PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR

FACULTAD DE INGENIERIA

MAESTRÍA EN REDES DE COMUNICACIONES

ESTUDIO COMPARATIVO DE LOS SISTEMAS DE GESTIÓN Y MONITOREO BASADOS EN LOS REQUERIMIENTOS GENERALES DE LA RED DE UN CAMPUS UNIVERSITARIO.

PÉREZ SANTOS LEONARDO ANDRÉS

Trabajo previo a la obtención del Título de:
MAGISTER EN REDES DE COMUNICACIONES

Quito, 2013

ÍNDICE

CAPITULO 1. MARCO TEÓRICO GESTIÓN DE REDES 6

1.1. INTRODUCCIÓN 6

1.2. GESTIÓN DE REDES 8

1.2.1. DEFINICIÓN DE GESTIÓN DE RED 8

1.2.2. OBJETIVOS DE LA GESTIÓN DE RED 10

1.2.3. ELEMENTOS QUE INTERVIENEN EN LA GESTIÓN DE REDES 10

1.2.3.1. EL GESTOR 12

1.2.3.2. EL AGENTE 12

1.2.3.3. PROTOCOLO DE GESTIÓN DE REDES 13

1.2.4. IMPORTANCIA Y BENEFICIOS DE LA GESTIÓN DE RED 16

1.3. SISTEMAS DE GESTIÓN Y ADMINISTRACIÓN DE RED 18

1.3.1. EVOLUCIÓN DE LA GESTIÓN DE RED 18

1.3.1.1. GESTIÓN AUTÓNOMA 19

1.3.1.2. GESTIÓN HOMOGÉNEA 20

1.3.1.3. GESTIÓN HETEROGÉNEA 20

1.3.1.4. GESTIÓN INTEGRADA 20

1.3.2. MODELO DE GESTIÓN OSI 21

1.3.3. MODELO DE GESTIÓN TMN 33

1.3.3. MODELO DE GESTIÓN DE TELECOMUNICACIONES TOM / e-TOM 37

1.3.4. MODELO DE GESTIÓN DE GESTIÓN RED INTERNET O SNMP 40

1.4. ANÁLISIS DE LOS MODELOS DE GESTIÓN DE RED 54

CAPITULO 2. ESTUDIO COMPARATIVO DE LOS SISTEMAS DE GESTIÓN 56

2.1. INTRODUCCIÓN 56

2.2. CARACTERÍSTICAS DE LOS SISTEMAS DE GESTIÓN 58

2.3. CARACTERÍSTICAS GENERALES PARA ESCOGER UN SISTEMA DE GESTIÓN DE RED 58

2.3.1. INTERFAZ SIMPLE 59

2.3.2. ESTABLECER LINEAS BASE 60

2.3.3. GENERACIÓN DE REPORTES 60

2.3.4. AUTO DESCUBRIMIENTO 60

2.3.5. CONFIGURACIÓN Y ANÁLISIS 61

2.3.6. CONFIGURACIÓN DE POLÍTICAS Y DESPLIEGUE DE INFORMACIÓN 62

2.3.7. RECOLECCIÓN DE INFORMACIÓN 64

2.3.8. SOPORTE 64

2.4. PLATAFORMAS DE GESTIÓN DE MONITOREO 65

2.4.1.1.- HP Openview 65

2.4.1.2.- IBM Tivoli 66

2.4.1.3.- Solarwinds Orion Network Performance Monitor 66

2.4.2. APLICACIONES DE GESTIÓN LIBRES 66

2.4.2.1.- MRTG 66

2.4.2.2.- RRDTools 67

2.4.2.3.- SmokePing 67

2.4.2.4.- Cacti 67

2.4.2.5.- OpenNMS 68

2.4.2.6.- ZABBIX 68

2.4.2.7.- Pandora FMS24 68

2.4.2.8.- ZENOSS 69

2.4.2.9.- Nagios 70

CAPITULO 3. ESTUDIO COMPARATIVO DE GESTIÓN Y MONITOREO DE ACUERDO A LAS CARACTERÍSTICAS DEL TIPO DE RED SELECCIONADO 73

3.1. INTRODUCCIÓN 73

3.2. CARACTERÍSTICAS DE LA RED SELECCIONADA 75

3.3 MODELO DE GESTIÓN A SER TOMADO EN CUENTA 78

3.4. METODOLOGÍA DE DESARROLLO 80

3.5. INFRAESTRUCTURA GENERAL DE UNA RED PARA CAMPUS UNIVERSITARIO 83

3.6. REQUERIMIENTOS 88

3.6.1. MONITOREO DE SERVICIOS 90

3.6.2. MONITOREO DE LOGS 92

3.6.3. MONITOREO DE UPS 93

3.3.4. ENVÍO DE NOTIFICACIONES 94

3.6.5. REQUERIMIENTOS ADICIONALES 95

3.7 ESTUDIO COMPARATIVO DE LOS SISTEMAS DE GESTIÓN DE ACUERDO A LOS REQUERIMIENTOS DEL TIPO DE RED SELECCIONADO 98

3.7.1. SELECCIÓN DEL SISTEMA DE GESTIÓN 99

3.7.2. VENTAJAS Y DESVENTAJAS 101

3.8. ESTUDIO DE LAS SOLUCIONES A LOS REQUERIMIENTOS CON EL SISTEMA SELECCIONADO 105

CAPITULO 4. INSTALACIÓN Y PRUEBAS DE FUNCIONAMIENTO – DEMO 107

4.1. INTRODUCCIÓN 107

4.2. CARACTERÍSTICAS 110

4.3. SISTEMA DE GESTIÓN Y MONITOREO 112

4.3.1. REQUERIMIENTOS DEL ORDENADOR 112

4.3.2. INSTALACIÓN DEL SOFTWARE 113

4.3.3. CONFIGURACIÓN 120

4.3.3.1. CONFIGURACIÓN BÁSICA 120

4.3.3.2. CONFIGURACIÓN ESPECÍFICA 129

4.3.3.3. MONITOREO 135

4.3.3.4. ALERTAS 139

4.4. PRUEBAS DE FUNCIONAMIENTO 140

4.4.1. POSIBLES FALLAS 140

CAPITULO 5. RECOMENDACIONES Y CONCLUSIONES 142

5.1. RECOMENDACIONES 142

5.2. CONCLUSIONES 143

BIBLIOGRAFÍA 146

CAPITULO 1. MARCO TEÓRICO GESTIÓN DE REDES.

1.1. INTRODUCCIÓN.

Durante la década de los años 80 se produjo una gran expansión en el área de implantación de sistemas y redes de telecomunicaciones. A medida que las organizaciones trataban de aprovechar los beneficios de estos sistemas en cuanto a reducción de costes y aumento de productividad, comenzaron a añadir nuevas redes y expandir las existentes a gran velocidad. Las redes comenzaron a crecer en tamaño y también en complejidad, con un gran aumento de las aplicaciones y de los usuarios de estas redes. Esta tendencia al crecimiento en tamaño y complejidad de las redes tuvo como consecuencia un aumento de los costes de explotación de dichas redes, ya que se requería de más personal cualificado para su administración y la gestión de sus recursos de manera eficiente. Ante este problema surgió la necesidad de disponer de herramientas que facilitasen las tareas de administración de red: gestión de la capacidad, aumento de la disponibilidad, supervisión y resolución de problemas, etc. Estas herramientas o aplicaciones son las que se denominan **sistemas de gestión de red.**

Como consecuencia de este auge de las redes de telecomunicaciones surgen en el sector diversos fabricantes de equipos de telecomunicaciones, así como diferentes tipos de tecnologías de red. En un primer momento, los fabricantes de equipos de telecomunicaciones imponían soluciones de gestión de red propietarias, de manera que el administrador de una red con equipos de distintos fabricantes se encontraba con el problema de la heterogeneidad tecnológica: los equipos de cada fabricante requerían un sistema gestor exclusivo para ellos, y basado en mecanismos (protocolos y lenguajes) particulares, por lo que no era posible gestionar la red conjuntamente. Además, cada nuevo tipo de tecnología de red precisaba de su propio equipo de administradores expertos, lo que de nuevo aumentaba los costes de explotación.

Con el fin de terminar con esta dependencia de la gestión con respecto al fabricante, a finales de los 80 y principios de los 90 surgieron los modelos de gestión de red integrada, que proponían una serie de mecanismos estandarizados y abiertos, con el objetivo de que fuesen adoptados por los distintos fabricantes,

permitiendo así la interconexión de un equipo de cualquier fabricante con el gestor de otro. Puesto que en los entornos más actuales coexisten elementos de distintos dominios de gestión, se hace necesario establecer mecanismos que posibiliten la interoperabilidad de los sistemas de gestión con dichos dominios, de forma que un sistema gestor pueda tener una vista unificada de los recursos gestionados, independientemente del dominio de gestión al que pertenezcan.

Los estudios existentes se centran en las posibilidades de traducir tanto el modelo de información como el protocolo de comunicaciones entre los distintos dominios: si es posible dicha traducción entre dominios, entonces la interoperabilidad es posible. Un ejemplo importante de modelo de gestión y arquitectura que trata de establecer la interoperabilidad entre dominios de gestión es la iniciativa WBEM[1] (Web Based Enterprise Management, Gestión de Empresa Basada en Web), que permite el acceso a diversos dominios mediante una interfaz neutral a todos ellos.

Aún así, un gestor capaz de gestionar varios dominios de gestión, no puede realizar una gestión verdaderamente integrada, ya que no puede discernir acerca de la semántica de recursos definidos en distintos modelos para poder aplicar políticas de gestión común a un mismo recurso, de forma independiente al modelo bajo el cual estén definidos. Una traducción meramente sintáctica de un modelo origen no se corresponderá generalmente con el concepto existente en el modelo destino. Además un gestor debe ser capaz de relacionar la información de modelos distintos para gestionarlos conjuntamente. Se hace por tanto necesaria una traducción semántica que haga corresponder los conceptos de distintos dominios, para poder alcanzar una verdadera gestión integrada. Las aplicaciones al campo de gestión de redes y servicios permitiría realizar una gestión verdaderamente integrada de los diversos recursos que conforman las complejas redes de hoy en día, en las que los recursos deben ser gestionados mediante distintos mecanismos de gestión: dispositivos de red gestionables por SNMP[2].

---

1 *La gestión de redes y sistemas contempla las aplicaciones determinadas que concentran las posibilidades de gestión e interacción en parámetros asociados a su rendimiento, las plataformas Web, bases de datos y en definitiva los sistemas que componen la arquitectura de una organización; es decir, los servidores.*

2 *El Protocolo Simple de Administración de Red o SNMP (Simple Network Management Protocol) es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento.*

1.2. GESTIÓN DE REDES.

1.2.1. DEFINICIÓN DE GESTIÓN DE RED.

La gestión de redes es un concepto bastante general, que implica la utilización de herramientas para ayudar en el manejo de dispositivos, sistemas y redes.

Según Sayman [SAY1996]: “La gestión de redes incluye el despliegue, integración y coordinación del hardware, software y los elementos humanos para monitorizar, probar, sondear, configurar, analizar, evaluar y controlar los recursos de la red para conseguir los requerimientos de tiempo real, desempeño operacional y calidad de servicio a un precio razonable”.

La **gestión de red** consiste en monitorizar y controlar los recursos de una red con el fin de evitar que esta llegue a funcionar incorrectamente degradando sus prestaciones.

1.2.2. OBJETIVOS DE LA GESTIÓN DE RED.

La gestión de redes es el conjunto de tareas de monitorización, información y control necesarias para operar efectivamente en una red. Estas tareas pueden estar distribuidas sobre diferentes nodos de la red, lo cual puede requerir acciones de recogida de datos y análisis cada vez que sucede un nuevo evento en la red. Las tareas de gestión de red se llevan a cabo por el personal responsable o por procesos automáticos de gestión.

Las actuales redes de telecomunicación se caracterizan por un constante incremento del número, complejidad y heterogeneidad de los recursos que los componen.

Los principales problemas relacionados con la expansión de las redes son la gestión de su correcto funcionamiento día a día y la planificación estratégica de su crecimiento. De hecho más se estima que más del 70 % del coste de una red corporativa se atribuye a su gestión y operación.

Por todo ello, la gestión de red, como conjunto de actividades dedicadas al control y vigilancia de recursos de telecomunicación bajo el mismo sistema de gestión, se ha

convertido en un aspecto de enorme importancia en el mundo de las telecomunicaciones.

La gestión de red nos permite: organizar, mantener, supervisar, evaluar, y controlar los elementos de las redes para adaptarse a la calidad de servicio necesario, algunos de los objetivos en la gestión de redes son los siguientes:

- Alta disponibilidad de la red: proveyendo eficiencia operacional, reduciendo los tiempos de inoperabilidad de la red y del sistema, y proveyendo tiempos de respuesta aceptables. Los problemas de la red deben ser rápidamente detectados y corregidos.
- Reducción de costos operacionales de red: este es uno de los motivos primarios detrás de la administración de redes. Como las tecnologías cambian rápidamente, es deseable la administración de sistemas heterogéneos y múltiples protocolos.
- Reducción de cuellos de botella en la red: dependiendo de cada caso en particular, puede ser deseable un monitor centralizado para administración y en otros casos esta tarea debe ser distribuida.
- Incrementar flexibilidad de operación e Integración: las tecnologías de redes están cambiando a velocidades mayores que los cambios de requerimientos y necesidades. Cuando se usa una nueva aplicación, los protocolos usados en redes deberán cambiar también. Debe ser posible absorber nueva tecnología con un costo mínimo y adicionar nuevo equipamiento sin mucha dificultad. Además, debe permitir lograr una fácil migración de un software de administración de redes a otra versión.
- Alta eficiencia: debemos incrementar la eficiencia en detrimento de otros objetivos de la administración pero dependerá de otros factores tales como utilización, costo operacional, costo de migración y flexibilidad.
- Facilidad de uso: las interfaces de usuario son críticas para el éxito de un producto. El uso de aplicaciones de administración de redes no debe incrementar la curva de aprendizaje.

- Seguridad: existen casos en donde la seguridad es un aspecto a tener en cuenta tales como información de contaduría, información gerencial, etc.

El objetivo final de la gestión de red es garantizar un nivel de servicio en los sistemas de una organización el máximo tiempo posible, minimizando la pérdida que ocasionaría una parada o funcionamiento incorrecto del sistema.

Los elementos que son objetos de control por un sistema de gestión de red en las redes de computadores son fundamentalmente los equipos conectados: servidores, terminales, computadores personales, estaciones de trabajo, así como los elementos y equipos de interconexión tales como cables, concentradores, repetidores, puentes, ruteadores, etc.

1.2.3. ELEMENTOS QUE INTERVIENEN EN LA GESTIÓN DE REDES.

La gestión de red se suele centralizar en un centro de gestión, donde se controla y vigila el correcto funcionamiento de todos los equipos integrados en las distintas redes de la empresa en cuestión. Un centro de gestión de red dispone de tres tipos principales de recursos:

- Métodos de gestión. Definen las pautas de comportamiento de los demás componentes del centro de gestión de red ante determinadas circunstancias.
- Recursos humanos. Personal encargado del correcto funcionamiento del centro de gestión de red.
- Herramientas de apoyo. Herramientas que facilitan las tareas de gestión a los operadores humanos y posibilitan minimizar el número de éstos.

La práctica totalidad de los sistemas de gestión que existen actualmente, utilizan una estructura básica, conocida por paradigma gestor-agente, cuyo esquema queda reflejado en la siguiente figura.

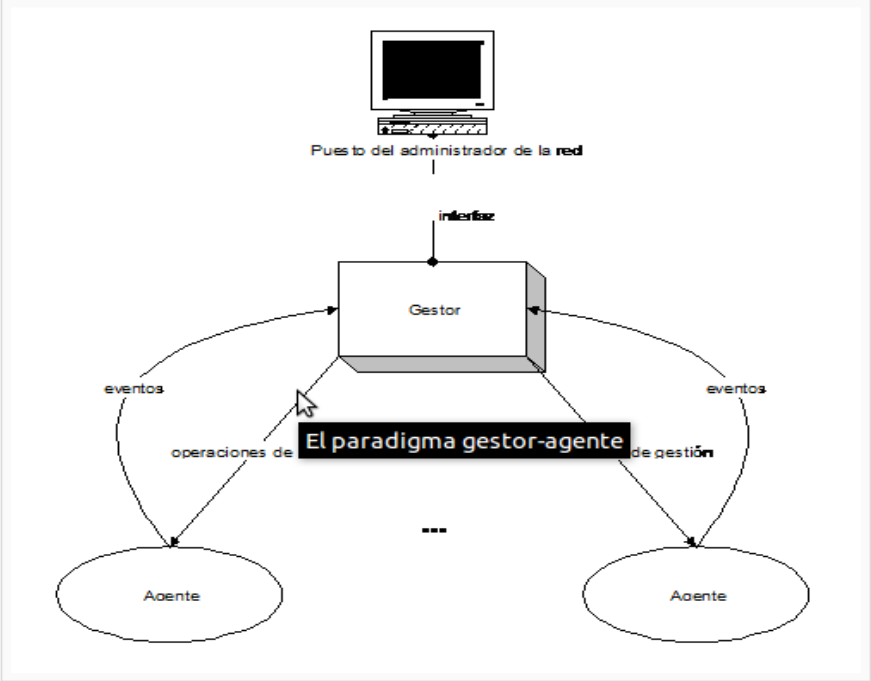


Figura 1.1. Paradigma gestor – agente.

Los sistemas de apoyo a la gestión se componen, por lo general:

- Interfaz con el operador o el responsable de la red. Esta interfaz a la información de gestión, a través de la cual el operador puede invocar la realización de operaciones de control y vigilancia de los recursos que están bajo su responsabilidad, es una pieza fundamental en la consecución de un sistema de gestión que tenga éxito. Se puede componer de alarmas y alertas en tiempo real, análisis gráficos y reportes de actividad.
- Elementos hardware y software repartidos entre los diferentes componentes de la red.

