 Esquema sobre el Plan de Contención

- *Tecnología:* Se refiere a una falla tecnológica dentro de la Infraestructura IT Universitaria que no pueda ser superada de una manera inmediata por la Función de Administración de Fallas del Modelo de Gestión propuesto. Esto debido, muy posiblemente a uno o varios de los escenarios descritos anteriormente.

Una vez superado el desastre de los posibles escenarios contemplados, entra la fase de Restauración de la Infraestructura IT. Mediante la utilización de los elementos de Back-Up físicos y lógicos que contempla el Modelo de Gestión propuesto.

Después es fundamental realizar las pruebas necesarias para verificar el retorno de la Infraestructura IT a su funcionamiento normal.

Una vez terminados estos pasos y restablecido el funcionamiento de la infraestructura IT, es oportuno realizar el reporte respectivo, documentando todo lo sucedido y la solución que se le dio al desastre, para de esta manera retroalimentar y mejorar el Plan de Contención ante Desastres.

3.7 REPERCURSIONES DE IMPLEMENTACIÓN DEL MODELO

Una vez explicada la Metodología de Implementación del Modelo de Gestión propuesto, se puede visualizar las repercusiones que este tendrá dentro de la Infraestructura IT Universitaria y de la misma Universidad.

Entre las principales repercusiones tenemos las siguientes:

Este modelo garantiza la escalabilidad y flexibilidad de la infraestructura IT universitaria debido a que se ha utilizado un esquema modular para las diferentes capas de la red (Modelo de Capas) y del modelo de gestión (TMN-FCAPS/SMNP).

Permitiendo de esta manera dividir los posibles problemas complejos que enfrente la infraestructura universitaria en problemas simples de breve y sencilla resolución.

Otra repercusión importante es el aumento en la calidad del servicio prestado hacia los diferentes usuarios de la red y el aumento en el número de los mismos. Como es el caso de los servicios Web, e-mail y almacenamiento centralizado.

Por otra parte la implementación de este modelo permite una administración no solo de la infraestructura IT. Si no que posibilita visualizar a la administración desde un punto más alto, como es el de negocio y permite optimizar recursos y contribuir de una mejor manera a la misión y visión de la Universidad.

3.8 PLAN DE MIGRACIÓN

La implantación de una arquitectura orientada a servicios debe realizarse en las organizaciones de forma incremental, sin interferir en la marcha normal de arquitecturas tradicionales; y a través de la introducción de proyectos pilotos evaluables, ya que su éxito condicionará su ampliación para ir abarcando áreas aplicativas más extensas.

3.8.1 OBJETIVO

Este punto tiene como objetivo principal generar el Plan Maestro para la implementación del Modelo de Gestión y Administración dentro de la UTEQ, con lo que se logrará una mejora e incremento en los servicios prestados por la Intranet, en sus seguridades y administración.

El alcance del plan comprende las siguientes etapas:

- Inventario
- Back-up
- Implementación de Hardware
- Implementación de Software
- Implementación de Políticas de Seguridad
- Redistribución
- Divulgación e Información
- Integración
- Monitoreo y Estabilización

Cada etapa se la detalla a continuación:

3.8.2 INVENTARIO

En esta etapa se realizara el inventario del equipo que será parte de la nueva infraestructura *IT* de la universidad, esto incluye al equipo propuesto en este

proyecto, así como al equipo reutilizado; además el inventario detalla su función y ubicación dentro de la red. (Ver tabla 3.15)

UBICACIÓN	EQUIPO	FUNCIÓN	OBSERVACIÓN
NÚCLEO	SWITCH CISCO 2960G	Equipo principal de conmutación de la red	Equipo antiguo
ACCESO A INTERNET	ROUTER CISCO 2600	Acceso al Internet	Equipo antiguo
CAPA DE DISTRIBUCIÓN	SWITCH CISCO 2960G	Equipos de conmutación de las subredes de la UTEQ	Equipo antiguo.
RED INALÁMBRICA	ROUTER ORINICO OR 1100	Acceso Inalámbrico Inter facultad	Equipo antiguo
	DLINK DWL 2100AP	Acceso inalámbrico a la red LAN	Equipo antiguo
	DLINK DWL 3200AP	Acceso inalámbrico a la red LAN	Equipo antiguo
	LINKSYS WAP54G	Acceso inalámbrico a la red LAN	Equipo antiguo
INTRANET	UNICOM DYNA SWITCH/16	Equipos de Acceso a la red LAN de las facultades.	Equipo antiguo
	3COM BASELINE 2824	Equipos de Acceso a la red LAN de las facultades.	Equipo antiguo
	8 servidores	Servidores WEB, Correo, bases de datos y Proxy.	Equipo antiguo
	1 Servidor de Respaldo de información	Equipo para respaldar las bases de datos más sensibles de la red. Servidor Redundante.	Equipo nuevo
	1 Servidor de Administración y Gestión de Red.	Servidor para gestionar toda la red de la UTEQ.	Equipo nuevo
	FIREWALL CISCO ASA 5520 Adaptive Security Appliance	Protección de la red de la UTEQ	Equipo nuevo

Tabla 3.15 Inventario

3.8.3 BACK-UP

Esta etapa consiste en realizar el respaldo de la información crítica para el funcionamiento de la Intranet, como es la:

- Base de datos de Servidores

- Configuraciones de Switches, Routers, etc.
- Documentación Crítica.

Esta acción posibilita la restauración del sistema en caso de algún error o falla presentada dentro de la migración.

Para el caso en estudio se recomienda realizar el Back-Up de las configuraciones de los Switches y Routers presentes en las capas de Núcleo, Distribución y Acceso. También aquellas configuraciones de las bases de datos de los servidores presenten en la zona de servicios.