Los elementos del sistema de gestión de red, bajo el paradigma gestor-agente, se clasifican en dos grandes grupos:

- Los gestores son los elementos del sistema de gestión que interaccionan con los operadores humanos y desencadenan acciones necesarias para llevar ha cabo las tareas por ellos invocadas.

- Los agentes, por otra parte, son los componentes del sistema de gestión invocados por el gestor o gestores de la red.

El principio de funcionamiento reside en el intercambio de información de gestión entre nodos gestores y nodos gestionados. Habitualmente, los agentes mantienen en cada nodo gestionado información acerca del estado y las características de funcionamiento de un determinado recurso de la red. El gestor pide al agente, a través de un protocolo de gestión de red, que realice determinadas operaciones con estos datos de gestión, gracias a las cuales podrá conocer el estado del recurso y podrá influir en su comportamiento.

Cuando se produce alguna situación anómala en un recurso gestionado, los agentes, sin necesidad de ser invocados por el gestor, emiten los denominados eventos o notificaciones que son enviados a un gestor para que el sistema de gestión pueda actuar en consecuencia.

1.2.3.1. EL GESTOR.

Gestor: Es una estación de trabajo donde se ejecutan las aplicaciones de gestión de red, que disponen de interfaces gráficas para presentar información al usuario y para facilitarle la invocación de operaciones de gestión. Es la parte de la aplicación que emite las directivas de operaciones de gestión y recibe notificaciones y respuestas. Este se implementa en una estación de gestión.

Integran la información asociada con varios sistemas gestores de elementos, usualmente ejecuta una correlación de alarmas entre los diversos gestores de elementos. En estos sistemas se debe recolectar la información necesaria acerca de la fuente (objeto gestionado), reducirla a algo significativo y presentarla en la consola central para su análisis.

1.2.3.2. EL AGENTE.

El agente es el equipamiento lógico alojado en un dispositivo gestionable de la red. Almacena datos de gestión y responde a las peticiones sobre dichos datos. Cuya función es, por un lado, recoger información de los eventos que se producen en el

dispositivo, y por otro comunicarse con el gestor.

La comunicación puede producirse de dos maneras:

1. El gestor puede preguntar al agente acerca del valor de alguna variable

2. El agente puede informar al gestor acerca de algún hecho importante.

El gestor, además de poder leer el contenido de las variables del agente, puede modificar su valor. El conjunto global podría resumirse en el siguiente gráfico:

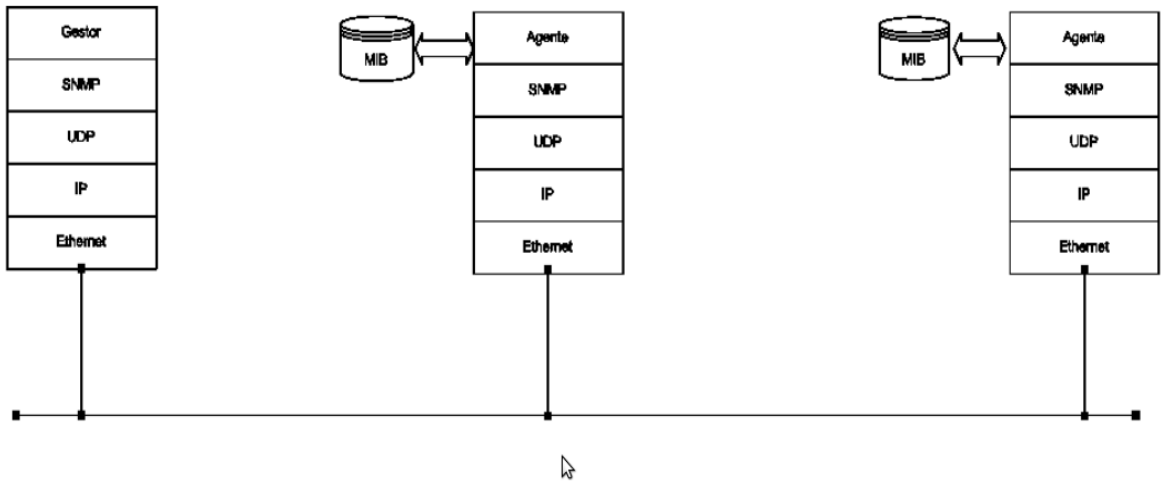


Figura 1.2. Gestor - Agente

1.2.3.3. PROTOCOLO DE GESTIÓN DE REDES.

La mayor parte de los sistemas operativos de red ponen los protocolos adecuados para realizar una gestión de red. Son escasos los sistemas que proporcionan una consola de análisis de lo que está ocurriendo en la red; normalmente, este software suele ser suministrado por terceras compañías. Empieza a ser habitual que la gestión de dispositivos de red se realice a través del navegador de Internet. Bastantes dispositivos que se conectan a la red incorporan, además de su funcionalidad propia, un pequeño servidor web que sirve para configurarlo y administrarlo. En la actualidad, los protocolos de gestión de red se encuentran en plena evolución.

Los protocolos de gestión de red definen la comunicación entre los nodos gestionados y las estaciones gestoras. El protocolo depende del modelo de gestión utilizado. Uno de los protocolos de gestión de red mas utilizados es SNMP.

SNMP son las siglas de “Simple Network Management Protocol”, es un protocolo que permite realizar la gestión remota de dispositivos. El predecesor de SNMP, SGMP (Simple Gateway Management Protocol) fue diseñado para administrar routers, pero SNMP puede administrar prácticamente cualquier dispositivo, utilizando para ello comandos para obtener información y para modificar la información. Este protocolo ha sido definido por la IETF, para lo cual ha publicado una serie de RFCs.

SNMP es un protocolo de nivel de aplicación para consulta a los diferentes elementos que forma una red, (*routers, switches, hubs, hosts, módems, impresoras, etc.*). Cada equipo conectado a la red ejecuta unos procesos (**agentes**), para que se pueda realizar una administración tanto remota como local de la red. Dichos procesos van actualizando *variables* (manteniendo históricos) en una base de datos, que pueden ser consultadas remotamente.

Por ejemplo, en el caso de:

- Un **router**: interfaces activos, la velocidad de sus enlaces serie, número de errores, bytes emitidos, bytes recibidos
- En una **impresora**: que se terminó el papel
- En un **modem**: la pérdida de conexión, etc.
- En un **switch**: bocas conectadas, desconectar una boca en el caso de IPs duplicadas, si la máquina está infectada de virus, etc.

Por la forma en la que el protocolo está implementado, se distinguen dos entidades: estaciones administradoras y elementos de la red. Una estación administradora es un servidor que, por medio de un programa, realiza la gestión de los dispositivos por medio de comandos y consultas SNMP. El programa que realiza la gestión es denominado NMS (Network Management System). Por otro lado en los elementos a administrar residen los agentes, que son los que responden los mensajes y realizan las acciones indicadas por el NMS.

El protocolo SNMP corresponde a la capa de aplicación del modelo de referencia OSI. Los datagramas correspondientes a este protocolo viajan sobre UDP utilizando normalmente el puerto 161 para mensajes y el 162 para traps. El utilizar UDP implica que no se establece una sesión entre el NMS y los agentes, lo cual hace que las transmisiones sean más rápidas y que la red no se sobrecargue, pero también implica que el que envía los mensajes debe, por algún medio, asegurar que este ha sido recibido, en el caso del sondeo el NMS puede esperar un tipo por la respuesta y, en caso esta no se reciba, se puede reenviar el paquete. El problema se da en el caso de los traps, ya que el agente no espera ninguna respuesta del NMS, entonces el trap puede perderse y ninguno de los equipos es notificado.

El protocolo SNMP define la forma más básica para el intercambio de información de gestión de redes donde existen: un gestor, agentes y bases de información de gestión.

La simplicidad que presenta produce deficiencias para transferir grandes cantidades de información, poca o ninguna seguridad, entre otras cosas.

El protocolo SNMP funciona en la capa aplicación. SNMP ofrece un entorno de trabajo estandarizado y un lenguaje común empleado para la monitoreo y gestión de los dispositivos de una red, éste entorno consta de tres partes:

- Gestor SNMP.
- Agente(s) SNMP.
- MIB (Base de Información de Gestión).

El protocolo SNMP proporciona un formato de mensajes para el intercambio de información entre gestores y agentes de SNMP, ya que funciona bajo el ambiente cliente/servidor.

Los agentes SNMP emplean el puerto UDP (Protocolo de Datagramas de Usuario) 161, donde mantienen la escucha de peticiones por parte del gestor SNMP. El gestor por medio del puerto UDP 162 recibe las notificaciones que genera el o los agentes y en donde debe existir un proceso gestor de interrupciones (trap manager) que las procese.

A continuación se muestra la los componentes del protocolo SNMP.

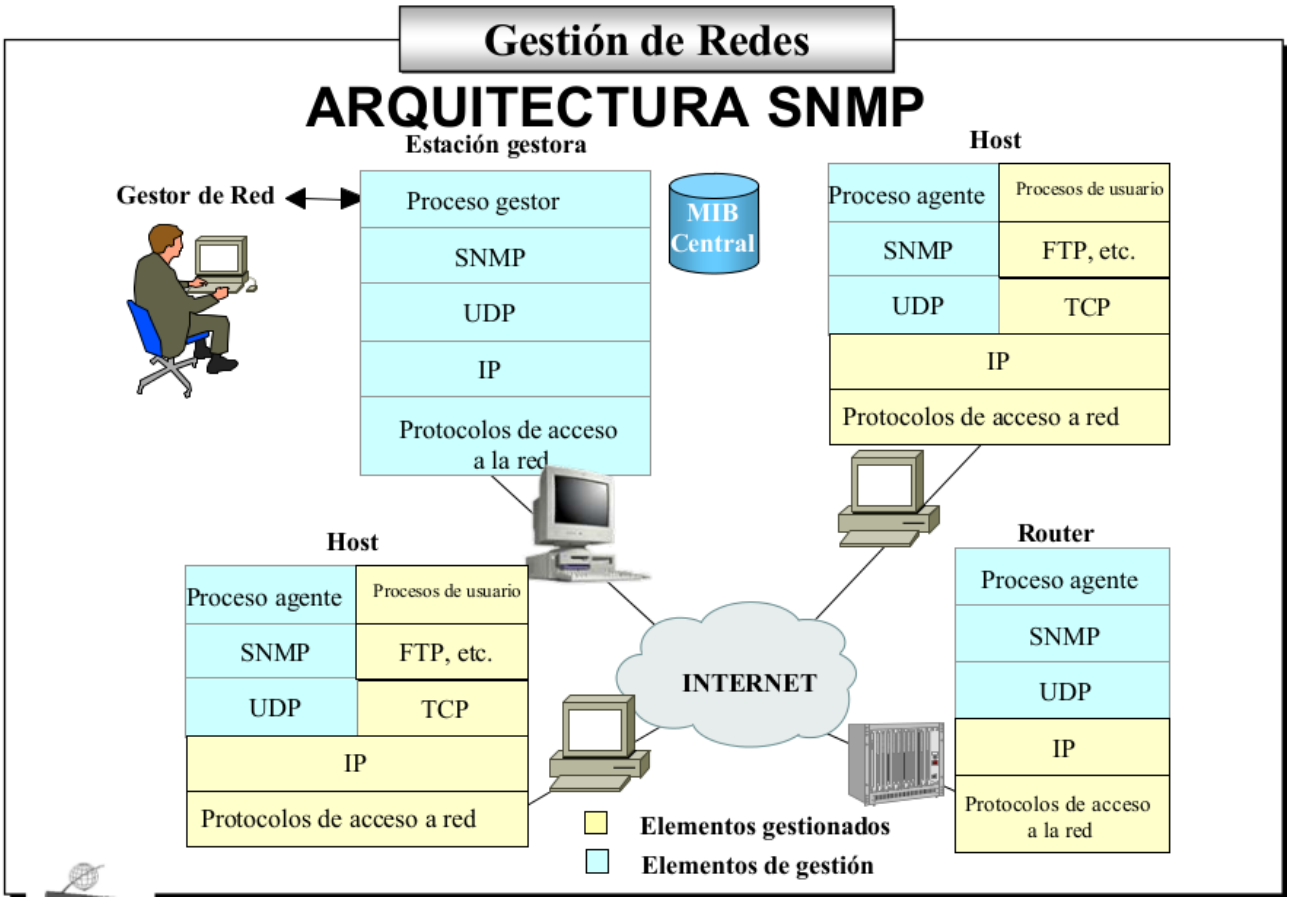


Figura 1.3. Arquitectura del protocolo de gestión de red SNMP.

1.2.4. IMPORTANCIA Y BENEFICIOS DE LA GESTIÓN DE RED.

La gestión de red es un proceso eminentemente en el cual se observa el estado y comportamiento de la configuración de red y sus componentes. Además de agrupar todas las operaciones para la obtención de datos acerca del estado de los recursos de la red. Las funciones de la gestión de red se llevan a cabo por agentes que realizan el seguimiento y registro de la actividad de red, la detección de eventos y la comunicación de alertas.

La Organización Internacional de Estándares ISO (International Organization for Standardizations) ha definido la arquitectura de Administración OSI (Open System Interconnection), cuya función es permitir supervisar, controlar y mantener una red

de datos. Ésta arquitectura de administración se basa en áreas funcionales y/o específicas de gestión.

Entre los principales beneficios en la gestión de red está: medir la calidad de funcionamiento, proveer información disponible del desempeño de la red (hardware y software), asegurar que la capacidad y prestaciones de la red correspondan con las necesidades de los usuarios, analizar y controlar parámetros como: utilización, rendimiento, tráfico, cuellos de botella, tiempo de respuesta, tasa de error, throughput, etc.; esto de los distintos componentes de red como switches, ruteadores, hosts, etc., para poder ajustar los parámetros de la red, mantener el funcionamiento de la red interna en un nivel aceptable, poder efectuar análisis precisos y mantener un historial con datos estadísticos y de configuración, predecir puntos conflictivos antes de que éstos causen problemas a los usuarios.

El conocimiento de esta información nos permite en el futuro tomar acciones correctivas como balanceo o redistribución de tráfico, establecer y reportar tendencias para ser utilizadas en la toma de decisiones y planificación del crecimiento. Se debe definir claramente los parámetros de funcionamiento o desempeño alrededor de los cuáles, se van a organizar las tareas de gestión de prestaciones, tales como:

- Obtención de la información de funcionamiento de la red a través del monitoreo sobre los recursos disponibles.
- Análisis de la información recolectada para determinar los niveles normales de utilización de la red.
- Comparación entre los valores obtenidos y los normales, para generar acciones de inicio de alarmas que pueden generar la toma de medidas preventivas o correctivas

1.3. SISTEMAS DE GESTIÓN Y ADMINISTRACIÓN DE RED.

1.3.1. EVOLUCIÓN DE LA GESTIÓN DE RED.

Durante los años del monopolio, con la gestión de red se buscaba, además de encontrar y solucionar problemas, automatizar de forma remota y centralizada aquellas tareas que suponían para los operadores la dedicación de mucho tiempo y, generalmente, el desplazamiento físico del personal técnico, como efectuar cambios en la configuración de los equipos o gestionar su rendimiento. La liberalización de los antiguos monopolios de telecomunicaciones, a finales de los años 90, introdujo grandes cambios en la gestión de red, haciéndose necesario, entre otras cuestiones, controlar un número creciente de equipos y tecnologías de diferentes suministradores, e introducir nuevos servicios de forma gradual. La gestión de redes surgió con las redes mismas puesto que siempre hubo necesidad de controlar, configurar, etc., los recursos de interconexión. Ahora bien, al igual que las redes han ido cambiando, los sistemas de gestión también han ido evolucionando con el paso del tiempo. Básicamente se pueden distinguir tres etapas fundamentales en la evolución de los sistemas de gestión: gestión autónoma, gestión homogénea, gestión heterogénea.

Un sistema de gestión opera bajo los siguientes pasos básicos:

1.- Colección de información acerca del estado de la red y componentes del sistema. La información recolectada de los recursos debe incluir: eventos, atributos y acciones operativas.

2.- Transformación de la información para presentarla en formatos apropiados para el entendimiento del administrador.

3.- Transportación de la información del equipo monitoreado al centro de control.

4.- Almacenamiento de los datos coleccionados en el centro de control.

5.- Análisis de parámetros para obtener conclusiones que permitan deducir rápidamente lo que pasa en la red.

6.- Actuación para generar acciones rápidas y automáticas en respuesta a una falla mayor.

La característica fundamental de un sistemas de gestión de red moderno es la de ser un sistema abierto, capaz de manejar varios protocolos y lidiar con varias arquitecturas de red. Esto quiere decir: soporte para los protocolos de red más importantes, en la actualidad existe más de un protocolo dedicado a la gestión de redes, desde estándares propietarios como NBAR de Cisco y por otro lado protocolos completamente abiertos como el SNMP. Al ser este accesible a cualquier persona o empresa este último está mucho más difundido y se puede encontrar todo tipo de equipos que lo implementan. Dentro del contexto de una red se puede administrar los equipos encargados de su funcionamiento como equipos de red, así como equipos servidores y los servicios que corren dentro de ellos. Además también es posible incluir dentro de la administración otros equipos adicionales, como los UPS, controladores de temperatura, etc.

La gestión de redes está enfocada a controlar el funcionamiento y mantenimiento utilizando un conjunto de protocolos y técnicas que conjuntamente aplicadas pueden garantizar el correcto funcionamiento de una red, los sistemas de gestión de red están diseñados para ver la red como una arquitectura unificada, con direcciones y etiquetas asignadas a cada punto de red (nodo de red) capas de abarcar actividades que permitan a los gestores de red la planificación, organización, control del uso de los servicios de la red. Los protocolos para la administración de redes especifican modelos para facilitar la gestión, los principales modelos de gestión de redes son:

- Modelo OSI.
- Modelo TCP/IP o SNMP.
- Modelo TMN.

1.3.1.1. GESTIÓN AUTÓNOMA.

Las redes autónomas denominadas así por que estaban constituidas por pocos componentes y/o nodos de red, en éste tipo de redes cada nodo de red tenia un sistema de gestión de red local. Las decisiones que afectaban a más de un nodo implicaban la comunicación con cada uno de los administradores correspondientes.