3.8.4 IMPLEMENTACIÓN DE HARDWARE

En esta etapa se realizara la implementación de todo el Hardware nuevo propuesto por este proyecto, que son:

- Firewall CISCO ASA 5520 Adaptive Security Appliance
- Servidor de BackUp HP ProLiant ML370 G4
- Servidor de Administración y Gestión de Red.

La implementación se realizará siguiendo las sub-etapas mencionadas a continuación:

- *Instalación física*. Instalación de los equipos dentro del los racks y cuartos de comunicaciones correspondientes.
- *Prueba de capacidades*. Pruebas técnicas de los equipos nuevos, constatación de recursos de memoria y CPU.
- *Configuraciones*. Realización de configuraciones básicas de los nuevos equipos.
- *Pruebas de Configuraciones*. Pruebas de las configuraciones básicas realizadas previamente.

3.8.5 IMPLEMENTACIÓN DE SOFTWARE

De manera similar que en la etapa anterior, en esta etapa se realizará la implementación de todo el Software nuevo propuesto por este proyecto, que es:

- Herramientas de Administración y Gestión de Red (Nagios. MRTG, NetDot, *OCS Inventory NG 1.02,* etc.).
- Symantec Veritas NetBackUp 6.5.
- McAfee Linux Shield 300 licencias.

Siguiendo las sub-etapas mencionadas a continuación:

- *Instalación*. Del nuevo software en los servidores correspondientes.
- *Registro*. Registro de licencias y permisos.
- *Actualización*. Actualización en línea de los nuevos recursos.
- *Configuraciones*. Realización de configuraciones básicas.
- *Pruebas de configuración*. Pruebas de las configuraciones básicas realizadas previamente.

3.8.6 IMPLEMENTACIÓN DE POLÍTICAS

Esta etapa es fundamental, ya que aquí se implementarán las configuraciones tanto en Hardware y Software que reflejarán las Políticas de Seguridad y Administración propuestas por este proyecto y descritas en capítulos anteriores.

3.8.7 REDISTRIBUCIÓN

En esta etapa se realizará la implantación del rediseño propuesto en capítulos anteriores. Esta etapa más que ser de cambios físicos, es de cambios lógicos e implementación del concepto de capas y estructuración propuesto por este proyecto.

3.8.8 DIVULGACIÓN E INFORMACIÓN

Este tema tiene que ver con la información desplegada sobre el proyecto tanto para autoridades como al personal administrativo, docente y a la comunidad universitaria en general.

Esta información debe ser clara y concisa en temas de afectación de servicios, Políticas de Seguridad y uso de la infraestructura *IT*.

Para una correcta integración y funcionamiento del nuevo modelo es necesario una adecuada información y concientización sobre el uso y manejo de la infraestructura *IT* de la Universidad.

También es importante tener en cuenta las fechas en las que se van a realizar la migración y divulgación al público; además se debe considerar el tiempo de fuera de servicio que ocasionarían las diferentes etapas de la migración. Este tiempo debería ser reducido al mínimo dentro del Plan de Migración, y las actividades más críticas del mismo se deberán realizar en horas no laborables para de esta manera afectar lo menos posible a los clientes.

Es importante proporcionar al cliente la información de las actividades que se va realizar y su objetivo, así como publicar las nuevas capacidades y servicios que ofrecerá la Infraestructura *IT*.

A continuación se establecen las actividades principales que se deben cumplir por parte del Área de Informática (área encargada de las comunicaciones) de la Universidad para publicitar las nuevas capacidades y servicios de la Intranet; estas actividades se deben cumplir en lapsos previos, actuales y posteriores a la implementación de las diferentes etapas de la migración:

- Divulgación de Información General del Proyecto.
- Divulgación de las nuevas capacidades logradas con cada etapa implementada.

- Divulgación de los nuevos servicios que se implementarán con cada etapa.
- Divulgación de las fechas de corte e interrupción de los servicios causados por las diferentes etapas de implementación y pruebas de la misma.

3.8.9 INTEGRACIÓN

Esta etapa se refiere a la integración tanto física como lógica de los nuevos recursos de Software y Hardware implementados en etapas anteriores. Esta etapa es crítica debido a que se puede incurrir en posibles cortes de servicios debido a los trabajos de integración y pruebas.

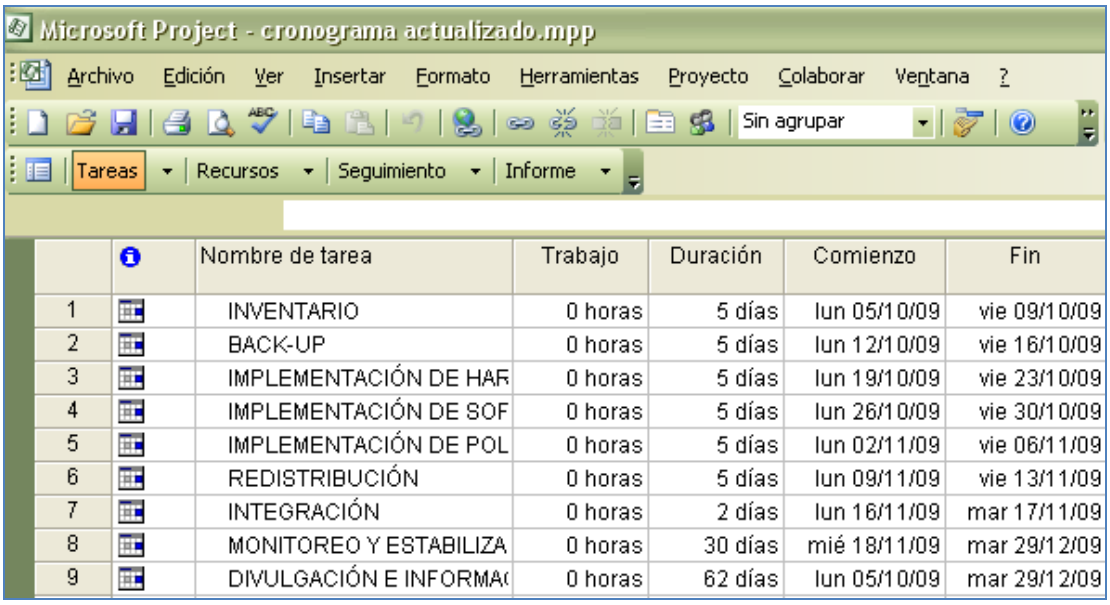
Por este motivo es importante realizar esta etapa en conjunto con la etapa de Divulgación e Información para alertar y prevenir a los usuarios de estos posibles cortes de servicio que involucre la Etapa de Integración.