1.3.1.2. GESTIÓN HOMOGÉNEA.

Con el advenimiento de nuevas tecnologías las redes fueron incrementando el número de componentes y de nodos de red y con ello las redes sufrieron un incremento considerable de tamaño, pero siempre utilizando máquinas, equipos y protocolos de un mismo fabricante, ese mismo fabricante diseñaba su propio sistema de gestión que casi siempre estaba dedicado a un único nodo de red centralizado.

En redes homogéneas, un computador de un fabricante posee un conjunto de reglas específicas diseñadas para usar la solidez de los sistemas operativos y arquitecturas de hardware propias del fabricante.

1.3.1.3. GESTIÓN HETEROGÉNEA.

En la actualidad las redes han ido creciendo y evolucionando en la implementación de nuevas y variadas tecnologías, los entornos de red homogéneos ya no son posibles mas bien en la misma red se encuentran elementos fabricados por diversos proveedores que necesariamente deben compartir y operar entre si, de ésta forma se ha conseguido aumentar los servicios ofrecidos por las redes a la vez que los explotadores de las mismas han podido maximizar el rendimiento de sus inversiones. Esta evolución de las redes ha traído consigo la necesidad de que coexistan sistemas de gestión de red de muy diversa naturaleza.

El objetivo de la gestión heterogénea es dar un servicio de comunicación de datos que involucre diversas redes con diferentes tecnologías de forma transparente para el usuario. Este concepto hace que las cuestiones técnicas particulares de cada red puedan ser ignoradas al diseñar las aplicaciones que administren todos estos servicios.

1.3.1.4. GESTIÓN INTEGRADA.

La integración permite en teoría la interconexión de redes de manera abierta de recursos de red y aplicaciones de gestión, administración y monitoreo de red, entre los diferentes componentes de los sistemas de gestión integrados está el de

normalizar las comunicaciones, esto tiene que ver con el hecho de establecer comunicación entre los nodos de la red y el sistema de gestión independientemente del tipo y la tecnología del nodo de red, y de el tipo de sistema de gestión.

La normalización de la información es otra de las características de los modelos de gestión de red integradas, el objetivo es conseguir una definición sintácticamente uniforme de todos los elementos de la red, independientemente del fabricante.

1.3.2. MODELO DE GESTIÓN OSI.

La gestión OSI es una posibilidad a los sistemas de gestión integrada y son la base para ala comprensión de otras soluciones de gestión, el marco de gestión OSI propone tres formas distintas de llevar a cabo la gestión de entornos OSI, de manera que tenga cabida en éste marco las distintas formas de realizar la gestión.

Administración de la red significa diferentes cosas para diferentes personas. En algunas situaciones, comprende a un asesor de redes solitario supervisando la actividad con un analizador de protocolos obsoleto. En otras situaciones, la administración de la red puede involucrar una base de datos distribuida, auto-sondeo de los dispositivos de la red y estaciones de trabajo avanzadas que generan visualizaciones gráficas en tiempo real de los cambios de topología y del tráfico de la red. En general, la administración de la red es un servicio que emplea una variedad de herramientas, aplicaciones y dispositivos para ayudar a los administradores de red a supervisarlas y mantenerlas.

Antes de continuar con las formas de gestión en entornos OSI, se hará una breve explicación de un entorno OSI y su modelo de referencia.

El modelo de referencia OSI[3] proporciona un lenguaje común para los administradores de redes. Cuando se utiliza un enfoque sistemático en la documentación y en las arquitecturas de red, el modelo OSI es dominante en la solución de problemas de la red. El modelo permite que la solución de problemas se

3 *OSI.- Modelo de interconexión de sistemas abiertos, modelo de red descriptivo creado por la ORGANIZACIÓN INTERNACIONAL PARA LA ESTANDARIZACIÓN ISO en el año de 1984.*

realice en una forma estructurada. Los problemas son normalmente descriptos en base a la capa del modelo OSI relacionada. Una revisión rápida del modelo OSI puede ayudar a clarificar su rol en la metodología de la solución de problemas.

Los Protocolos de Internet (IPs) pueden ser usados para comunicarse a través de cualquier conjunto de redes interconectadas. La suite de Internet incluye especificaciones de capa inferior como TCP[4] e IP[5], y también especificaciones para aplicaciones comunes como e-mail, emulación de terminal y transferencia de archivos. La siguiente figura muestra a las capas de la suite TCP/IP y sus relaciones con el modelo de referencia OSI.

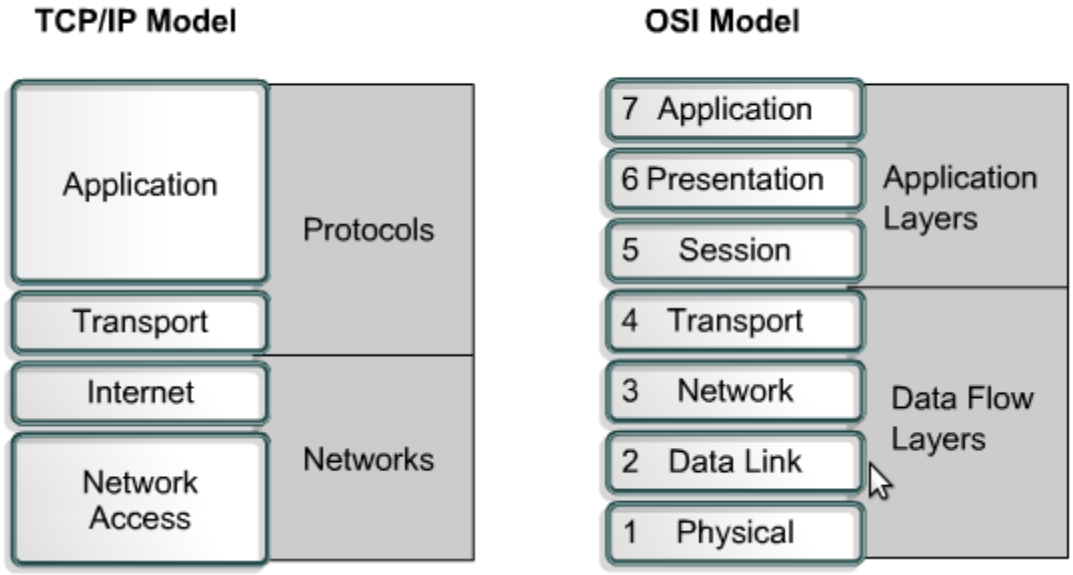


Figura 1.4. Modelo TCP/IP vs Modelo OSI

La ISO ha contribuido en mucho a la estandarización de la red. El modelo de administración de red ISO es el recurso principal para comprender las funciones más importantes de los sistemas de administración de red. Este modelo consiste en cinco áreas conceptuales, mostradas en la Figura 1.1.

4 *TCP.- Protocolo de control de transmisión es uno de los protocolos fundamentales en internet. Fue creado entre los años 1973 y 1974 por Vint Cerf y Robert Kahn.*

5 IP.- *Protocolo de internet para la comunicación de datos digitales.*

Cada capa está razonablemente auto-contenida, por lo que las tareas asignadas a cada una de ellas pueden ser implementadas en forma independiente. Esto permite que se puedan aplicar las soluciones ofrecidas por una capa sin afectar en forma adversa a las otras. El modelo OSI proporciona un marco de trabajo lógico y un lenguaje común usado por los administradores de redes para describir los escenarios de la red. La terminología de la Capa 1 a la Capa 7 es muy común.

El modelo de referencia OSI ofrece varias funciones entre las que tenemos:

- Proporciona una forma de entender cómo opera un sistema de gestión de redes.
- Sirve de guía o marco de trabajo para crear e implementar estándares de red, dispositivos y esquemas de gestión de red.

Estas son algunas de las ventajas de utilizar un modelo estructurado en capas:

- Separa la compleja operación de gestión de red en elementos más simples.
- Permite a los ingenieros centrarse en el diseño y desarrollo de funciones modulares.
- Proporciona la posibilidad de definir interfaces estándar para compatibilidad "plug-and-play" e integración multifabricante.

El modelo de referencia OSI consta de siete capas. Las cuatro capas de nivel inferior definen rutas para que los puestos finales puedan conectarse unos con otros y poder intercambiar datos. Las tres capas superiores definen cómo han de comunicarse las aplicaciones de los puestos de trabajo finales entre ellas y con los usuarios.

Las tres capas del modelo de referencia OSI se denominan habitualmente capas de aplicación. Estas capas están relacionadas con la interfaz de usuario, formatos y acceso a las aplicaciones. La figura 1.4 ilustra las capas superiores

Capa de aplicación. Es la capa de nivel superior del modelo. Aquí, el usuario o la aplicación dialoga con los protocolos para acceder a la red. Por ejemplo, se accede a un procesador de textos por el servicio de transferencia de archivos de esta capa.

Es la capa superior del OSI. Proporciona la interfaz entre las aplicaciones que utilizamos para comunicarnos y la red subyacente en la cual se transmiten los mensajes. Los protocolos de capa de aplicación se utilizan para intercambiar los datos entre los programas que se ejecutan en los hosts de origen y destino. Existen muchos protocolos de capa de aplicación y siempre se desarrollan protocolos nuevos.

Capa de presentación. La capa de presentación proporciona diversas funciones de conversión y codificación que se aplican a los datos de la capa de aplicación. Estas funciones aseguran que los datos enviados desde la capa de aplicación de un sistema podrán ser leídos por la capa de aplicación de otro sistema. Un ejemplo de funciones de codificación sería el cifrado de datos una vez que éstos salen de una aplicación. Otro ejemplo podrían ser los formatos de imágenes jpeg y gif que se muestran en páginas web. Este formato asegura que todos los navegadores web podrán mostrar las imágenes, con independencia del sistema operativo utilizado.

La capa de Presentación tiene tres funciones primarias:

1) Codificación y conversión de datos de la capa de aplicación para garantizar que los datos del dispositivo de origen puedan ser interpretados por la aplicación adecuada en el dispositivo de destino.
2) Compresión de los datos de forma que puedan ser descomprimidos por el dispositivo de destino.
3) Encriptación de los datos para transmisión y descifre de los datos cuando se reciben en el destino.

Las implementaciones de la capa de presentación generalmente no se vinculan con una stack de protocolos determinada. Los estándares para vídeos y gráficos son algunos ejemplos. Dentro de lo estándares más conocidos para vídeo encontramos QuickTime y el Grupo de expertos en películas (MPEG). QuickTime es una especificación de Apple Computer para audio y vídeo, y MPEG es un estándar para la codificación y compresión de vídeos.

Capa de sesión. La capa de sesión es la responsable de establecer, administrar y concluir las sesiones de comunicaciones entre entidades de la capa de presentación. La comunicación en esta capa consiste en peticiones de servicios y respuestas entre aplicaciones ubicadas en diferentes dispositivos. Un ejemplo de este tipo de coordinación podría ser el que tiene lugar entre un servidor y un cliente de base de datos.

Aplicación	Interfaz de usuario	Telnet HTTP
Presentación	Presentación de datos Proceso especial como cifrado	ASCII EBCDIC JPEG
Sesión	Mantener separados datos de distintas aplicaciones	Sistema operativo/ Programa de acceso a aplicaciones
Transporte		
Capa de red		
Enlace de datos		
Capa física		

Figura 1.5. Modelo OSI – CAPAS SUPERIORES

Las cuatro capas inferiores del modelo de referencia OSI son las responsables de definir cómo han de transferirse los datos a través de un cable físico, por medio de dispositivos de red, hasta el puesto de trabajo de destino y, finalmente, hasta la aplicación que está al otro lado.

Aplicación		
Presentación		
Sesión		
Transporte	Distribución fiable o no fiable Corrección de errores antes de enviar	TCP UDP SPX
Red	Proporcionar direccionamiento lógico para que los routers determinen las rutas	IP IPX
Enlace de datos	Combinar bits en bytes y bytes en tramas Acceso a medios con direcciones MAC Detectar(no corregir) errores	802.3 802.2 HDLC
Física	Trasladar bits entre dispositivos Especificar voltaje, velocidad y patillaje de cable.	EIA/TIA-232 V.35

Figura 1.6. Modelo OSI – CAPAS INFERIORES

Es responsabilidad de la pila de protocolo proporcionar comunicación entre los distintos dispositivos de la red. Una pila de protocolo es el conjunto de reglas que definen cómo ha de viajar la información a través de la red. Un ejemplo de esto podría ser TCP/IP. El modelo de referencia OSI proporciona un marco común necesario para la mayoría de las pilas de protocolo.

Cada capa del modelo permite que los datos circulen a través de la red. Estas capas intercambian información para proporcionar la debida comunicación entre los dispositivos de red. Las capas se comunican entre sí a usando unidades de datos del protocolo (PDU).Estas PDU[6] controlan información que se agrega a los datos del usuario. La información de control reside en campos denominados cabecera de información final. En la figura 1.7, la cabecera MAC (Control de accesoal medio) y la secuencia de verificación de trama (FCS) de la capa de enlace de datos representan una cabecera y una información final. Debido a que la PDU puede incluir información diferente según suba o baje por las capas, se le asignan nombres con arreglo al tipo de información que transporta. Por ejemplo, en la pila de protocolos TCP/IP, una vez que se ha agregado una cabecera TCP de capa de transporte a los datos de la capa superior, dicha unidad se denomina segmento. El segmento se baja entonces a la capa de red, donde se le añade una cabecera IP, convirtiéndose en un paquete. El paquete se inserta en una cabecera de capa, convirtiéndolo en una trama. Por último, la trama se convierte en bits y las señales eléctricas se transmiten a través del medio de la red.

Este método de bajar datos a la pila y agregar cabeceras e información final se denomina encapsulado. Una vez que los datos han sido encapsulados y pasados a través de la red, el dispositivo receptor quita toda la información agregada, usando los mensajes de la cabecera como instrucciones para subir los datos de la pila hasta la aplicación apropiada.

El encapsulado de datos es un concepto muy importante en redes. Su función es describir cómo comunican las capas de cada dispositivo, llamadas capas iguales, parámetros críticos como una dirección e información de control.

---

6 *Las **unidades de datos de protocolo**, se utilizan para el intercambio entre unidades disparejas, dentro de una capa del modelo OSI.*

Aunque el encapsulado puede parecer un concepto muy abstracto, en realizad es muy simple.

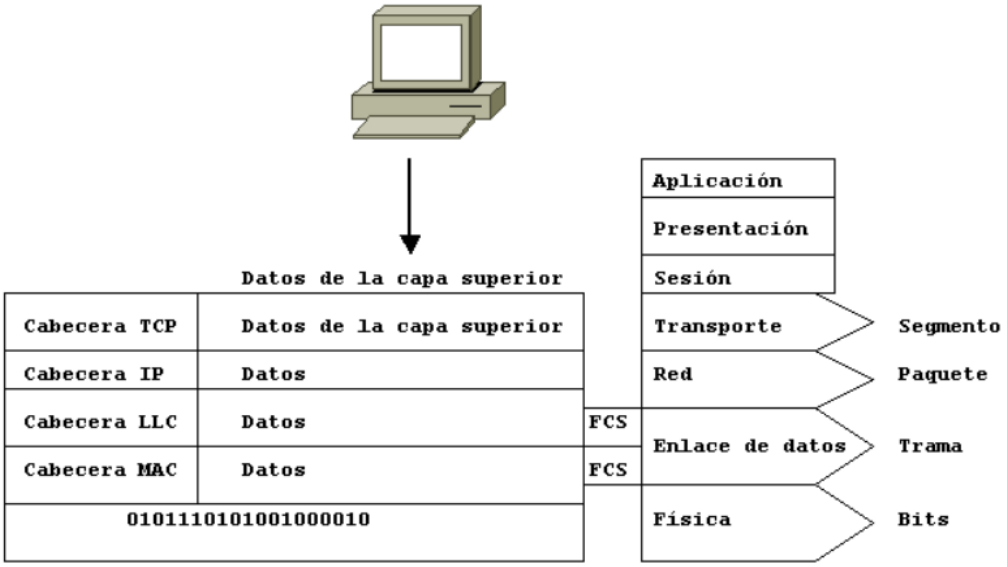


Figura 1.7. Modelo OSI – PROCESO DE ENCAPSULADO

La capa física define el tipo de medio, tipo de conector y tipo de señalización. Éste especifica los requisitos eléctricos, mecánicos, procedimentales y funcionales para activar, mantener y desactivar el vínculo físico entre sistemas finales. La capa física especifica también características tales como niveles de voltaje, tasas de transferencia de datos, distancias máximas de transmisión y conectores físicos. En el ejemplo que hemos usado anteriormente, la capa física sería la carretera por la cual se transporta la taza. La carretera es una conexión física entre diferentes ciudades que permiten ir de un sitio a otro. Cada carretera posee sus propias reglas, como las relativas al límite de velocidad o al peso, del mismo modo que cada medio de red posee su propio ancho de banda y unidad máxima de transmisión (MTU)[7].

La capa de enlace tiene la finalidad de proporcionar las comunicaciones entre puestos de trabajo en una primera capa lógica que hay por encima de los bits del cable. El direccionamiento físico de los puestos finales se realiza en la capa de enlace de datos con el fin de facilitar a los dispositivos de red la determinación de si deben subir un mensaje a la pila de protocolo. También hay campos en esta capa

7 *La unidad máxima de transferencia es un término de redes de computadores que expresa el tamaño en bytes de la unidad de datos más grande que puede enviarse usando un protocolo de comunicaciones.*

para indicar al dispositivo cual es la pila de la capa superior donde deben pasar los datos (como IP, IPX, Apple Talk, etc.). La capa de enlace de datos da soporte a servicios basados en la conectividad y no basados en ella, y proporciona la secuencia y control de flujo.

Para proporcionar estas funciones, la capa de enlace de datos está definida mediante dos subcapas: Subcapa de control de acceso al medio y Subcapa de control de enlace lógico. La Subcapa de control de acceso al medio (MAC) es la responsable de determinar cómo han de ser transportados los datos a través del cable físico. Ésta es la parte de la capa de vínculo de datos que se comunica hacia abajo con la capa física. En ella se definen funciones tales como el direccionamiento físico, topología de la red, disciplina de la línea, notificación de errores, distribución ordenada de tramas u control óptimo de flujo.