3.8.10 MONITOREO Y ESTABILIZACIÓN

Como última etapa es necesario tener un período de evaluación y estabilización del sistema después de la implementación total del modelo. Esta etapa servirá para afinar y depurar fallas de la migración y como evaluación de los logros y carencias del proyecto. La Tabla 3.16 detalla el cronograma a seguir para la implementación del modelo. Se ha estimado un período promedio de una semana laboral (5 días) para la mayoría de actividades detalladas en el Plan de Migración.

Se sugiere que actividades que puedan incurrir en cortes de servicio se las realice en días no laborables. La figura 3.34 presenta el diagrama de flujo de las diferentes etapas del Plan de Migración propuesto. Cabe mencionar que el desarrollo de las actividades propuesto permite minimizar los posibles impactos negativos que pudieran darse, y permite dar la suficiente holgura y flexibilidad para la implementación de cada etapa.

3.8.10.1 Cronograma de Actividades para la Migración al nuevo Modelo de Gestión



	Nombre de tarea	Trabajo	Duración	Comienzo	Fin
1	INVENTARIO	0 horas	5 días	lun 05/10/09	vie 09/10/09
2	BACK-UP	0 horas	5 días	lun 12/10/09	vie 16/10/09
3	IMPLEMENTACIÓN DE HAR	0 horas	5 días	lun 19/10/09	vie 23/10/09
4	IMPLEMENTACIÓN DE SOF	0 horas	5 días	lun 26/10/09	vie 30/10/09
5	IMPLEMENTACIÓN DE POL	0 horas	5 días	lun 02/11/09	vie 06/11/09
6	REDISTRIBUCIÓN	0 horas	5 días	lun 09/11/09	vie 13/11/09
7	INTEGRACIÓN	0 horas	2 días	lun 16/11/09	mar 17/11/09
8	MONITOREO Y ESTABILIZA	0 horas	30 días	mié 18/11/09	mar 29/12/09
9	DIVULGACIÓN E INFORMA	0 horas	62 días	lun 05/10/09	mar 29/12/09

Tabla 3.16 Cronograma de actividades para el Plan de Migración al Nuevo Modelo de Gestión

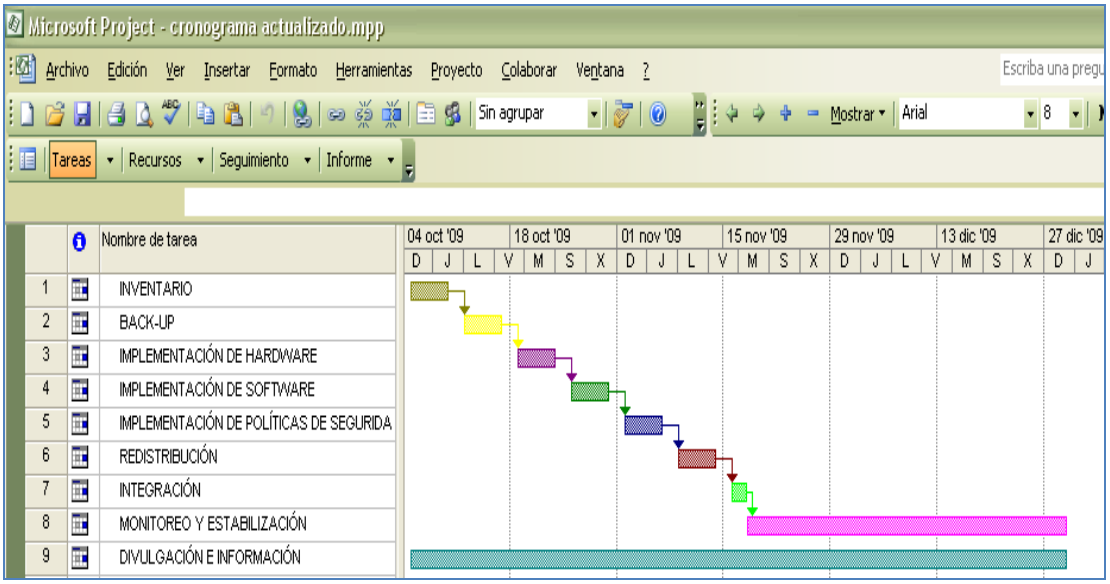


Figura 3.33 Flujograma para la realización del Plan de Migración al nuevo modelo de Gestión de Red para la UTEQ