La Subcapa de control de enlace lógico (LLC) es la responsable de la identificación lógica de los distintos tipos de protocolos y el encapsulado posterior de los mismos para ser transmitidos a través de la red. LLC define servicios fiables y no fiables para la transferencia de datos, en lugar de la capa de transporte.

La capa de red define cómo tener lugar el transporte de tráfico entre dispositivos que no están conectados localmente en el mismo dominio de difusión. Para conseguir esto se necesitan dos elementos de información:

- Una dirección lógica asociada a cada puesto de origen y de destino.
- Una ruta a través de la red para alcanzar el destino deseado.

Los esquemas de direccionamiento lógico se utilizan para identificar redes y la ubicación de los dispositivos dentro del contexto de dichas redes. Estos esquemas varían en función del protocolo de capa de red que se utilice.

La capa de transporte define las directrices de la conexión entre dos puestos finales. Para poder conectar dos dispositivos en la construcción de una red, es necesario establecer una conexión o sesión. Una sesión constituye una conexión lógica entre las capas de transporte iguales en los puestos de origen y destino.

Los protocolos que operan en esta capa proporcionan diferentes funciones de capa de transporte. Concretamente, la capa de transporte define las funciones que se describen a continuación:

Permitir a los puestos finales ensamblar y desensamblar múltiples segmentos de capa superior en el mismo flujo de datos de la capa de transporte. Esto se consigue asignando identificadores de aplicación de capa superior. Dentro de la suite del protocolo TCP/IP estos identificadores se conocen como números de puerto. El modelo de referencia OSI denomina a estos identificadores como puntos de acceso al servicio (SAP). La capa de transporte utiliza estos números de puerto para identificar elementos de la capa de aplicación como FTP[8] o Telnet. Un ejemplo de número de puerto es el 23, que identifica la aplicación Telnet. Los datos con un número de puerto de transporte 23 serán destinados a la aplicación Telnet. Permitir a las aplicaciones solicitar transportes fiables de datos entre sistemas finales que están en comunicación. Los transportes fiables utilizan una relación orientada a la conexión entre los sistemas en comunicación para conseguir los siguientes objetivos:

- Asegurar que los segmentos distribuidos serán confirmados al remitente.
- Proporcionar la retransmisión de cualquier segmento que no sea confirmado.
- Colocar de nuevo los segmentos en su orden correcto en el puesto receptor.
- Proporcionar control y evitar congestiones.

En la capa de transporte, los datos pueden ser transmitidos de forma fiable o no fiable. Para IP, el protocolo TCP es fiable u orientado a conexión, mientras que UDP no es fiable, o independiente de la conexión.

Con el objetivo original de lograr la gestión de recursos de la torre de comunicaciones OSI, se han definido tres distintas formas de realizar tareas de gestión.

8 *Protocolo de Transferencia de Archivos, es un protocolo de red para la transferencia de archivos.*

1) **Gestión de Sistemas.-** Pretende llevar a cabo la gestión de una torre de comunicaciones OSI de una manera específica, por medio de protocolos de nivel de aplicación.
2) **Gestión de nivel.-** Este método de gestión OSI está pensando para permitir el intercambio de información de gestión entre equipos o elementos de red que no interactúan con toda los niveles de la torre de protocolos OSI, como por ejemplo un puente, un ruteador, etc.
3) **Operación o gestión en nivel.-** Su objetivo es controlar y monitorear una comunicación que atraviese un determinado nivel del modelo OSI.

Sin embargo, restricciones tales como que la gestión OSI solo se ocuparía de recursos con capacidad de comunicación y limitarla únicamente a entornos OSI, se decidió generar una nueva norma denominada visión general de la gestión de sistema, definida en la norma ISO[9]92, que ampliaba el ámbito de actuación y las funcionalidades de la gestión de sistemas definida en el marco de gestión OSI.

La gestión de sistemas se basa en el uso de protocolos del nivel de aplicación para el intercambio de información de gestión según el paradigma gestor-agente explicado anteriormente. La entidad agente se encarga de aplicar operaciones actuando sobre los denominados objetos gestionados, que son abstracciones de los recursos controlados a través de agentes.

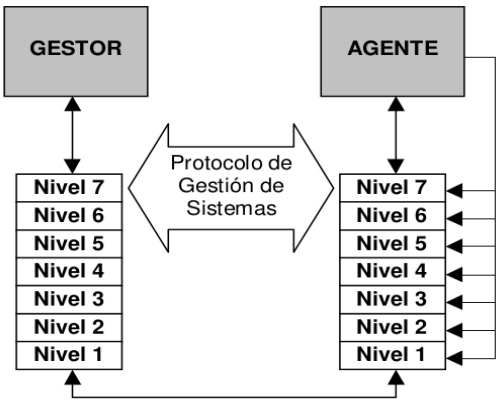


Figura 1.8. Modelo OSI – GESTIÓN DE SISTEMAS

9 *Organización internacional de normalización, 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.*

MODELO FUNCIONAL.

Define las funciones de gestión que proporcionan servicios básicos de gestión a las aplicaciones de gestión. Dichas funciones están sujetas a normalización, ejemplos de dichas funciones son informe de alarmas, control de registros, gestión de estados, monitoreo de ancho de banda, etc. El objetivo de estas funciones es ofrecer a las aplicaciones de gestión una funcionalidad un poco más elaborada que el simple acceso al protocolo de gestión, de ésta manera es posible desarrollar distintos tipos de aplicaciones de gestión que aprovechan estas funcionalidades.

MODELO DE ORGANIZACIÓN.

Es el modelo menos tratado en la normativa de gestión OSI , éste modelo tiene por objeto proporcionar pautas para dividir redes gestionadas en distintos dominios de gestión, basándose en los cómo está configurada la red, cómo están repartidas las funcionalidades de gestión, quién tiene el papel de gestor en la red o una mezcla de los anteriores.

MODELO DE COMUNICACIONES.

En el caso de la gestión de sistemas OSI se ha definido el protocolo común de información de gestión CMIP, está en la capa de aplicación del modelo OSI y proporciona el servicio común de información de gestión CMIS.

SERVICIOS DE OPERACIÓN.

Son servicios usados por el gestor para invocar operaciones de gestión a los agentes y permitir a estos devolver los resultados de dichas operaciones a los gestores, por ejemplo servicio como:

- M-GET: Pedir información de los objetos gestionados.
- M-SET: Modificar o añadir información en los objetos.
- M-ACTION: Llevar a cabo una acción por parte de un objeto.

- M-CREATE: Crear un nuevo objeto gestionado.
- M-DELETE: Eliminar un objeto gestionado.
- M-CANCEL-GET: Cancelar una petición anterior.

Así mismo se han definido una serie de métodos para poder invocar dicho servicio sobre un conjunto de objetos distintos:

- Scoping: Especifica el alcance o conjunto de objetos sobre los cuales se aplican un filtro.
- Filtrado: Operación que se va a aplicar a los atributos de todos los objetos seleccionados por el scoping.
- Sincronización: especifica el tipo de operación.

MODELO DE INFORMACIÓN

Para poder realizar una gestión integrada es necesario modelar de una manera común todos los recursos de comunicaciones susceptibles de ser gestionados remotamente.

El concepto básico del modelo de información OSI es el de objeto gestionado, que define como la abstracción de recursos de comunicación o de procesado de información, con el propósito de su abstracción, consiste en operaciones sobre el objeto, el resultado de dichas operaciones y notificaciones generadas por el recurso, informando un suceso especial.

Los conceptos utilizados para la estructura de información derivan de la Teoría de Diseño Orientado a objetos, una vez definidas las clases de objetos gestionados es necesario poder referirse a los ejemplares de esas clases por parte del gestor. Para ellos se utilizan los nombres de ejemplares o instancias, esto se basa en el concepto de jerarquía de agregación en la que unos objetos superiores contienen a otros subordinados, esta jerarquía da lugar al denominado árbol de información de gestión MIT (Management Information Tree).

Para especificar la organización de la jerarquía, la definición de una clase debe ir acompañada de la enumeración de las clases cuyos ejemplares pueden ser superiores de un ejemplar de la clase que se define, ésta parte de la definición se denomina ligadura de nombrado.

1.3.3. MODELO DE GESTIÓN TMN.

TMN (Telecommunications Management Network) fue introducido por la ITU-(International Telecommunications Union – Telecommunication sector) en 1988.Para conseguir el desarrollo de entornos de gestión distribuidos y heterogéneos. TMN proporciona una arquitectura en capas para todas las funciones de las aplicaciones de gestión de red, además de los protocolos de comunicación entre los elementos de red y el gestor centralizado de red, entre distintos gestores de red y los operadores humanos.

Sin embargo, TMN presenta también muchos inconvenientes, destacando: su complejidad, que se basa en un sistema de computación distribuida relativamente antiguo, que sólo contempla una extensión de CMIP como protocolo de gestión de red (no soporta SNMP), y que el protocolo de transporte de datos que emplea es X.25 (no admite TCP/IP). Por ello, y a la espera de que estas limitaciones sean solventadas en versiones posteriores, es empleado principalmente como marco de referencia para el desarrollo de herramientas de gestión de red.

TMN define también una serie de funciones de gestión, distinguiendo claramente las que se encuentran en el gestor local y las que lo hacen en el gestor de red. El gestor local es el software encargado de la configuración de los elementos de red, y puede ser utilizado en las dependencias locales. El gestor de elemento es el software utilizado en el centro de supervisión remoto para realizar la gestión de fallos, configuración, contabilidad, rendimiento y seguridad (conocida como FCAPS en terminología TMN), sin considerar la topología de la red (enlaces, circuitos, etc.). El gestor de subred, integrado en muchas ocasiones en la misma plataforma que el gestor de elemento, es utilizado para manejar todas las áreas funcionales definidas en FCAPS, incluyendo la provisión de circuitos y la representación de la topología de la red.

ARQUITECTURA TMN

La arquitectura TMN debe estar orientada hacia la cooperación entre la gestión de los sistemas individuales para conseguir un efecto coordinado sobre la red. Para ello, en TMN se define un conjunto de arquitecturas situadas a diferente nivel de abstracción. El modelo TMN define cuatro arquitecturas diferenciadas.

1) Arquitectura Funcional: Describe una distribución de la funcionalidad de gestión en TMN. Se basa en la definición de un conjunto de bloques funcionales, que son

- Bloque Funcional de Sistema de Operación (Operations System Function, OSF). Funciones típicas de un gestor en el paradigma Gestor-Agente.
- Bloque Funcional de Elementos de Red (Network Element Function, NEF).Funcionalidades de los equipos de la red que les permiten funcionar como agentes de gestión.
- Bloque Funcional de Estación de Trabajo (Work Station Function, WSF). Proporciona los medios para conectar al usuario con el sistema de operaciones, permitiéndole interpretar la información de gestión de TMN.
- Bloque Funcional de Adaptador Q (Q Adaptor Function, QAF). Permite que TMN pueda gestionar elementos de red que posean un sistema de gestión propietario.
- Bloque Funcional de Mediación (Mediation Function, MD). Actúa sobre la información que llega de los NEF y de los QAF para adaptarla, filtrarla y condensarla adecuándola al formato utilizado por los OSF.

2) Arquitectura Física.- Se encarga de definir como se implementan los bloques funcionales mediante equipamiento físico y los puntos de referencia en interfaces. Se definen los siguientes bloques constructivos:

- Sistemas de operaciones (OS).
- Redes de comunicaciones de datos (DCN).
- Dispositivos mediadores (MD).

- Estaciones de trabajo (WS).
- Elementos de red (NE).
- Adaptadores Q (QA).

3) Arquitectura Organizativa.- Tiene por objeto introducir una relación jerárquica entre los diferentes gestores (sistemas de operación) que existen en una red TMN de manera que haya gestores de bajo nivel más orientados a la resolución de problemas técnicos de los recursos y gestores de más alto nivel, orientados a garantizar calidades de servicio. Para ello se divide el bloque funcional OSF en capas; la comunicación entre bloques de diferentes capas se lleva a cabo mediante una relación gestor-agente a través de un punto de referencia.

4) Arquitectura de Información.- Describe conceptos que tiene que estar adoptado por la administración del modelo OSI.

FUNCIONES ASOCIADAS A UN MODELO DE GESTIÓN TMN.

En lo que respecta al área funcional de gestión de TMN, se lista cinco funciones de gestión.

1) **Gestión de Performance.-** La gestión de performance (algunas veces también referida como gestión de tráfico y performance) 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.
2) **Gestión de Fallas (Mantenimiento)**.- La gestión de fallas de mantenimiento es un conjunto de funciones las cuales habilitan la detección, aislamiento, y corrección de operaciones anormales en la red de telecomunicaciones 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 ello está apuntado, primero que nada, a explorar los errores y ser capaces de repararlos en el tiempo más corto posible.

3) **Gestión de Configuración.-** La gestión de configuración provee funciones para operar, controlar, identificar, y colectar datos desde o proveer datos a elementos de red. En la práctica de gestión de redes actuales de, la gestión de configuraciones generalmente incluye dos funciones esenciales lógicamente diferentes; gestión de configuración estática, y dinámica. La gestión de configuración estática involucra la asignación y desasignación de elementos de red o desde la red lógicamente, 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. La gestión de configuración dinámica involucra el establecimiento de las rutas actuales para las interconexiones requeridas vía red. Esto implica la reconfiguración de la red mediante el establecimiento de una posible nueva ruta, si la ruta actual desaparece, o bien 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.

4) **Gestión de Contabilidad.-** La gestión de contabilidad 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.

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 contraseñas, 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.

1.3.3. MODELO DE GESTIÓN DE TELECOMUNICACIONES TOM / e-TOM.

Es un modelo de gestión de red creado por el TeleManagement Forum, Mapa de Operaciones de Telecomunicaciones (TOM) fue creado para sustituir al modelo de gestión de redes de telecomunicaciones (TMN).

La extensión del Mapa de Operaciones de Telecomunicaciones (enhanced Telecom Operations Map) eTOM es la versión actual de este modelo. En el eTOM se describe toda la gama de procesos de negocio requeridos por un proveedor de servicios y se definen los elementos clave y cómo interactúan. eTOM ha sido adoptado como la recomendación internacional de UIT-T[10]. eTOM fue diseñado y desarrollado para describir los procesos de las empresas en el sector de la Telecomunicaciones. Dado su éxito y amplio uso por los proveedores de servicio y los desarrolladores de aplicaciones fue rápidamente adoptado por la Unión Internacional de Telecomunicaciones (UIT). A pesar de todo esto su alcance se ha extendido más allá, ya que otras empresas fundamentalmente en el área de los servicios han comenzado ha utilizar los principales conceptos de eTOM, sobre todo los expuestos en los niveles superiores. eTOM pretende estandarizar los conceptos de los procesos y darles estructura coherente, para lo cual abarca tres grandes áreas: Gestión Empresarial, Estrategia-Infraestructura-Productos, y Operaciones. En las áreas de Operaciones y Estrategia-Infraestructura-Productos existen divisiones verticales y horizontales: las verticales representan flujos de procesos extremos a extremo pasando por las capas horizontales de Interfaz con el cliente,

10 ***Normalización de las Telecomunicaciones de la UIT (UIT-T)*** *es el órgano permanente de la Unión Internacional de Telecomunicaciones (UIT) que estudia los aspectos técnicos, de explotación y tarifarios y publica normativa sobre los mismos.*

servicios, recursos e interfaz con los socios y proveedores.

La importancia de eTOM como marco referencial de procesos, se determina por el valioso aporte que da a todas aquellas personas interesadas en conocer los procesos de negocio de uno de los sectores sino el más pujante de la industria, nos referimos a las Telecomunicaciones.

El eTOM se encuentra organizado en tres áreas de procesos:

1. Estrategia, Infraestructura y Producto, que cubre la planificación y la gestión de los ciclos de vida. El eTOM agrega esta área al mapa de procesos, con el propósito de destacar los procesos de planificación y desarrollo, de los operacionales, que están más relacionados con el día a día del negocio.

El Área de Procesos de Estrategia, Infraestructura y Producto incluye los procesos que desarrollan la estrategia, comprometen a la empresa, construyen la infraestructura, desarrollan y gestionan los productos, y los que desarrollan y gestionan la Cadena de suministro. En el eTOM, la infraestructura se refiere a algo más que sólo la infraestructura de tecnología de información y recursos que soporta los productos y servicios. Incluye la infraestructura requerida para soportar los procesos funcionales, como la Gestión de las Relaciones con el Cliente (CRM). Estos procesos dirigen y hacen posible los procesos de Operaciones.

2. Operaciones, que cubre el núcleo de la gestión operacional. El eTOM recoge los procesos operacionales establecidos por el TOM, los cuales constituyen los procesos end-to-end fundamentales de Aprovisionamiento, Aseguramiento, y Facturación, agrupándolos en el área de Operaciones del nuevo mapa. El Área de Procesos de Operaciones es el corazón del eTOM. Incluye todos los procesos de operaciones que soportan las operaciones y la gestión del cliente, así como también aquellos que hacen posible las operaciones directas con el cliente. Estos procesos incluyen los del día a día y los de soporte y alistamiento de operaciones. La vista del eTOM de las Operaciones también incluye la gestión de ventas y la gestión de las relaciones con el proveedor/aliado.

3. Gestión Empresarial, que cubre la gestión corporativa o de soporte al negocio. En esta área se concentran los procesos que toda empresa debe tener para su normal funcionamiento. El Área de Procesos de Gestión Empresarial incluye los procesos de negocio básicos requeridos para que cualquier negocio funcione. Estos procesos se enfocan en los procesos del Nivel de Empresa, metas y objetivos dichos procesos tienen interfaces con casi todos los otros procesos en la empresa, ya sean operacionales, de producto o de infraestructura. Son considerados algunas veces funciones y/o procesos corporativos, como la Gestión Financiera, los procesos de Gestión de Recursos Humanos, etc.