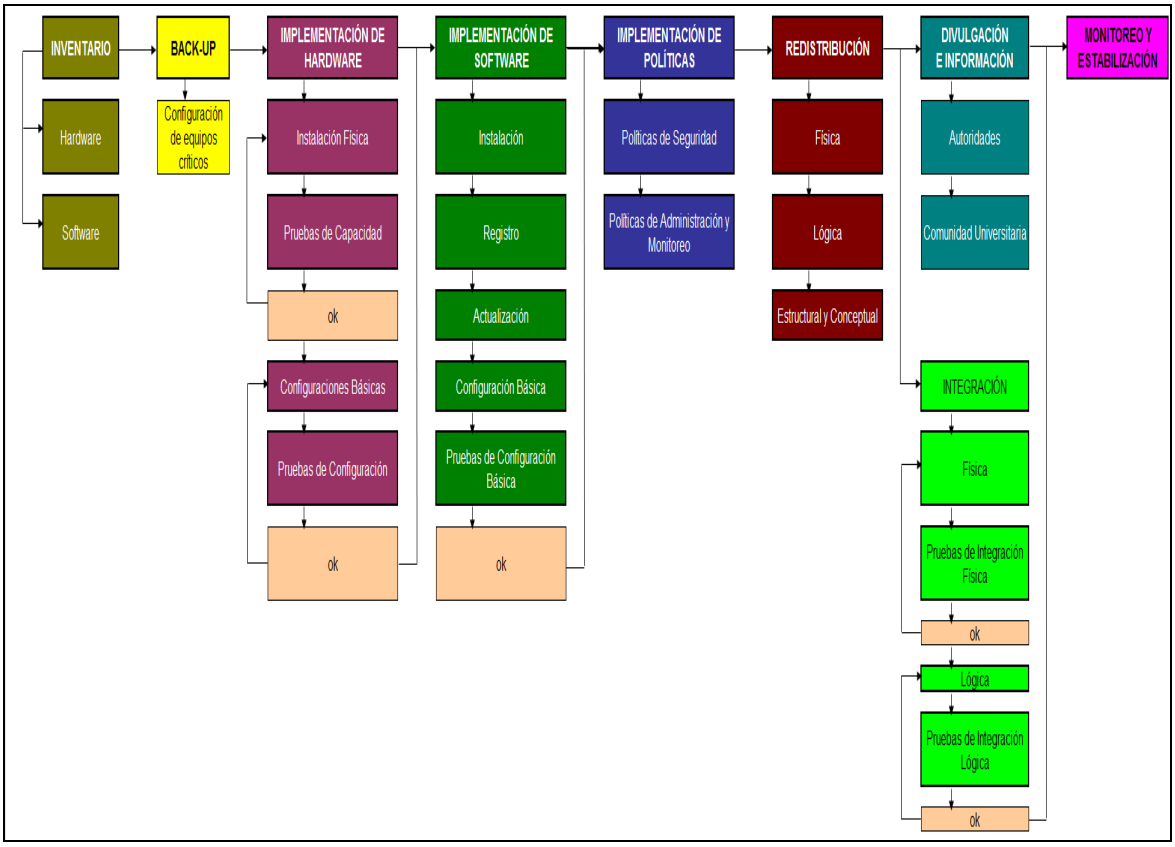


Figura 3.34 Diagrama de flujo sobre actividades para el Plan de Migración al Nuevo Modelo de Gestión

3.9 NIVEL DE ACUERDO DE SERVICIOS *(SLA: Service Level Agreement)*

Es importante que una vez implementado el modelo, se defina un nivel de servicio con el cual se garantice la satisfacción del usuario (estudiantes, personal docente y administrativo) y que el prestador de los servicios (UTEQ) cumplan con acuerdos definidos para el correcto funcionamiento de todos los sistemas y ofrecer un servicio confiable, altamente disponible y con todas la seguridades necesarias para su operatividad, respaldado en acuerdos de nivel de servicio (SLA) firmados con TELCONET (ANEXO I). Por tal motivo se propone los puntos que deben constar en un SLA interno de la UTEQ hacia sus usuarios:

ACUERDO DE NIVEL DE SERVICIOS INTERNO DE LA UTEQ	
Definición	Descripción de las características del servicio.
Disponibilidad	Contempla la plataforma tecnológica (sistemas), las comunicaciones y el soporte técnico.
Atención al usuario	Describe el método a seguir por el usuario (estudiante, empleados, personal administrativo, etc.) frente a incidencias o consultas sobre el servicio. Es vital un soporte técnico cualificado y eficiente para asegurar el nivel de servicio adecuado y con atención en horarios establecidos.
Tiempo de respuesta	Compromiso de tiempo mínimo en cuanto a resolución de incidencias.
Mantenimiento	Condiciones sobre el mantenimiento, la reparación de equipos y las posibles intervenciones que afecten al servicio de forma programada.
Penalizaciones	Compensaciones relativas al incumplimiento del nivel de servicio comprometido porte de la universidad con sus usuarios.

Tabla 3.17 Puntos que deben constar en el SLA interno de la UTEQ

Este acuerdo es más que todo un compromiso de confianza que se realiza entre la institución y sus usuarios, un documento que debe ser público para los usuarios de la red de la universidad, quienes deben saber cuál es la calidad en el servicio que deben recibir.