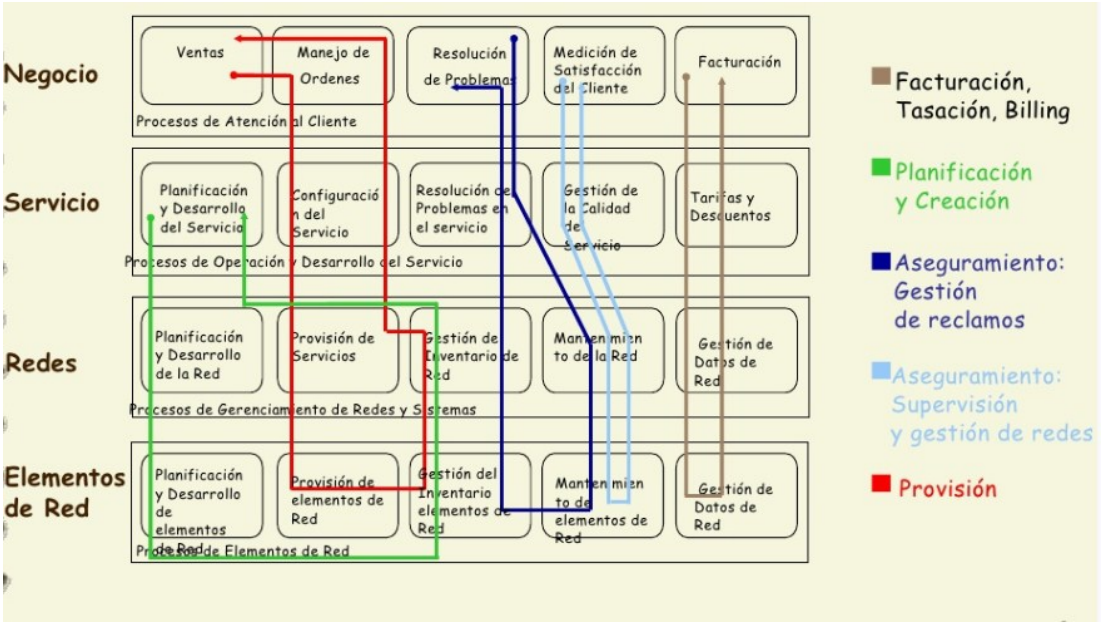


Figura 1.9. MODELO DE GESTIÓN - eTOM

El eTOM también ha definido cuatro áreas funcionales que, de alguna manera, corresponden con los cuatro niveles de la Arquitectura Lógica definidos en el modelo de Red de Gestión de las Telecomunicaciones (RGT) y afinan los grupos de procesos definidos en su antecesor, el TOM. Estas áreas son:

- Los procesos de Mercado, Producto y Cliente, incluyen aquellos relacionados con la gestión de ventas y canales, gestión de mercadeo, y gestión de productos y ofertas, así como también la Gestión de las Relaciones con el Cliente, el manejo de órdenes y problemas, la gestión de Acuerdos de Niveles de Servicio (ANS) y la facturación.

- Los procesos de Servicio incluyen aquellos relacionados con el desarrollo y configuración de servicios, gestión de problemas y análisis de calidad de los servicios, y tarifación.
- Los procesos de Recursos incluyen los que tienen que ver con el desarrollo y la gestión de la infraestructura de la empresa, ya sea relacionada con los productos y servicios, o con el soporte de la empresa en sí.
- Los procesos del Proveedor/Aliado incluyen los relacionados con la interacción de la empresa con sus proveedores y aliados. Esto involucra tanto los procesos que gestionan la Cadena de Suministro que soporta los productos y la infraestructura, como aquellos que soportan la interfaz de Operaciones con sus proveedores y aliados.

eTOM es ampliamente utilizado en la industria de servicios debido a sus beneficios, entre los cuales tenemos:

Proporciona la base para la comprensión de tecnologías informáticas, carteras de aplicaciones para procesos de negocio.

Sienta las bases para la estructura, clasificación y terminología de los diferentes procesos de negocio y sus bloques de construcción.

Permite la formación de un rendimiento superior de extremo a extremo de los flujos de procesos que pueden dar lugar a mejoras en los costos y el rendimiento y también lograr la reutilización en los procesos y sistemas existentes.

1.3.4. MODELO DE GESTIÓN DE GESTIÓN RED INTERNET O SNMP.

El modelo de gestión SNMP proporciona una manera sistemática de supervisar y administrar una red informática, de ésta manera se puede decir que SNMP es un estándar de facto para la administración de redes.

SNMP, en sus distintas versiones, es un conjunto de aplicaciones de gestión de red que emplea los servicios ofrecidos por TCP/IP y que ha llegado a convertirse en un estándar. Surge a raíz del interés por encontrar un protocolo de gestión que fuese válido para la red Internet.

El modelo de gestión SNMP de una red administrada consta de cuatro componentes:

1. Nodos administrados.
2. Estaciones administradas.
3. Información de administración.
4. Un protocolo de administración.

El Modelo de Administración Internet o SNMP depende de que en cada dispositivo de de red a administrar existan agentes SNMP Protocolo Simple de Administración de Red (Simple Network Management Protocol), que principalmente se encargan de la recolección de la información sobre dicho dispositivo, ésta información se puede dividir en tres tipos:

1) Información de estado.
2) Advertencias.
3) Alarmas.

La información que los agentes recogen, la envían a una aplicación central que controla el sistema. Esta se compone de una base de datos jerárquica o MIB (Management Information Base), por un lado, y una consola de administración, por el otro.

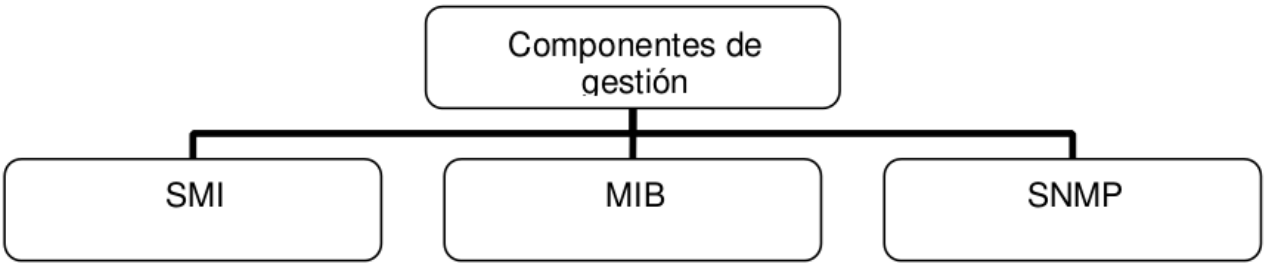


Figura 1.10. MODELO DE GESTIÓN SNMP – COMPONENTES

Los periféricos que tienen integradas las capacidades para SNMP ejecutan un paquete de software agente para administración, cargado como parte de un ciclo de arranque o incrustado en la memoria fija (firmware) del dispositivo. Estos dispositivos que tienen **Figura** SNMP se denominan dispositivos administrados.

Los dispositivos administrados por SNMP se comunican con el software servidor SNMP que está localizado en cualquier parte de la red. El dispositivo se comunica con el servidor de dos formas: por sondeo o por interrupción. El administrador SNMP maneja el software general y las comunicaciones entre los dispositivos que utilizan el protocolo de comunicación SNMP. Todos los dispositivos administrados por SNMP contienen el software agente SNMP y una base de datos llamada Base de Información sobre la Administración (MIB).

La MIB tiene 126 áreas de información sobre el estado del dispositivo, el desempeño del dispositivo, sus conexiones hacia los diferentes dispositivos y su configuración. El administrador SNMP consulta al MIB a través del software agente y puede especificar los cambios hechos a la configuración. La mayor parte de los administradores SNMP consultan a los agentes en un intervalo regular, 15 minutos por ejemplo, a menos que el usuario indique otra cosa.

El software agente SNMP por lo general es bastante pequeño, comúnmente de 64 KB dado que el protocolo SNMP es sencillo. SNMP está diseñado para ser un protocolo de sondeo (polling), lo que quiere decir que el administrador produce mensajes para el agente. Los mensajes SNMP se colocan dentro de un datagrama UDP y se enrutan vía IP (aunque podrían utilizarse otros protocolos).

El puerto UDP 161 se utiliza para todos los mensajes, excepto para los traps[11], que llegan al puerto UDP 162. Los agentes reciben sus mensajes del administrador a través del puerto UDP 161 del agente.

11 *Traps.- Alarmas enviadas por los agentes cuando ocurren ciertos eventos*

SMI

El SMI define las reglas para describir los objetos gestionados y cómo los protocolos sometidos a la gestión pueden acceder a ellos. La SMI (Structure of Management Information), define la estructura bajo la cual podrá ser definida y construida una MIB. Señala aspectos tales como el tipo de datos que podrá albergar la MIB, cómo pueden representarse y denominarse los recursos en la MIB, etc.

SMI sólo permite la utilización de tipos de datos simples en la construcción de MIB: escalares y arrays bidimensionales de escalares, y no permite la creación o recuperación de estructuras complejas de datos. SMI proporciona técnicas para:

- Definir la estructura de una MIB particular.
- Definir los objetos individuales, la sintaxis y valor de cada objeto.
- Codificar el valor de los objetos.

Los objetos MIB, así como toda la estructura del MIB, están constituidos por:

- **Integer**. Algunas variables son declaradas como enteros sin restricciones, otras son definidas para tomar valores específicos y otras con valores máximos y mínimos.
- **Octect string**. Es una cadena de 0 o más bytes. Por delante de la cadena se incluye el número de bytes que la componen.
- **Object identifier.** Es un identificador de cada uno de los objetos definidos en la MIB.
- **Null**. Indica que la variable correspondiente no tiene ningún valor.
- **Sequence.** Es una estructura similar a la del lenguaje C.
- **Secuence of**. Es la definición de un vector donde todos los elementos tienen el mismo tipo de datos.

Además de estos existen otros tipos de datos pero que no son más que restricciones sobre los tipos universales. Por mencionarlos, estos son:

Ipaddress, Physaddress, CounterGauge, Opaque, Timeticks.

Identificadores de objeto

De todos los tipos de datos los identificadores de objeto constituyen el elemento básico para la construcción de la MIB. Es un tipo de dato que especifica un objeto y es asignado por la autoridad competente. Las normas para la asignación de identificadores de objeto son las siguientes:

1) Cada identificador es único, y su valor consiste en una secuencia de números enteros.
2) El grupo de objetos definidos formará una estructura en árbol.
3) Los objetos concretos estarán en las hojas del árbol.

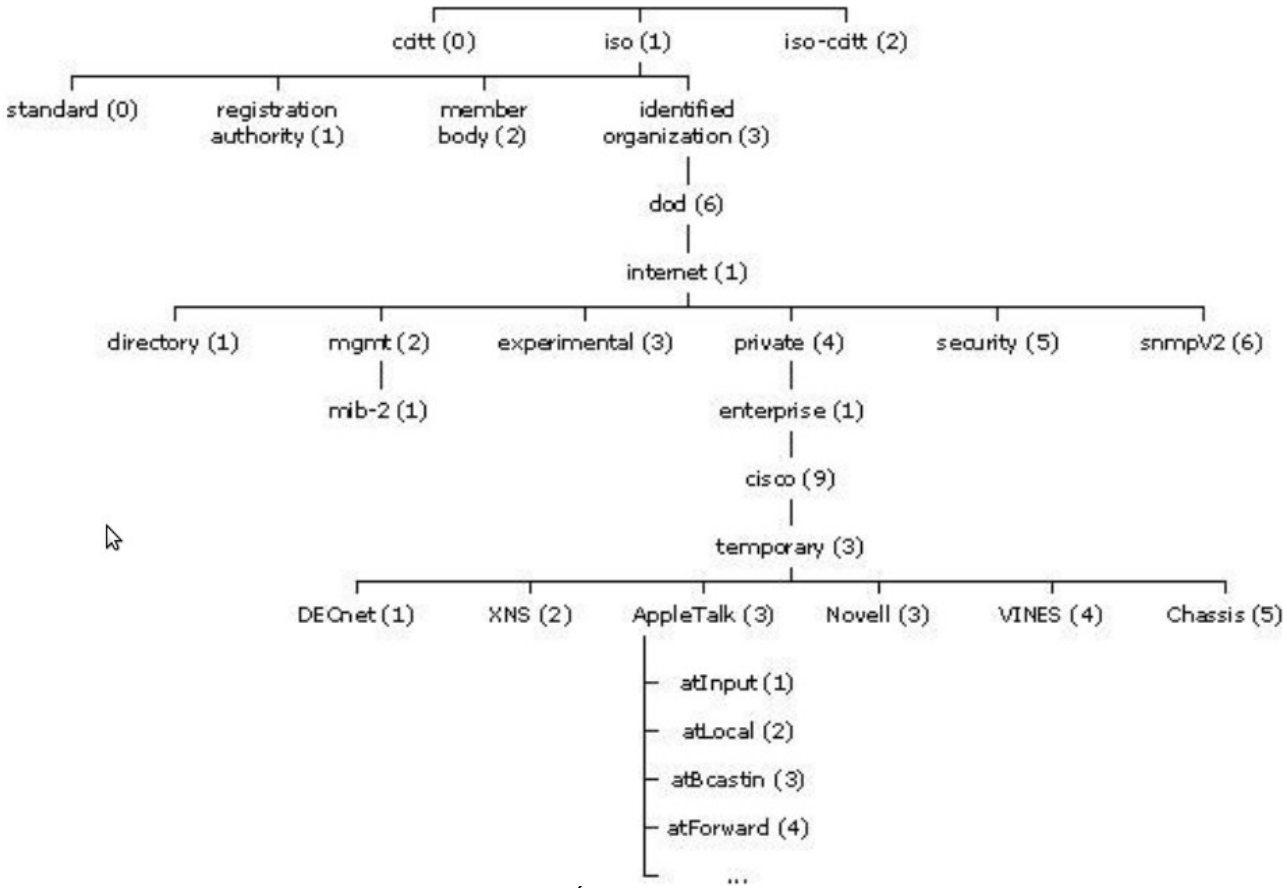


Figura 1.11. MODELO DE GESTIÓN SNMP – ESTRUCTURA DE IDENTIFICADORES DE OBJETO

Un identificador de un objeto es una secuencia de números enteros separados por puntos decimales. Estos tienen una estructura arborescente. Comenzando a partir de la raíz del árbol de identificadores de objetos, cada valor del componente identificador de objeto identifica una rama del árbol. A partir de la raíz hay tres nodos

en el primer nivel: “iso,itu-t,” y “joint-iso-itu-t”. Bajo el nodo “iso”, se usa un subárbol para otras organizaciones, una de las cuales es el DOD (Department Of Defense).

Así, el nodo tiene el valor de identificador 1.3.6.1, que sirve como prefijo para los nodos por debajo de él. Cada nodo del árbol recibe también un nombre textual con el fin de hacerlo más inteligible.

Existe una rama denominada “private (4).enterprise (1)”, de esta rama colgarán otras correspondientes a cada empresa, por ejemplo cisco (9) para que estas creen sus propios objetos.

Codificación de la información.

Cuando se pasa información entre diferentes arquitecturas, los sistemas deben acordar la representación de esta. SNMP se basa en dos estándares para la representación de la información: ASN.1[12] y BER[13] el cual es parte de ASN.1.

ASN.1 es un lenguaje de especificación formal que puede ser serializado en una secuencia de bytes haciendo uso de BER. SNMP sólo utiliza un subconjunto de ASN.1, los tipos integer, octect string, object identifier, sequence y null; si se utilizan otros tipos deben poder ser resueltos en estos tipos primitivos. Todos los datos codificados usando BER son precedidos por un campo Tipo y Longitud. El campo tipo indica la construcción de los datos transportados y el campo longitud su tamaño, lo que permite al receptor descifrar diferentes tipos de información.

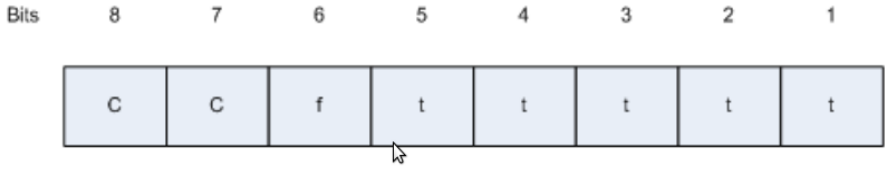
Para proporcionar mayor flexibilidad para otras estructuras que puedan necesitarse en el futuro, el campo tipo tiene tres subdivisiones, tal y como muestra la figura 1.10; los bits 7 y 8 son denominados Tag class (cc), elt bit 6 el Form (f) y los bits 5 al 1 el tag number que identifica el tipo de dato en si. Si el número de tag vale 31 significa que el campo tipo ocupa más de un byte.

---

12 *Abstract Syntax Notationes una norma para representar datos independientemente de la máquina que se esté usando y sus formas de representación internas.*

13 *Basic Encoding Rules Las Reglas de Codificación Básicas son las reglas definidas originalmente en el estándar ASN.1 para codificar información abstracta en un flujo de bits único, esto es, que pueda ser interpretado en cualquier máquina de la misma manera.*

Por ejemplo, el tipo INTEGER es UNIVERSAL, primitivo (simple) y su número de tag es 2, luego se codifica: 00 0 00010.



Donde:

8	7	Tag class	6	Form	54321
0	0	Unviersal	0	Primitive	Tag number
0	1	Application wide	1	Constructed	
1	0	Context specific			
1	1	Private use			

El campo Longitud tiene generalmente un byte, pero puede utilizar más bits para describir estructuras más largas; para ello se utiliza el bit 8 del campo de longitud que cuando se pone a 1 denota que la longitud del propio campo longitud, medida en bytes, viene representada en los restantes 7 bits de dicho campo.

Por ejemplo, la longitud 4 se codifica 0 0000100 y una longitud de mil bytes se codifica 10000010 00000011 11101000. Existe un valor especial de longitud (10000000) para representar una longitud indefinida. El campo valor acaba con un byte especial denominado "Fin de contenido" ("End Of Content" o EOC).

MIB

Es una base de datos a través de la cual se tiene acceso a la información para la gestión, contenida en la memoria interna del dispositivo en cuestión. MIB es una base de datos completa y bien definida, con una estructura en árbol, adecuada para manejar diversos grupos de objetos (información sobre variables/valores que se pueden adoptar), con identificadores exclusivos para cada objeto. Podemos encontrar en el RFC 1213 (MIB-II). La base de información de gestión o MIB es una definición de los objetos que deberían ser proporcionados en cada nodo gestionado

por el agente SNMP, para ello identifica los elementos de red, objetos gestionados y define nombres no ambiguos asociados con cada objeto.

Los objetos gestionados están organizados en grupos, cada uno de los cuales se relaciona con un de los protocolos o niveles TCP/IP o con el sistema en sí. No todos los grupos de variables definidas son obligatorios para todos los componentes, lo que sí es obligatorio es soportar todas las variables que un grupo tiene si soporta algún elemento del grupo.

Cuando se desea consultar o modificar un valor de un objeto MIB es necesario identificarlo. SNMP solo puede hacer referencia a los nodos finales (hojas) y no a las ramas del árbol; además, SNMP no manipula filas o columnas enteras de una tabla.

La arquitectura SNMP opera con un reducido grupo de objetos que se encuentran definido con detalle en la RFC 1066 "Base de información de gestión para la gestión de redes sobre TCP/IP".

Para definir una variable u objeto MIB es necesario especificar lo siguiente:

- Sintaxis: Especifica el tipo de datos de la variable, un valor entero, etc.
- Acceso: Especifica el tipo de permiso como: Leer, leer y escribir, escribir, no accesible.
- Estado: Define si la variable es obligatoria u opcional.
- Descripción: Describe textualmente a la variable.

Grupos de la MIB

La MIB-1 define 126 objetos de administración, divididos en los siguientes grupos:

Grupo de Sistemas

- Usado para registrar información del sistema, por ejemplo:
- Compañía fabricante del sistema.
- Tipo de Software.
- Tiempo que el sistema ha estado operando.

Grupo de Interfaces

Registra la información genérica acerca de cada interfaz de red, como el número de mensajes erróneos en la entrada y salida, el número de paquetes transmitidos y recibidos, el número de paquetes de broadcast enviados, MTU[14] del dispositivo, etc.

Grupo de traducción de dirección.

Comprende las relaciones entre direcciones IP y direcciones específicas de la red que deben soportar, como la tabla ARP[15], que relaciona direcciones IP con direcciones físicas de la red LAN.

Grupo IP.

Almacena información propia de la capa IP, como datagramas transmitidos y recibidos, conteo de datagramas erróneos, etc. También contiene información de variables de control que permite a las aplicaciones remotas ajustar el TTL (Time To Live) de omisión de IP y manipular las tablas de ruteo de IP.

Grupo TCP.

Este grupo incluye información propia del protocolo TCP, como estadísticas del número de segmentos transmitidos y recibidos, información acerca de conexiones activas como dirección IP, puerto o estado actual.

Grupo de ICMP y UDP.

Lo mismo que el grupo IP y TCP.

Grupo EGP.

En este grupo se requieren sistemas (ruteadores) que soporten EGP (Protocolo de Gateway o Salida Exterior).

14 *Unidad máxima de transferencia.*
15 *Protocolo de resolución de direcciones*

SNMP

El protocolo SNMP define la forma más básica para el intercambio de información de gestión de redes donde existen: un gestor, agentes y bases de información de gestión. La simplicidad que presenta produce deficiencias para transferir grandes cantidades de información, poca o ninguna seguridad, entre otras cosas.

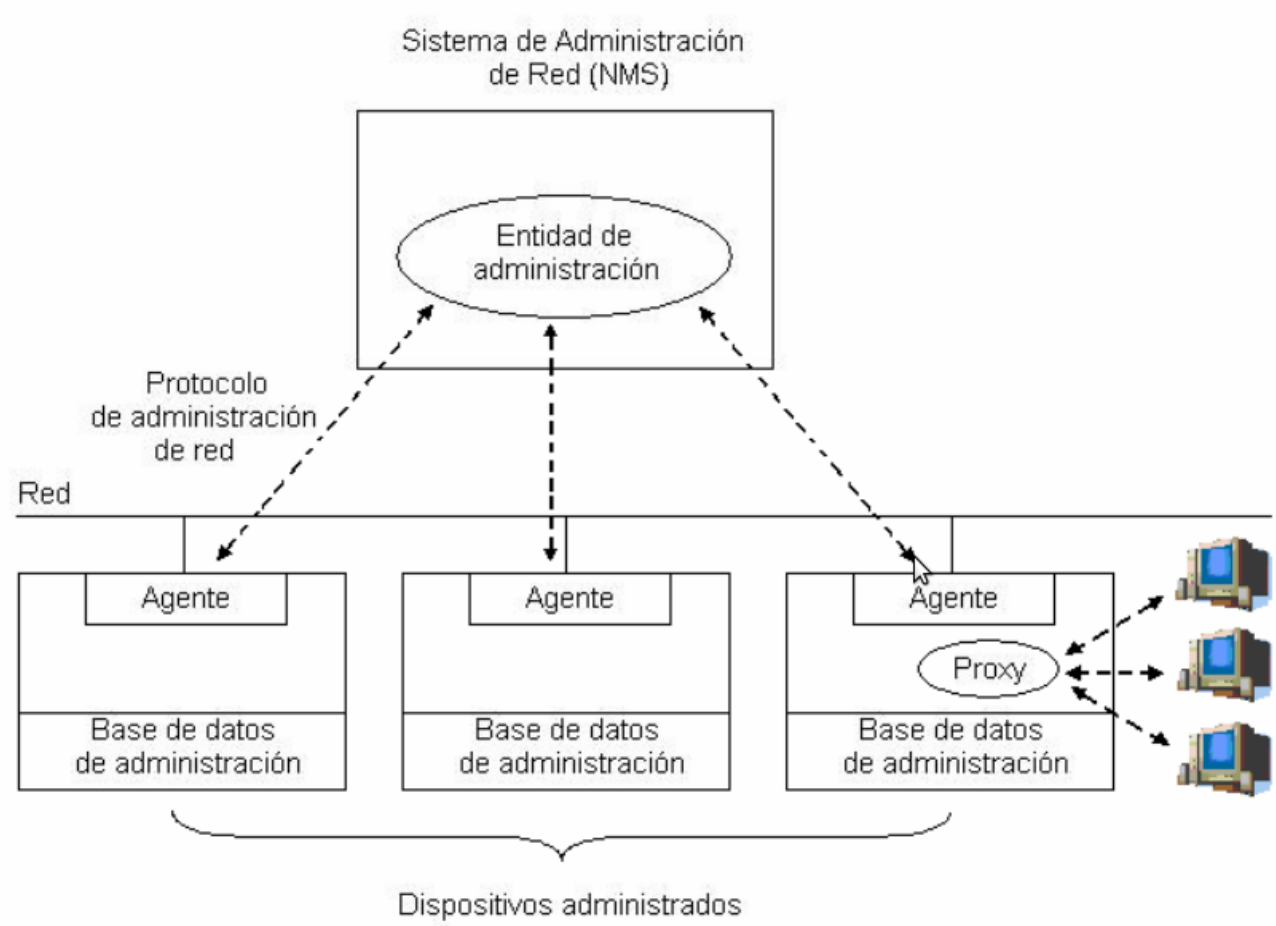


Figura 1.11. MODELO DE GESTIÓN SNMP – ARQUITECTURA PROTOCOLO SNMP

Tipos de mensajes SNMP.

Los diferentes tipos de mensajes se describen a continuación:

- GetRequest: el gestor pide al agente el valor de un dato.
- GetNextRequest es similar al GetRequest, permitiendo extraer datos de una tabla.

- SetRequest: el gestor pide al agente que modifique los valores de las variables que especifique. El agente modificará todos o ninguno de los valores.
- GetResponse: Respuesta del agente a las peticiones GetRequest, GetNextRequest y SetRequest.
- Trap: Mensaje generado por el agente en respuesta a un evento que afecte a la MIB o a los recursos gestionados. El gestor no confirma la recepción de un trap al agente.

Comunidades SNMP

A continuación se describen las diferentes características que deben cumplir los agentes y comunidades SNMP:

a) Cada agente es responsable de su MIB local, controlando sus estaciones gestoras.
b) Control de acceso a la MIB de un agente: concepto de comunidad.
c) Comunidad es la relación que se tienen entre un agente SNMP y un conjunto de estaciones de gestión SNMP, definen unas características de autentificación y control de acceso.
d) El agente establece una comunidad para cada combinación deseada de autentificación y control de acceso, y a cada comunidad se le da un nombre de comunidad (community name) que es su nombre único dentro del agente. Este nombre las estaciones de gestión pertenecientes a una comunidad la emplean en todas las operaciones GetRequest, GetNextRequest y SetRequest.
e) El agente puede establecer cualquier número de comunidades. Y a su vez una estación de gestión puede pertenecer a varias comunidades.
f) Una estación de gestión debe almacenar los nombres de comunidad asociados a cada agente.

g) Mediante el uso de comunidades, un agente puede limitar el acceso a su MIB en dos formas:

   - Vistas de la MIB: subconjunto de los objetos de la MIB.
   - Modos de Acceso: solo lectura o solo escritura.

h) El agente sólo atiende la petición si el nombre de la comunidad es correcto para el tipo de acceso solicitado.

SNMPV.2

Como resultado de una serie de propuestas para mejorar las características de SNMP, en 1996 se publica un nuevo estándar, el protocolo SNMPv.2. Los cambios se traducen fundamentalmente en una mejora de las prestaciones de intercambio de información de gestión, como la implementación de seguridad que fue una de las principales limitaciones de SNMPv.1.

Seguridad.

SNMPv.2 define métodos para controlar las operaciones que están permitidas, a diferencia de SNMPv.1 que no incorpora ningún mecanismo de seguridad. Pero luego, surgieron dos planteamientos diferentes en cuanto al modelo de seguridad, que han dado lugar a dos especificaciones conocidas como SNMPv.2[16] y SNMPv.2u[17]

Principales características de SNMPv.2

Ésta versión ya permite el soporte de comunicación gestor-gestor (PDU-Protocol Data Unit- informrequest). La lectura de tablas completas en una sola operación (PDU getbulkrequest), es otra de las variantes. Pero la seguridad sigue siendo una falencia, ya que todavía se basa en “comunidades” (un nombre con un conjunto de

16 *La versión SNMPv.2 proporciona niveles de seguridad adecuados, pero no alcanzó el necesario nivel de estandarización y aceptación por el IETF.*

17 *La identificación se lleva a cabo mediante usuarios. Es decir que un mismo usuario puede estar definido en varias entidades SNMP diferentes.*

operaciones permitidas) hasta la versión 3. Los diferentes tipos de mensajes que se manejan en SNMPv.2 son los siguientes:

- get-request.
- Get-next-request.
- Get-bulk-request.
- Response.
- Set-request.
- Inform-request.
- snmpV2-trap.
- report.

Interoperabilidad con SNMPv.1

La versión 2 de SNMP permite ínteroperar con SNMPv.1, bajo las siguientes características:

- Los agentes pueden emplear tanto la versión 1 como la 2.
- Los gestores deben emplear tanto la versión 2 como la 1 para poder comunicarse con agentes de versión 1.
- El gestor intentará primero emplear la versión 2 con un agente, si:
  a) El agente emplea versión 2 le contestará.
  b) El agente emplea versión 1 responderá con un mensaje de error; el gestor entonces, lo intentará con versión 1, para ello deberá hacer conversiones (por ejemplo, convertir getbulk en getnext).

SNMPV.3

La falta de consenso en la versión final de SNMPv.2 (SNMPv.2u y SNMPv.2*) finalmente hizo que las mejoras a la seguridad sean descartadas. En 1998, a partir de estas dos versiones anteriores, surge SNMPv.3 con las siguientes características:

- SNMPv.3 no modifica las PDUs de SNMPv.2.
- Define una serie de capacidades de seguridad y un marco que hace posible su uso junto con las PDUs de SNMPv.2.
- SNMPv.3 es SNMPv.2 con mayor seguridad y administración.

Mejoras en la seguridad en SNMPv.3

SNMPv.3 debió definir un conjunto de mecanismos de seguridad que incluyen la protección contra las amenazas de:

- Modificación de la información.
- Enmascaramiento.
- Modificación del flujo de mensajes.
- Revelación de contenidos.

Pero no se contempla la protección frente a:

- Denegación de servicio.
- Análisis de tráfico.

Arquitectura de Gestión de red en SNMPv.3

SNMPv.3 define una arquitectura de gestión de red:

- Colección de entidades SNMP que interaccionan entre sí.

Cada entidad implementa una parte de las capacidades de SNMP y puede actuar como agente, gestor o una combinación de ambos.

- Cada entidad consiste en una colección de módulos que interaccionan entre sí para proporcionar servicios. Una entidad incluye un motor SNMP, este motor implementa funciones para enviar y recibir mensajes, autentificar y encriptar/desencriptar mensajes, y controlar el acceso a los objetos gestionados.

1.4. ANÁLISIS DE LOS MODELOS DE GESTIÓN DE RED.

Luego de haber expuesto los distintos modelos de gestión observamos que, los elementos de un modelo de gestión típico son: protocolos, lenguajes y modelos de información, y distintas estrategias de estandarización en relación a estos conceptos, y llegamos a resaltar tópicos relevantes tales como.

El paradigma gestor-agente, con la arquitectura que soporta la especificación e implantación tradicional de comportamiento de gestión y cuáles son sus límites en la integración de otros modelos, así como conceptos de monitorización y control.

Modelos de gestión, dificultades de adopción y limitaciones de los modelos de gestión expuestos en el presente documento.

Los modelos de gestión de red realizan una gestión de los equipos gestionados, y para ello se ocupan de normalizar la información gestionada esto es, lenguaje y modelo de información, y cómo se deben llevar a cabo las comunicaciones en cuanto a protocolo y servicios de gestión, con el objetivo de conseguir interoperabilidad entre gestor y agentes.

Sin embargo, estos modelos de gestión no definen las operaciones que el gestor debe llevar a cabo en relación a los agentes, ni de su especificación ni de su implantación, únicamente definen qué se puede gestionar y como se puede gestionar. Esto se debe a que asumen que estas operaciones las realiza manualmente el administrador de la red o son sencillas actividades automáticas que se pueden programar en el gestor.

Tampoco estos modelos resultan especialmente adecuados para especificar el comportamiento que deben seguir los propios elementos de la red cuando éste empiece a ser complejo y variado, ni para el intercambio entre estos y el gestor de las reglas que regulan dicho comportamiento.

No obstante, ante el gran crecimiento de las redes hoy en día, lo que se busca es poder automatizar al máximo las operaciones sobre la red, de forma que se pueda liberar a los administradores de red de realizar tareas repetitivas o simples, cuya programación podría trasladarse a un sistema con cierta “inteligencia” o capacidad de reaccionar.

De lo expuesto podemos definir el comportamiento de gestión como aquel ámbito de la gestión que se centra en el comportamiento de la red, tanto en su especificación como en su implantación.

CAPITULO 2. ESTUDIO COMPARATIVO DE LOS SISTEMAS DE GESTIÓN.

2.1. INTRODUCCIÓN.

El crecimiento constante y la incorporación de nuevas tecnologías, gradualmente se van complicando y muchas veces degradando la performance de la red. Por esta razón hay que realizar un "Análisis Comparativo", orientado a prevenir, plantear soluciones concretas ante nuevos problemas o requerimientos y, seleccionar la tecnología que más convenga para asegurar la estabilidad, operabilidad y flexibilidad en el tiempo del Sistema en General.

Para brindar el mejor servicio en el control y mantención de la Red y ser un apoyo real en la incorporación de las soluciones tecnológicas, se propone un análisis de los parámetros y criterios de comparación más relevantes y de vital importancia dentro de cada tecnología con el objetivo de seleccionar la mejor para gestionar una red de manera adecuada.

Hoy en día las redes en un campus universitario son cada vez más heterogéneas y las exigencias de su correcta operación son amplias, esto conlleva a operaciones más complejas de monitoreo y administración.

Las redes de campus universitario soportan ahora mucho más aplicaciones y servicios estratégicos; además su crecimiento constante y la incorporación de nuevas tecnologías van evidenciando la necesidad de contar con herramientas de monitoreo de red que permitan dar un seguimiento adecuado a los host de la red, así como a sus componentes más importantes como por ejemplo:

- Procesador.
- Memoria.
- Disco.
- Tarjetas.
- Ópticos.
- Puertos, etc.

Debido a la gran importancia que tiene una red en la productividad y eficiencia en un campus universitario, es indispensable analizar y monitorear el software y los niveles de saturación de tráfico en la red, esta acción se ha convertido en una labor cada vez más importante y de carácter pro activo para evitar posibles problemas que puedan afectar el normal rendimiento de la red.

Este monitoreo pro activo le da más control al departamento de TI en un campus universitario, ya que al tener una herramienta que ayude a detectar los problemas de la red, les permite corregirlo a tiempo y prevenir futuros inconvenientes que le pueden salir caros a la universidad.

Ahora, sin un monitoreo adecuado en una red de campus universitario, la caída de los servicios provoca:

- Descontento de los usuarios finales.
- Pérdida de productividad.
- Mala imagen de la empresa.

Para evitar que la pérdida de servicios sea repentina, el monitoreo en una red de campus universitario se debe basar equipos de red y de usuario final, tales como:

- Routers.
- Switches.
- Firewalls.
- Equipos de escritorio.
- Servidores.

El monitoreo de estos dispositivos, permite enviar eventos cuando se detecta cierto cambio inusual, dichos eventos pueden ser absorbidos mediante el protocolo SNMP, lo cual permite anticiparse a los problemas, y de esta forma, resolver problemas antes de que los usuarios finales los detecten y mejorar notablemente la imagen y los servicios.

2.2. CARACTERÍSTICAS DE LOS SISTEMAS DE GESTIÓN.

El objetivo principal de un sistema de gestión de red es mantener la disponibilidad de la misma, mientras facilita sus modificaciones y ampliaciones, mejora sus prestaciones que ofrece, reduce las tareas repetitivas y minimiza sus costes de operación y mantenimiento.