Como punto crítico dentro del servicio de Internet entre la Universidad UTEQ y el proveedor TELCONET y conforme a las normas establecidas por el Consejo Nacional de Telecomunicaciones (CONATEL), se propone aumentar en el acuerdo firmado y mencionado en el ANEXO I, lo siguiente (Tabla 18):

PUNTOS ADICIONALES QUE DEBEN AGREGARSE AL ACUERDO DE NIVEL DE SERVICIOS PROVEEDOR DE INTERNET: TELCONET	
Definición	**Descripción de las características del servicio [41]**
Compartición.	TELCONET debe garantizar la compartición de 1:1 en el canal de Internet.
Congestión.	El canal no debe presentar un índice de congestión mayor a 0.7, de acuerdo a la norma de calidad de Servicios Agregados, artículo 5 literal 2. [41] Si existiere un caso de congestión mayor, se debe proveer la nota de crédito por el tiempo excedente al tiempo normal de congestión.
Medición del Ancho de Banda	TELCONET debe proveer una página específica para la medición del ancho de banda, así mismo una dirección FTP para pruebas de UP y Down en caso de existir congestión.
Interrupción y restitución del servicio	TELCONET se compromete a cumplir con el tiempo de UPTIME acordado en el contrato, así mismo, para cortes programados se compromete a notificar 48 horas antes del evento y la respectiva notificación y pruebas en la apertura y cierre del evento. En caso de un evento fortuito, TELCONET deberá analizar la gravedad y tomar medidas de restitución alterna por un tiempo indefinido de solución así mismo con las notas de crédito correspondientes por el tiempo sin servicio.
Categorización	Por el nivel de facturación, se solicita a TELCONET, categorizar a la Universidad UTEQ como cliente VIP.

Tabla 3.18 Puntos propuestos para el SLA con TELCONET

BIBLIOGRAFÍA DEL CAPÍTULO III

[1] ROBALINO LÓPEZ, Jorge Andrés / CEDEÑO MENDOZA, Simón Adrián. Rediseño de la Infraestructura del Proveedor de Servicios de Internet ONNET S.A. para la optimización del Servicio en el Distrito Metropolitano de Quito. Escuela Politécnica Nacional 2008.

[2] http://www.simpleweb.org/tutorials/tmn/index-24.html

[3] http://www.telefonica.es/sociedaddelainformacion/pdf/05_la_gestion.pdf

[4] http://www.ceenet.org/workshops/lectures2001/Marcin%20Cieslak/netmgmt-cieslak-2001.pdf

[5] http://www.aprendaredes.com/downloads/Como_Administrar_Redes.pdf

[6] http://ipref.wordpress.com/2008/11/28/modelo-jerarquico-de-red/

[7] http://www.aprenderedes.com/2006/06/19/las-tres-capas-del-modelo-jerarquico-de-cisco/

[8] Alexander Clemm, PhD. Cisco Press. NETWORK MANAGEMENT FUNDAMENTALS. 2007.

[9] http://www.proredes.com/tec_respaldo.html

[10] http://linux.softpedia.com/screenshots/MRTG_1.png

[11] http://www.scribd.com/doc/2994263/PROCEDIMIENTO-DE-MONITOREO-RED

[12] http://www.mrtg.jp/en/es_es/

[13] http://www.mid1.cz/solutions/NTOP.html

[14] http://www.ldc.usb.ve/~rgonzalez/2005abriljulio/ci5832/videoconferencias/VideoConferencia5.pdf

[15] http://www.ntop.org/Monitoring.html

[16] http://www.ethereal.com/

[17] http://www.ethereal.com/docs/eug_html_chunked/ChUseMainWindowSection.html

[18] http://oss.oetiker.ch/smokeping/

[19] http://www.nsrc.org/workshops/2008/walc/presentaciones/smokeping.ppt

[20] http://www.solarwinds.com/products/orion/fault_management.aspx

[21] http://www.solarwinds-iberica.com/home/index.php/Documentacion-Solarwinds/Ver-categoria.html

[22] http://oriondemo.solarwinds.com/Orion/NetPerfMon/NodeDetails.aspx?NetObject=N:144

[23] http://www.solarwinds-iberica.com/home/index.php/Documentacion-Solarwinds/Ver-categoria.html

[24] http://en.wikipedia.org/wiki/OpenView

[25] http://www.aethis.com/solutions/hp_openview/index.html

[26] http://www.ramonmillan.com/tutorialeshtml/gestionred.htm

[27] http://www.optivoz.com/index.php?contenido=productos/seccion7.php&m=3&v=2

[28] http://manageengine.adventnet.com/products/opmanager/system-requirements.html

[29] http://manageengine.adventnet.com/products/opmanager/OpManagerOverview.htm

[30] http://nagios.sourceforge.net/docs/nagios-3.pdf

[31] http://wiki.linuxbaja.org/doku.php?id=nagios

[32] http://nagios.sourceforge.net/images/screens/big/statusmap.jpg

[33] http://www.kavanagh.co.uk/pdfs/network_node_manager_advanced_edition.pdf

[34] http://www.uteq.edu.ec/universidad/general.htm

[35] http://www.addlink.es/productos.asp?pid=457

[36] https://netdot.uoregon.edu/trac/

[37] http://www.ocsinventory-ng.org/index.php?page=architecture

[38] http://es.kioskea.net/contents/attaques/attaques.php3

[39] http://www.router-switch.com/

[40] http://tools.cisco.com/ITDIT/MIBS/MainServlet?ReleaseSel=195&PlatformSel=46&fsSel=1092 (CISCO IOS MIB Locator)

[41] RESOLUCIÓN 534-22-CONATEL-2006 : **“**NORMA DE CALIDAD DEL SERVICIO DE VALOR AGREGADO DE INTERNET**”**

CAPÍTULO IV
ANÁLISIS DE COSTOS

4.1 INTRODUCCIÓN

En éste capítulo se realizará el análisis de los costos en los que debería incurrir la UTEQ para el desarrollo completo del proyecto propuesto en esta tesis. Como es una entidad estatal, no se puede analizar la recuperación de la inversión, pero se puede evaluar los beneficios que van a obtener al implementar el Modelo de Gestión propuesto en este proyecto. Por lo tanto, se hará una propuesta de costos y se evaluará todos los puntos positivos de su implementación.