Por tanto, un sistema de gestión de red asegura que los equipos y programas que constituyen la red junto con el personal y sus procedimientos de actuación sobre la misma, presentan una operación correcta, eficiente y enfocada a la misión encomendada, y de esta manera contribuir a la satisfacción de los usuarios de la red.

Básicamente, los sistemas de gestión de red se conforman de cuatro tipos de componentes:

1) El centro de gestión, ya sea central o distribuido.
2) Agentes, que median sobre los nodos gestionados.
3) Protocolos de gestión.
4) Información de gestión, constituye y actualiza la base de información de gestión.

Los sistemas de gestión de red definidos de ésta forma son de aparición muy reciente y aunque se han realizado importantes inversiones, tanto por los fabricantes de equipos y sistemas como por los administradores de red, aun queda un notable esfuerzo de normalización para conseguir estándares universalmente aceptados que garanticen la interoperabilidad de sistemas de diferentes suministradores.

2.3. CARACTERÍSTICAS GENERALES PARA ESCOGER UN SISTEMA DE GESTIÓN DE RED.

Un sistema de gestión debe contemplar cualquier aspecto relacionado con los recursos de red que gestiona, tanto físicos como lógicos. Los primeros se refieren a la gestión de los componentes físicos de la red tales como, enlaces, fuentes de

alimentación, conmutadores, etc. Los segundos consideran actividades tales como los servicio al usuario final, estas podrían ser: programación de trabajos de instalación y mantenimiento, planificación, etc.

Aunque con los dos niveles inferiores podría ser suficiente para la gestión de redes, la realidad es que cada vez es más necesario disponer de los superiores, que tienen que ver con la planificación y calidad de servicio al usuario, esto es nivel de servicio y nivel de negocio, para disponer de herramientas válidas que garanticen tanto la calidad como la viabilidad del entorno de red desde el punto de vista del giro de negocio.

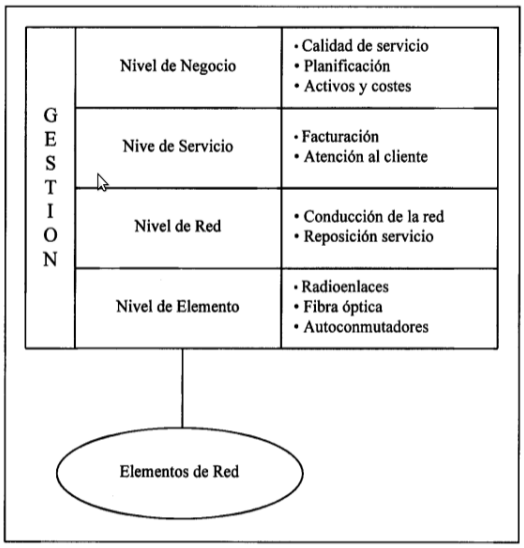


Figura 2.1. GESTIÓN RED – CARACTERÍSTICAS GENERALES.

2.3.1. INTERFAZ SIMPLE.

Una de las principales características de un sistema de gestión de red es su interfaz de usuario, ésta debe presentar una vista intuitiva, simple y agradable orientada a la administración de la red a gestionar, capaz de disminuir y facilitar el trabajo, que muestre la información de estado y rendimiento de la red.

Una interfaz que unifique alertas generadas de acuerdo a la identificación de situaciones de disponibilidad, configuración y calidad de servicio.

2.3.2. ESTABLECER LINEAS BASE.

La línea base resuelve problemas frecuentes de la improvisación en la planeación y brinda elementos ciertos para una evaluación sistemática de las políticas de gestión, porque define previamente indicadores estables en el tiempo o indicadores estructurales, seleccionados en virtud de su importancia frente a las funciones de la red de gestión que sirven de y regulación de las políticas administración de red y establece una referencia para observar la evolución y el comportamiento de la red.

Este aspecto es una de las características de los sistemas de gestión de red, es, reconocer el normal funcionamiento de la red este proceso se lo realiza analizando el tráfico de red por un determinado periodo de tiempo y crear una "línea base" de comparación con el tráfico analizado, en el que si el tráfico varia demasiado con respecto a la línea de comportamiento se genera una alarma de manera automática.

2.3.3. GENERACIÓN DE REPORTES.

En una aplicación de red es muy importante la versatilidad de los reportes donde se detalle el uso de los recursos de red, tales como: información de uso de puertos, información de usos de enlace en un tiempo demandado regularmente. La generación de informes debe ser flexible y poder generarse en base a parámetros como: región, sitio o nodo de la red. Los informes deben ser oportunos con información válida para el análisis sobre el desempeño de la red en cualquier momento, así como detalles de desempeño de recursos de la red.

2.3.4. AUTO DESCUBRIMIENTO.

Por definición las herramientas de auto descubrimiento representan a la red como un conjunto de iconos, que hacen referencia a los diferentes nodos, enlaces, que los unen físicamente, es decir describir la infraestructura de red de forma automática y facilitar la tarea de determinar los nodos que comprenden la red a gestionar.

Funciona de manera que chequea el entorno para comprobar la existencia de dispositivos y crear, automáticamente entradas o puntos de red, desde éste momento dichas entradas serán componentes de la red.

2.3.5. CONFIGURACIÓN Y ANÁLISIS.

El seteo inicial de las políticas de gestión para el entorno de red a gestionar es sumamente importante, ésta configuración inicial no solo reducirá el riesgo de errores en la gestión de red, sino que también contribuirá a la mejora de tareas como la gestión del rendimiento y de fallos, llegando finalmente a conseguir el alineamiento de los recursos de red con los objetivos del "negocio".

El primer paso es el inventario o auditoría de red, actividad que evidenciará los dispositivos presentes en la infraestructura del entorno de red, se requiere que los datos a obtener sean con el mayor detalle posible. La información que se obtenga en éste primer paso deberá ser almacenada en un repositorio fácilmente modificable, información que será crucial para la recuperación en caso de desastres.

Las políticas de gestión de la configuración variarán en cada entorno específico pese a ello existen cuestiones genéricas para tener en cuenta:

(a) Políticas de cambios de configuración. Los cambios en la infraestructura de red son inevitables. Por ello, es preciso crear políticas que claramente delimiten el proceso de aprobación de dichos cambios, identificando al personal autorizado para realizarlos y marcando las condiciones de su registro. Conviene, además, evaluar los cambios de configuración antes de su implementación en el entorno de producción.

(b) Respaldo de configuración de dispositivos y política de recuperación de fallos. Lo ideal es que los datos actuales sobre configuración de dispositivos sean almacenados en un repositorio del que puedan ser fácilmente recuperados cuando se producen fallos o incluso una catástrofe. Los procedimientos para que tales datos sean recuperados y reiniciados deben ser definidos prudentemente.

(c) Política de verificación de la configuración de dispositivos. Quizá la función más crítica sea la verificación de los datos de configuración actuales. La detección a tiempo de dispositivos erróneamente configurados reducirá significativamente las situaciones de inestabilidad de la infraestructura de red, inestabilidad que podría llegar a dar lugar a fallos catastróficos. Además, la

verificación de la configuración es una de las mejores maneras de eliminar las brechas de seguridad internas y externas.

(d) Monitorización, informes y recuperación de desastres. Las actividades de monitorización y de generación de informes relativas a la gestión de la configuración pueden y deben reflejar:
Inventario de dispositivos/configuración. Para determinar los dispositivos existentes, dónde se encuentran y cómo están configurados. Este requerimiento primario, ya visto más arriba, también puede ser una fuente de actualizaciones futuras para reflejar los cambios en la infraestructura en red. Asimismo, resulta fundamental para la planificación y gestión de activos.

(e) **Auditorías de cambios/configuración**. Las configuraciones iniciales de red deberían permitir realizar una auditoría de las condiciones de los accesos de los usuarios (quién hace qué y cuándo, y en qué dispositivo). Estos informes deben ser capaces de ofrecer una visión automatizada de los cambios, y, en algunos casos, alertar de las desviaciones que dichos cambios experimenten respecto de las políticas esperadas.

2.3.6. CONFIGURACIÓN DE POLÍTICAS Y DESPLIEGUE DE INFORMACIÓN.

Para afrontar la gestión de los nuevos entornos más complejos surgen una serie de propuestas que tratan de especificar el comportamiento de gestión mediante políticas, con el objeto de estandarizar la gestión y posibilitar la interoperabilidad en el entorno.

Según el IETF[18] el término “política” puede definirse como:

- Un objetivo definido, o método de acción para guiar y determinar decisiones presentes y futuras. Las “políticas” se ejecutan dentro de un contexto particular (como por ejemplo políticas definidas en una unidad de negocio)
- Políticas como un conjunto de reglas para administrar, gestionar, y controlar acceso a los recursos de red.

18 *Internet Engineering Task Force o Fuerza de Tareas de Ingeniería de Internet, es una organización internacional abierta de normalización.*

La creación de políticas de gestión tiene por objeto el ahorro de tiempo y la disminución de errores, una de las ventajas principales es la elaboración de plantillas para la realización de determinadas tareas, y con ello facilitar actualizaciones y/o futuros cambios de forma simultánea en los nodos de la red.

La aplicación de políticas también es útil para programar los tiempos de actualización en los periodos de poco tráfico de red. Para la configuración y aplicación de políticas un sistema de gestión incluye elementos como:

Herramientas que sirvan de ayuda a la creación de las mismas, por ejemplo una política pudiera ser, que el tráfico desde determinada área de la red no sobrepase un ancho de banda límite. Estas políticas pueden ser almacenadas, los conceptos y herramientas para la gestión de redes, los administradores de red deberían configurar y manipular los elementos de la red manualmente a través de interfaces de control, proceso propenso a errores y que consume tiempo. Además, proporciona las siguientes ventajas:

Empleo, para aplicaciones críticas, de políticas de prioridad en el tratamiento de flujos basados en mejor esfuerzo. Mejoras en el rendimiento de aplicaciones de importancia en una empresa. Optimización de la infraestructura de la red, incremento de la eficiencia del personal que administra la red, y reducción del tiempo, costo, y problemas asociados con la configuración de los dispositivos.

En un entorno de gestión se pueden implementar un conjunto de políticas de gestión entre las cuales tenemos:

- Políticas de Autorización: indica sobre los permisos de un “sujeto” sobre un “dominio”.
- Políticas de Delegación: indica sobre la posibilidad de un “sujeto” para delegar sus privilegios o permisos.
- Políticas de Obligación: especifica las acciones que un “sujeto” debe realizar como respuesta ante eventos o el cumplimiento de determinadas condiciones.
- Políticas de Restricción: indica las acciones que un “sujeto” no podrá realizar en el “dominio”.

- Políticas Compuestas: políticas que agrupan varios de los tipos anteriores.

2.3.7. RECOLECCIÓN DE INFORMACIÓN.

El proceso de recolección y análisis continuo de datos con el fin de anticipar problemas en la red y reportar en tiempo real es muy importante para mantener una red estable y operable, además permite reconocer problemas de rendimiento y/o desempeño de la red y resolverlos antes de que dichos problemas repercutan sobre el desempeño de la red.

La constante recolección de información como objetivo principal, busca áreas vulnerables en los nodos de la infraestructura de red, así como proporcionar los conocimientos necesarios para monitorear las principales actividades de cada uno de ellos.

La seguridad también es importante, puesto que con la recolección de información se puede conocer el tipo de tráfico que esta fluyendo en la red, y así detectar tráfico de carácter malicioso que genera cada nodo de la red, de manera oportuna.

En base a lo detallado la recolección de información sirve para detectar cambio en la infraestructura de la red, problemas de eficiencia y desempeño de los recursos, y problemas de seguridad.

2.3.8. SOPORTE.

Soporte es un conjunto de prestaciones facilidades para satisfaces necesidades específicas respecto de dudas o falencias en cuanto al manejo de la aplicación de gestión de red. Es necesario contar con un soporte adecuado de la herramienta a utilizar.

En el caso de herramientas libres, es común encontrar comunidades detrás de cada aplicación de software libre, éstas provees soporte para el mismo así como un constante desarrollo de nuevas versiones, parches de seguridad o de corrección de errores.

La mayoría de comunidades son tan libres como el software, por lo que cualquier persona con conocimientos y tiempo puede aportar para el desarrollo o para la depuración de errores. Además es común encontrar al creador o creadores del software respondiendo preguntas en los foros.

2.4. PLATAFORMAS DE GESTIÓN DE MONITOREO.

Dentro de lo que se refiere a la gestión de redes existen múltiples implementaciones de sistemas de tipo comercial y libre, muchos de ellos se enfocan a necesidades específicas del administrador de redes y otros son más generales.

2.4.1. APLICACIONES DE GESTIÓN COMERCIALES.

2.4.1.1.- HP Openview.- Es un software de gestión de red que ofrece un conjunto de soluciones de software para administrar y optimizar los servicios de red en una infraestructura de tecnologías informáticas de imagen, voz y datos. Dentro de las herramientas principales para la gestión de red se pueden mencionar:

(a) Network Node Manager NNM.-

(b) Customer Views CV.

(c) Services Information Portal SIP.

Descubre todos los elementos a los que tiene acceso y los agrega a la topología, muestra además un sistema de de alertas de los que tiene configurados. Dentro de la topología conforme se navega al segmento de red que se quiere observar, es posible tomar más acciones sobre los host, como observar alarmas específicas, monitorear interfaces, realizar conexiones telnet, entre otras. Si bien este es un sistema muy completo su implementación implica un costo bastante elevado. Además el software necesita una máquina relativamente “poderosa” para funcionar sin problemas.

2.4.1.2.- IBM Tivoli.

Es una herramienta que cuenta con una interfaz WEB que permite visualizar datos de manera remota, supervisa programas en servidores, aplicaciones, bases de datos y software intermedio.

2.4.1.3.- Solarwinds Orion Network Performance Monitor.

Este es un sistema, basado completamente en Web, orientado al manejo de fallas y performance, utiliza SNMP para analizar datos de routers, switches, servidores, etcétera. El sistema corre sobre Windows 2000 o 2003 Server lo que incrementa el costo de licencias.

2.4.2. APLICACIONES DE GESTIÓN LIBRES.

Se entiende por software libre, el software que puede ser copiado, modificado y redistribuido sin costo alguno. Lo cual trae consigo muchas ventajas, entre las cuales destaca el no tener que pagar ningún tipo de licencia, la posibilidad de ver el código fuente y realizar modificaciones, por ejemplo, para adaptar algo a necesidades específicas.

Es común encontrar comunidades detrás de cada producto de software libre, estas proveen soporte para el mismo así como un constante desarrollo de nuevas versiones, parches de seguridad o de corrección de errores.

La mayoría de comunidades son tan libres como el software, por lo que cualquier persona con conocimientos y tiempo puede aportar para el desarrollo o para la depuración de errores. Además, es común encontrar al creador o creadores del software respondiendo preguntas en los foros.

2.4.2.1.- MRTG.

El Multi Router Traffic Grapher, es un software que permite realizar gráficas de dispositivos SNMP, de manera que se pueda analizar la performance, las tendencias, entre otras cosas.

Está escrito en Perl y funciona tanto en Linux como en Windows, la aplicación puede generar páginas HTML con los gráficos como figuras GIF.

2.4.2.2.- RRDTools.

RRDTools (Round Robin Database Tools) es un software libre del mismo autor del MRTG, está orientado al almacenamiento de datos y la generación de gráficos basados en estos. Provee un motor de bases de datos cíclicas, es decir trabaja con una cantidad fija de datos y cuando todos los registros se llenan se escribe sobre el dato más antiguo. Esto proporciona una estructura de datos fija cuyo tamaño y resolución serán definidos al crearla. Se puede establecer más de una base de datos para cada dispositivo a monitorear de manera que se mantengan promedios a diferentes resoluciones para una misma información.

2.4.2.3.- SmokePing.

Este es un programa escrito en Perl, para medir la latencia en un enlace. Utiliza RRDTools, para graficar y los datos son guardados en RRDs. Con esto se puede observar tendencias en latencia y pérdida de paquetes, permite además configurar alarmas en función a límites o patrones.

2.4.2.4.- Cacti.

Cacti es una interfaz Web, escrita en PHP, que hace uso del RRDTools, provee todo un conjunto de programas para hacer el sondeo así como scripts para equipos específicos y plantillas para diversos tipos de gráficos y equipos. Incluye además el manejo de usuarios, y a cada cual se le puede asignar diferentes permisos para ver o para crear nuevos gráficos. Está escrito en PHP, y es posible implementarlo en Linux, Solaris, BSD, e incluso Windows. Cuenta con una arquitectura de plugins que puede ser instalada de manera opcional, esta proporciona nuevas funcionalidades, por ejemplo definir límites y alertas cuando estos sean alcanzados, permitir descubrir nuevos dispositivos, mostrar mapas de red, etc.

2.4.2.5.- OpenNMS.

OpenNMS apunta a ser un sistema completo comparable al HP OpenView o IBM Tivoli, está escrito principalmente en Java, se enfoca principalmente en el monitoreo de servicio, de forma similar al Nagios, para esto simula un usuario accediendo a los servicios, por ejemplo para un servidor Web pide una página, para un servidor de correos manda un correo, etc. Se enfoca en cubrir todas las áreas del modelo OSI para la gestión de redes, algunas por defecto y otras mediante integración con otras herramientas. Cuenta con un modelo de monitoreo distribuido, que permite realizar eficientemente el monitoreo de redes de gran tamaño.

2.4.2.6.- ZABBIX.

Es un sistema de gestión diseñado para monitorear y rastrear el estado de varios servicios de red, servidores y otros equipos de red, está escrito en C y cuenta con una interfaz web escrita en PHP, ofrece varias opciones de monitoreo, controles simples pueden comprobar la disponibilidad y capacidad de respuesta de los servicios estándar, como SMTP o HTTP sin necesidad de instalar ningún software en el host monitoreado.

2.4.2.7.- Pandora FMS24.