4.2 DETALLE DE COSTOS

4.2.1 DETALLE DE COSTOS DE HARDWARE

En el cuadro siguiente, se expone un resumen de los equipos que se necesitan para la implementación del Modelo de Gestión de Red y elementos de Back Up.

COSTOS DE HARDWARE			
Hardware	**Cantidad**	**Precio Unitario (USD)**	**Precio Total (USD)**
Switch CISCO 2960G	1	$ 2.500,00 [1]	$ 2.500,00
WIC - 1T Interface Serial	1	$ 200,00 [1]	$ 200,00
CISCO ASA 5520	1	$ 7.995,00 [7]	$ 7.995,00
Servidor HP ProLiant ML370 G4	1	$ 2.301,26 [2]	$ 2.301,26
Servidor de Gestión y Administración	1	$ 758,24 [2]	$ 758,24
Unidad de Almacenamiento HP SAS 10K 146 GB	4	$ 396,00 [3]	$ 1.584,00
Total Costos			**$ 15.338,50**

Tabla 4.1 Costos de Hardware

Como la UTEQ es una entidad estatal, no se paga el IVA en los productos adquiridos. Dentro de la tabla 4.1 se incluyen equipos para implementar en lo referente al servidor de respaldo, al servidor de administración, la seguridad perimetral y elementos de BackUp.

4.2.2 DETALLE DE COSTOS DE SOFTWARE

Para la implementación del software correspondiente, se evaluará sólo lo necesario de implementar. Se trabajará sobre la base que ya se tiene en la Universidad.

A continuación la tabla 4.2 de costos de software:

COSTOS DE SOFTWARE			
Software	**Cantidad**	**Precio Unitario (USD)**	**Precio Total (USD)**
Symantec Veritas BackUp (5 Licencias Clientes Windows)	1	$ 3.995,00 [6]	$ 3.995,00
McAfee Linux Shield (300 Licencias)	1	$ 6.600,00 [5]	$ 6.600,00
Total Costos			**$ 10.595,00**

Tabla 4.2 Costos de Software

4.2.3 DETALLE DE COSTOS DE OPERACIÓN Y MANTENIMIENTO

Para poner en marcha el presente proyecto, se debe tomar en cuenta los siguientes costos:

- Costo del personal necesario para la implementación y mantenimiento del proyecto.
- Costos adicionales por servicios básicos e imprevistos.

4.2.3.1 Costos del Personal necesario para la Implementación, Operación y Mantenimiento

COSTOS DE PERSONAL DE OPERACIÓN Y MANTENIMIENTO			
Posición	**Función**	**Salario Mensual (USD)**	**Salario Anual (USD)**
Ingeniero Senior	Administrador de la Red	$ 840,00 [8]	$ 10.080,00
Ingeniero Junior	Monitoreo Nivel 2 y Soporte	$ 654,00 [8]	$ 7.848,00
Operador Junior	Monitoreo Nivel 1	$ 500,00 [8]	$ 6.000,00
Total de salario		$ 1.994,00 [8]	**$ 23.928,00**

Tabla 4.3 Costos de Personal de Operación y Mantenimiento

Este personal descrito, estará bajo la supervisión del actual administrador de la Red y la función principal de cada uno debe ser la siguiente:

- *Ingeniero Senior*. Soporte Técnico especializado en la red, verificación de *SLAs (Service Level Agreement)*, puesta en marcha de nuevas configuraciones o actualizaciones. Trabajos sobre la infraestructura de la Universidad UTEQ.

- *Ingeniero Junior*. Soporte Técnico al personal de la Universidad, trabajos emergente y monitoreo del estado de la infraestructura de la Universidad UTEQ.

- *Operador Junior*. Monitoreo nivel 1, detección de problemas, soporte técnico sobre todo al nivel físico de la red, encargado del nivel de escalamiento ante problemas.

Con esto, se espera proporcionar, un área técnica especializada y bien organizada, que de solución a cualquier inconveniente que presente los sistemas o equipos de red, basándose estrictamente en el Modelo de Gestión de Red descrito en capítulos anteriores.

4.2.3.2 Costos Adicionales

Entre los costos adicionales se estima una cantidad mensual para cubrir cualquier imprevisto y lo que se refiere a servicios básicos que conlleva mantener la infraestructura para gestionar la red. Este se detalla en la Tabla 4.4.

COSTOS ADICIONALES		
Rubro	**Costo Mensual (USD)**	**Costo Anual (USD)**
Servicios Básicos	$ 400,00	$ 4800,00
Imprevistos	$ 300,00	$ 3600,00
Total		**$ 8.400,00**

Tabla 4.4 Costos por Imprevistos y Servicios Básicos

4.2.4 DETALLE DE COSTOS POR INSTALACIÓN

A continuación se detallan los costos que se deben incurrir para la instalación de sistemas y equipos para la puesta en marcha del modelo de Gestión de Red para la UTEQ. El criterio utilizado para calcular estos costos, es considerar el 17% del valor total de costos de hardware y de software, para su instalación y configuración.

COSTOS DE INSTALACIÓN	
Rubro	**Costo Total (USD)**
Instalación y Configuración de Software	$ 2.607,55
Instalación y Configuración de Hardware	$ 1.801,15
Total Costos	**$ 4.408,70**

Tabla 4.5 Costos por Instalación

4.3 COSTO TOTAL DEL PROYECTO

El costo total del proyecto contempla todos los costos detallados en los apartados anteriores.

COSTOS TOTALES	
Rubro	**Costo (USD)**
COSTOS DE HARDWARE	$ 15.338,50
COSTOS DE SOFTWARE	$ 10.595,00
COSTOS DE PERSONAL DE OPERACIÓN Y MANTENIMIENTO	$ 23.928,00
COSTOS ADICIONALES	$ 8.400,00
COSTOS INSTALACIÓN	$ 4.408,70
COSTO TOTAL	**$ 62.670,20**

Tabla 4.6 Costos totales del Proyecto

Para financiar este proyecto existen 2 opciones:

- Financiamiento con Presupuesto Institucional Anual de la UTEQ
- Financiamiento del SENACYT

4.3.1 FINANCIAMIENTO CON PRESUPUESTO INSTITICIONAL ANUAL DE LA UTEQ

Se puede incluir en la Planificación Operativa Anual (POA) de cada departamento un rubro de aporte al desarrollo del sistema de gestión de red, para cubrir los costos del proyecto, es decir se propone dividir el gasto anual del proyecto entre todas las unidades ejecutoras del POA, ya que todas se beneficiarían del sistema de gestión de la red de la UTEQ.

4.4 EVALUACIÓN DEL COSTO DEL PROYECTO Y BENEFICIOS

El costo total del proyecto asciende a $ 62.670,20 para el primer año, y un costo extra a la nomina de trabajadores desde el segundo año de $ 23.928. En estos

rubros está considerado nuevo personalmente altamente calificado sobre redes de información. Además, los equipos poseen garantía de 2 años provistos por el fabricante internacional y Partners nacionales que garantizarán una pronta respuesta ante incidentes. La compra de equipos se hará mediante representantes de las fabricas internacionales establecidas en el país, mientras que el software se hará la compra vía online con los proveedores, con las seguridades y garantías respectivas. Cabe la pena mencionar, que los precios están sujetos a variaciones.

Los beneficios que se pueden derivar del análisis y evaluación de los costos son:

- El costo total del proyecto no supera ni el 15% del costo total de la implementación de toda la red con sus respectivos equipos y cableado estructurado y proporcionando un 100% extra de administración y seguridad a toda la infraestructura.

- La inclusión de nuevo personal permitirá dar un impulso diferente al área de informática, teniendo personal especializado que proveerá de mayor experiencia a los estudiantes de la facultad. Así mismo, con una preparación adecuada, se puede crear bacantes para pasantías técnicas o inclusive estos puestos ser llenados con estudiantes propios de la universidad, dando así una nueva posibilidad ocupacional en el país.

- El costo del proyecto, se debe ver reflejado en la transformación total de los niveles de calidad de servicio y confiabilidad de los sistemas, alcanzando niveles cercanos al 99.98%, teniendo, sistemas más estables donde el personal docente, administrativo y estudiantes tendrá un acceso rápido y confiable a los servicios de la universidad, minimizando problemas de inestabilidad, inseguridad y caídas frecuentes de los enlaces, provocando con esto pérdidas económicas para la Universidad.

- Los equipos cotizados son CISCO y por lo tanto se garantiza la compatibilidad con todas las capas del modelo presentado en el presente proyecto.

- El software recomendado es compatible con todas las versiones de Microsoft Windows® y el software libre es complemente instalable con las versiones de Linux que se tiene en los servidores.

- Los sistemas de BackUp, se acoplan perfectamente al modelo de trabajo de los servidores, implementado específicamente el servidor de datos, con RAID 1.

- Con este modelo, el costo se reduce tremendamente al poder garantizar nuevos servicios internos de la red, por ejemplo con la seguridad, se puede implementar servicios de correo electrónico interno, ftp, tftp, servidores DNS, con la calidad de servicio proporcionada, se puede instaurar telefonía *VoIP (Voice over IP)*, teniendo señales claras y sin retraso o cortes en la comunicación. Así mismo, una sólida infraestructura y administración garantizará que los servidores no queden fuera demasiado tiempo ante eventuales problemas, pudiendo los mismos, ampliar sus servicios a niveles más altos y más confiables.

- Tanto el hardware como el software, tienen servicio técnico en todo el Ecuador y con técnicos plenamente capacitados por ser de marcas reconocidas, así, se podrá obtener servicio técnico de manera rápida, eficiente y económica.

Por todo lo anterior expuesto, la implementación del Modelo de Gestión y Administración de Red es un factor importante para la comunicación de todo el personal sea de una institución pública o privada. Su escalabilidad debe garantizar la compatibilidad con cualquier tecnología y su inversión en el crecimiento no debe ser alta comparada con la inversión inicial de la infraestructura. La Universidad mejorará su nivel de atención a los estudiantes, su

tiempo de respuesta y su eficiencia, evitando tener retrasos por falla de los sistemas y mejorando la eficiencia del personal administrativo y docente.

BIBLIOGRAFÍA DEL CAPÍTULO IV

[1] http://sinfotecnia.com/prestashop/

[2] TECNOMEGA internacional

[3] http://listado.mercadolibre.com.ec/146_OrderId_PRICE*DESC_DisplayType_G_NoQCat_

[4] http://shop.symantecstore.com

[5] http://shop.mcafee.com/products/LinuxShield.aspx?pid=LINUXSH&CID=MFE-3001

[6] http://shop.symantecstore.com/store/symnasmb/en_US/DisplayProductDetailsSmbPage/productID.77818000/ThemeID.106400/pgm.12858700 (Precio Veritas 5 licencias clientes windows)

[7] http://www.router-switch.com/catalog.asp?catid=13024&gclid=COihx4WO7ZoCFQKenAodjEBuCg

[8] Roles de pago de la Empresa TVCable.

CAPÍTULO V
CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- Del análisis de los modelos de gestión y sus metodologías, estamos seguros que la metodología propuesta en este proyecto será de gran innovación para la administración y gestión de la red de la UTEQ, lo que le permitirá a la universidad lograr los resultados esperados en cuestión de rendimiento de la red e índices de desempeño de todos los sistemas que la conforman y repercutiendo también con esto en el mejor desarrollo del trabajo de sus empleados.

- En la metodología propuesta en este proyecto se logró verificar como los modelos de gestión permiten normar los procesos que se siguen dentro de una institución o empresa. Con esto, podemos tener procedimientos definidos a seguir ante cualquier eventualidad. Así mismo, tendremos normas impuestas a los usuarios de la red para evitar su mal uso y por ende daños masivos que afecten el rendimiento de los equipos. Cada modelo tiene su lugar de desempeño específico pero la combinación de ellos en conjunto con la compatibilidad de protocolos, ha permitido flexibilizarlo para cualquier tipo de red.

- Actualmente la UTEQ tiene serios problemas de administración y sobre todo gestión de la red. No tiene normado procedimientos que permitan tener un control eficiente de toda la red. Su análisis de la información es básica dedicada a certificar que este o no un servicio arriba, sin tener un verdadero sistema de gestión de red.

- Con la elaboración del presente proyecto, se logrará una administración centralizada, con altos índices de efectividad. Así, los equipos de la red interactuaran directamente con el software de gestión obteniendo en

tiempo real informes sobre problemas suscitados, errores provocados y tener un bajo tiempo de respuesta ante desastres que ocasiones la perdida de las comunicaciones y sus servicios.

- La propuesta del modelo de seguridad, da los lineamientos básicos para que se puedan elaborar a corto plazo una verdadera infraestructura de seguridad normados y regidas por las políticas internas y externas y niveles de seguridad que permitan que la red sea seguro para cualquier tipo de transacciones que se realicen sobre esta.

- Un punto importante es la administración de fallos y manejo de reportes. Es necesario que toda falla siga un proceso hasta encontrar su solución y que todo esto sea documentado sobre reportes normados aprobados que sirvan como respaldo ante informes que deberán ser realizados. Las fallas provocan eventos y según el nivel de estas, se necesitan o no atención especializada en los puntos afectados. Con la implementación de las normas, automáticamente las notificaciones de los equipos interactuarán con las consolas de administración y generaran alarmas, categorizadas por niveles de criticidad. La respuesta debe ser inmediata ante el nivel del fallo y el reporte deberá contener claramente el problema y la solución de los mismos. Con esto logremos proveer a todos los usuarios alta disponibilidad y confiabilidad.

- Con la aplicación de este Modelo de Gestión se logra caracterizar al tráfico que circula por la red logrando detectar tráfico anormal o las causas de saturación de los enlaces, así mismo, se logra determinar los servicios más concurridos y prever futuros problemas de accesibilidad.

- Con este Modelo, se garantizará la Calidad de Servicio en la red, priorizando trafico de voz y de datos, controlando los paquetes de Internet y por ende evitando la pérdida de paquetes, retransmisiones y encolamiento en los equipos. Con esto se logrará que los servicios

sensibles (voz y datos) no tengan dificultades al circular por la red y por ende asegurar la integridad, confiabilidad y disponibilidad de la información.

- Con todos estos puntos se puede afirmar que le proyecto se vuelve necesario ante el crecimiento inminente de las redes de datos y telecomunicaciones sin quedarse atrás los servicios que circulan sobre estas redes, por lo tanto el control se vuelve extremadamente necesario y las garantías de cumplir niveles de calidad altamente aceptables para la comunicación confiable entre los usuarios y los servicios.

- Los costos del proyecto no son altos frente al beneficio que obtiene la Universidad, la inversión del estado en tecnología se vuelve cada día un factor importante del progreso a nivel de país. La ciencia necesita de las comunicaciones para el intercambio de información siendo esta oportuna e íntegra. Las Universidades necesitan laboratorios equipados con tecnología de punta para poder hacer pruebas veraces de cualquier índole y transmitir esta información a las unidades respectivas para la evaluación y desarrollo de los datos analizados.

- La UTEQ ganará eficiencia, confiabilidad, dispondrá de un sistema de gestión de punta, podrá asociarse con empresas para producir nuevos servicios garantizando niveles de confiabilidad altos y propiciando inversiones en la Universidad. Dispondrá de estudiantes capacitados con información actualizada y disponible lo cual se traducirá en profesionales capacitados para enfrentar nuevas tecnologías y retos del mundo actual.

5.2 RECOMENDACIONES

- Se recomienda la aplicación de la metodología propuesta en el presente proyecto, la misma que permitirá a la universidad aumentar sus niveles de desempeño institucional. Además que permitirá la optimización de los costos ya que permite hacer más eficiente las operaciones de la red y permite que los administradores de la red sean más productivos.

- Por todo lo expuesto se recomienda principalmente al estado en la inversión de nuevas tecnologías a todas las instituciones públicas del país para tener profesionales preparados con los nuevos retos que representa el crecimiento mundial en las telecomunicaciones.

- La UTEQ debe implementar esta metodología para normar sus procesos internos y externos, mejorar su Calidad de Servicio y mantener sus índices de disponibilidad en los niveles más altos.

- Para la implementación, se debe trabajar junto con el plan de migración, con grupos definidos de trabajo y tareas asignadas previamente al personal. Cada etapa debe ser evaluada para detectar cualquier imprevisto antes de pasar a la siguiente fase.

- Además de la implementación de la metodología propuesta en este proyecto, se sugieren realizar adicionalmente certificaciones de estándares internacionales como la ISO27001 tanto para las redes como para los servicios de TI (Tecnología de Información).y así asegurar la competitividad de la institución.