Es un software de código abierto que sirve para monitorizar y medir todo tipo de elementos. Monitoriza sistemas, aplicaciones o dispositivos. Permite saber el estado de cada elemento de un sistema a lo largo del tiempo. Puede detectar si una interfaz de red se ha caído, un ataque en una web, una pérdida de memoria en algún servidor de aplicaciones, o el movimiento de un valor del NASDAQ, puede enviar SMS si un sistema falla o recoger información de cualquier sistema operativo, con agentes específicos para cada plataforma, que recolectan datos y los envían al servidor. Hay agentes específicos para GNU/Linux, AIX, Solaris, HP-UX, BSD/IPSO y Windows 2000, XP y 2003.

Monitoriza cualquier tipo de servicio TCP/IP y sistemas de red como balanceadores de carga, routers, switches, sistemas operativos, aplicaciones o impresoras si se necesita hacerlo de forma remota. Pandora FMS también soporta WMI para comunicarse directamente con sistemas Windows de forma remota y SNMP para recolectar datos o recibir traps. Pandora FMS está publicado bajo licencia GPL2 GNU General Public License, Pandora FMS.

2.4.2.8.- ZENOSS.

Plataforma para la gestión de red y servidores basada en el servidor de aplicaciones Zope. Liberado bajo la Licencia Pública General de GNU (GPL) versión 2, Zenoss Core provee una interfaz web que permite a los administradores de sistemas monitorear disponibilidad, inventario/configuración, desempeño y eventos. Erik Dahl comenzó el desarrollo de Zenoss en el 2002 y en agosto del 2005 fundó Zenoss, Inc., con Bill Karpovich. Zenoss, Inc. patrocina el desarrollo de Zenoss Core y vende una versión empresarial basada en la versión básica.

Zenoss incluye una impresionante lista de funcionalidades que parece crecer cada mes. La herramienta hace un estupendo trabajo como monitor de estados, soportando incluso plugins de Nagios. El sistema Zenoss sirve además para monitorizar rendimientos y tendencias. El diseño de Zenoss posee una arquitectura modular, para añadir nuevas funcionalidades sólo hay que conectarle un nuevo módulo (un ZenPack, en la jerga de los masters de Zenoss).

Zenoss permite una implementación sencilla de su sistema, y que aporta a la reducción de los costos, para estas tareas de monitoreo. Sus tareas no son reducidas, es una suite muy completa que facilita el trabajo de los usuarios, y que trabaja nutriéndose de los aportes y sugerencias que estos puede brindar.

La aplicación y todas sus características están preparadas para funcionar bajo un entorno de software libre, como son las distribuciones Linux, pero también trabaja en plataformas Unix y sistemas Mac. Mención a parte sobre Windows; aunque Zenoss no fue diseñado para trabajar en el, es totalmente compatible y utilizable en este sistema.

Zenoss se ofrece en tres tipos de producto; la primera es la versión Core, la siguiente la versión Profesional y por último la versión Enterprise. Las dos últimas son versiones comerciales, que se distinguen por ofrecer un soporte más profesional y algunas herramientas adicionales, no indispensables. La versión Core, es la disponible y elaborada por la comunidad.

Las características que Zenoss Core ofrece, se demuestran en la potencia de sus módulos, el soporte brindado por parte de los propios usuarios y por el grado de usabilidad que demuestra frente a otras aplicaciones similares.

Es muy configurable, y está diseñado para realizar una eficiente administración centralizada.

2.4.2.9.- Nagios.

Nagios es un programa para el monitoreo de redes, equipos y servicios. Está escrito en C y puede ser instalado en Linux y algunas variantes de Unix. Nagios está diseñado para monitorear una sistema poniendo énfasis en los servicios que corren sobre él, y alertar en caso ocurra un error. El monitoreo se realiza mediante SNMP y scripts. Cuenta con un gran número de plugins, que permiten adicionar funcionalidades, por ejemplo el NRPE (Nagios Remote Plugin Executor) que permite ejecutar scripts de manera remota en los host monitoreados. Dentro de cada servidor se puede monitorear el estado de servidores de correo, servidores Web, manejadores de bases de datos, entre otros servicios. Así como llevar registro de la utilización del ancho de banda, utilización del disco duro y otras estadísticas. Además puede ser configurado para tomar acciones ante un problema, de forma que a la vez que se generan alertas, se pueda realizar una acción concreta, por ejemplo, reiniciar un demonio. Asimismo permite establecer formas de monitoreo jerárquico lo cual es muy ventajoso en entornos con una gran cantidad de equipos.

Luego de la descripción de las más destacadas herramientas de gestión de red, vemos que es perfectamente factible gestionar una red de forma eficiente con herramientas libres, pues como hemos detallado existen herramientas con similares y mejores características que las aplicaciones comerciales para gestión de redes.

Nagios está desarrollado en lenguaje C, lo cual asegura portabilidad y una rápida ejecución de la información procesada. Al ser un software gratuito y de libre distribución, permite que el usuario pueda disponer siempre de nuevas actualizaciones y de contar con el soporte de una gran comunidad de desarrolladores, e incluso tener acceso al código fuente para modificarlo y adaptarlo a nuestras necesidades.

Nagios permite al administrador de una red, realizar un monitoreo exhaustivo y tener control total de la misma, determinando los problemas que se presentan en ella antes de que estos sean percibidos por los usuarios de la red, para de esta manera tomar la iniciativa y dar las soluciones más idóneas en base al análisis e interpretación de la información proporcionada por Nagios, que basa su funcionamiento en distintos archivos de configuración, en los cuales se especifica los elementos de red que van a ser monitoreados, con qué frecuencia se lo va a realizar, a quién y de qué manera se van a enviar los resultados de la monitorización, para lo cual cuenta con una gran cantidad de Plugins o script desarrollados en distintos lenguajes de programación y que son los encargados de realizar el monitoreo y recopilar la información de acuerdo a lo especificado en dichos archivos.

Esta herramienta dispone de una interfaz web en la cual se pueden visualizar de una manera rápida y sencilla el estado de los dispositivos o servicios que se están monitoreando, además proporciona distintas opciones para la generación de reportes en base a la información recolectada. Nagios es muy utilizado en entornos como granjas de servidores o empresas que cuentan con equipos en grandes instalaciones, teniendo un funcionamiento muy óptimo mediante la obtención, interpretación y decisión de eventos.

En la siguiente tabla se resume un cuadro comparativo con las principales características de cada una de las aplicaciones de monitoreo anteriormente mencionadas.

NOMBRE	GRÁFIC.	ESTADÍST.	AUTO DESCUB.	SYSLOG	ALERTAS	LICENCIA	INTERFAZ	AGENTES
HP Openview	Si	Si	Si	Si	Si	Comercial	Gráfica	SNMP, NNM.
IBM Tivoli	Si	Si	Si	Si	Si	Comercial	Control total vía WEB	SNMP, con agente.
Solarwinds	Si	Si	Si	Si	Si	Comercial	Control total vía WEB	No
MRTG.	Si	Si	No	Si	Si	GPL	WEB	Si
RRDTools.	Si	No	No	Si	No	GPL	WEB	Si
SmokePing.	Si	No	No	Si	Si	GPL	WEB	Si
Cacti.	Si	Si	Si	Si	Si	GPL	Control total vía WEB	Si
OpenNMS	Si	Si	Si	Si	Si	GPL	Control total vía WEB	SNMP, WMI, JMX, etc
ZABBIX	Si	Si	Si	Si	Si	GPL	Control total vía WEB	Si
Pandora	Si	Si	Si	Si	Si	GPL	Control total vía WEB	Con agente y sin agente
ZENOSS	Si	Si	Si	Si	Si	GPL	Control total vía WEB	SNMP, WMI, JMX, etc
Nagios	Si	Si	Si	Si	Si	GPL	Solo Visualización	Si

CAPITULO 3. ESTUDIO COMPARATIVO DE GESTIÓN Y MONITOREO DE ACUERDO A LAS CARACTERÍSTICAS DEL TIPO DE RED SELECCIONADO.

3.1. INTRODUCCIÓN.

La noción de red está definida fundamentalmente con el concepto de centralidad. Por lo tanto en las redes no se habla de jerarquías absolutas, se introduce un nuevo concepto que es el de la noción de red está.

El término administración de redes es definido como la suma total de todas las políticas, procedimientos que intervienen en la planeación, configuración, control, monitoreo de los elementos que conforman a una red con el fin de asegurar el eficiente y efectivo empleo de sus recursos. Lo cual se verá reflejado en la calidad de los servicios ofrecidos.

A continuación se describen las actividades ubicadas dentro del proceso de la administración de la configuración. Estas actividades son la planeación y diseño de la red; la instalación y administración del software; administración de hardware, y el aprovisionamiento. Además se mencionan los procedimientos y políticas que pueden ser de ayuda para el desarrollo general de una infraestructura de red.

Selección de la infraestructura de red.

Esta selección se debe realizar de acuerdo a las necesidades y la topología propuesta. Si se propuso un diseño jerárquico, se deben seleccionar los equipos adecuados para las capas de acceso, distribución y núcleo (core). Además, la infraestructura debe cumplir con la mayoría de las necesidades técnicas de la red. Lo mas recomendable es hacer un plan de pruebas previo al cual deben ser sujetos todos los equipos que pretendan ser adquiridos.

Instalaciones y Administración del software.

El objetivo de estas actividades es conseguir un manejo adecuado de los recursos de hardware y software dentro de la red.

Instalaciones de hardware.

Las tareas de instalación de hardware contemplan, tanto la agregación como la sustitución de equipamiento, y abarcan un dispositivo completo, como un switch o un ruteador; o solo una parte de los mismos, como una tarjeta de red, tarjeta procesadora, un módulo, etc.

Administración del software.

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. 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.

Provisionamiento.

Esta tarea tiene la función de asegurar la redundancia de los elementos de software y hardware más importantes de la red. Puede llevarse a cabo en diferentes niveles, a nivel de la red global o de un elemento particular de la red. Es la responsable de abastecer los recursos necesarios para que la red funcione, elementos físicos como conectores, cables, multiplexores, tarjetas, módulos, elementos de software como versiones de sistema operativo, parches y aplicaciones. Además de hacer recomendaciones para asegurar que los recursos, tanto de hardware como de software, siempre se encuentren disponibles ante cualquier eventualidad.

3.2. CARACTERÍSTICAS DE LA RED SELECCIONADA.

En la actualidad nos encontramos en un momento decisivo respecto del uso de la tecnología para extender y potenciar una red. La globalización de internet se ha producido más rápido que lo que cualquiera hubiera imaginado. El modo en que se producen las interacciones sociales, comerciales, políticas, personales y educativas cambia en forma continua para estar al día con la evolución de esta red global, en éste capítulo se hará un análisis de la red a gestionar con la ayuda de productos y servicios diseñados específicamente para aprovechar al máximo las capacidades de la red.

Comunicación, colaboración y compromiso son los componentes básicos de la educación. Las instituciones educativas se esfuerzan continuamente para mejorar estos procesos y maximizar la diseminación del conocimiento. Redes confiables y sólidas respaldan y enriquecen las experiencias de aprendizaje de los estudiantes, los materiales de aprendizaje incluyen actividades interactivas, evaluaciones y comentarios. El acceso a una instrucción de alta calidad no está restringido a estudiantes que viven cerca del lugar de instrucción y una red bien gestionada ayuda a la tarea de impartir conocimientos y elevar la calidad de aprendizaje eliminando barreras geográficas, de ésta forma mejorando las oportunidades para los estudiantes.

Una red de campus universitario incluye dispositivos, medios y servicios unidos por reglas, que trabajan en forma conjunta para enviar y recibir datos y/o información. Para que funcione una red los dispositivos deben estar interconectados a través de medios para proporcionar servicios deben estar gobernados por reglas o protocolos. Los protocolos son reglas que utilizan los dispositivos de res para comunicarse entre si.

La red a gestionar es una plataforma definida como una red convergente, el flujo de voz, video y datos que viajan a través de la misma red elimina la necesidad de crear y mantener redes separadas. En una red de campus universitario hay muchos puntos de contacto y muchos dispositivos especializados pero una sola infraestructura en común.

Este tipo de redes deben admitir una amplia variedad de aplicaciones y servicios, así como también puede expandirse rápidamente para admitir nuevos usuarios y aplicaciones sin afectar el rendimiento del servicio enviado a los usuarios actuales.

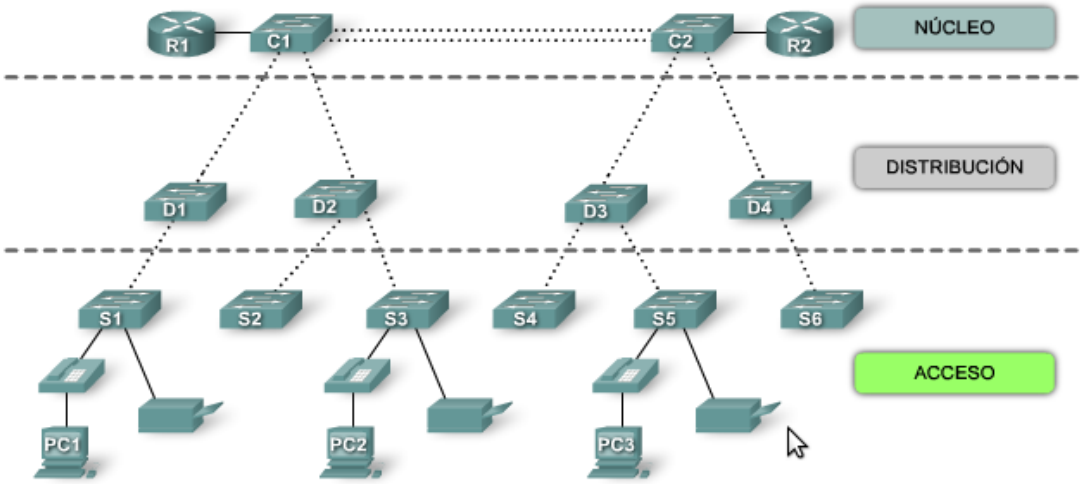


Figura 3.1. CARACTERÍSTICAS GENERALES DE LA RED – MODELO JERÁRQUICO.

Por lo general las redes en el ámbito educativo son de carácter jerárquico, es decir están estructuradas en tres capas: capa de acceso, capa de distribución capa de núcleo.

Capa de acceso.- Hace interfaz con dispositivos finales como las PC, impresoras, etc. Esta capa de acceso puede incluir ruteadores, conmutadores, puentes, etc. El propósito principal de la capa de acceso es aportar un medio de conexión de los dispositivos a la red y controlar que dispositivos pueden comunicarse en la red.

Capa de distribución.- Esta capa agrega los datos recibidos de los switches de la capa de acceso antes de que se transmitan a la capa de núcleo para el enrutamiento hacia su destino final. La capa de distribución controla el flujo de tráfico de la red con el uso de políticas y traza los dominios de braodcast al realizar el enrutamiento de las funciones entre las redes definidas en la capa de acceso.

Capa núcleo.- El núcleo del diseño jerárquico es la backbone de alta velocidad de la infraestructura de red. La capa de núcleo es esencial para la interconectividad entre los dispositivos de la capa de distribución, por lo tanto es importante que el núcleo sea sumamente disponible y redundante, el núcleo agrega el tráfico de todos los dispositivos de la capa de distribución, por lo tanto debe poder reenviar grandes cantidades rápidamente.

Existen muchos beneficios asociados con los diseños de la red jerárquica.

Escalabilidad.

Las redes jerárquicas escalan muy bien. La modularidad del diseño le permite reproducir exactamente los elementos del diseño a medida que la red crece. Debido a que cada instancia del módulo es consistente, resulta fácil planificar e implementar la expansión.

Redundancia.

A medida que crece una red, la disponibilidad se torna más importante. Puede aumentar radicalmente la disponibilidad a través de implementaciones redundantes fáciles con redes jerárquicas.

Rendimiento.

Luego, la capa de distribución utiliza sus capacidades de conmutar el alto rendimiento para reenviar el tráfico hasta el núcleo, donde se enruta hacia su destino final. Debido a que las capas núcleo y de distribución realizan sus operaciones a velocidades muy altas, no existe contención para el ancho de banda de la red. Como resultado, las redes jerárquicas con un diseño apropiado pueden lograr casi la velocidad de cable entre todos los dispositivos.

Seguridad.

La seguridad mejora y es más fácil de administrar, se cuenta con la flexibilidad de utilizar políticas de seguridad más avanzadas en la capa de distribución. Puede aplicar las políticas de control de acceso que definen qué protocolos de comunicación se implementan en su red y dónde se les permite dirigirse.

Facilidad de administración.

La facilidad de administración es relativamente simple en una red jerárquica. Cada capa del diseño jerárquico cumple funciones específicas que son consistentes en toda esa capa.

Capacidad de mantenimiento.

Debido a que las redes jerárquicas son modulares en naturaleza y escalan con mucha facilidad, son fáciles de mantener. Con otros diseños de la topología de la red, la administración se torna altamente complicada a medida que la red crece. También, en algunos modelos de diseños de red, existe un límite en cuanto a la extensión del crecimiento de la red antes de que se torne demasiado complicada y costosa de mantener.

3.3 MODELO DE GESTIÓN A SER TOMADO EN CUENTA.

La finalidad de llevar a cabo una administración de redes es dar un servicio para emplear una variedad de herramientas, aplicaciones y dispositivos que sirvan para ayudar en la supervisión y mantenimiento. Cabe destacar que esta tarea recae en un administrador de red, no es más que una persona responsable de supervisar y controlar el hardware y software de la misma, trabaja en la detección y corrección de problemas que hacen ineficiente o imposible la comunicación.

La administración de una red puede ser difícil por dos razones:

1.- La mayor parte de las redes son heterogéneas, es decir, la red consta de componentes de hardware y software fabricado por varias compañías. Los pequeños errores de un proveedor pueden hacer incompatibles los componentes.

2.- Las redes en su mayor parte son grandes. La detección de las causas de un problema de comunicación puede ser muy difícil si el problema sucede entre computadoras de sitios diferentes.

Aunque el hardware de red y el software de protocolo deben tener mecanismos para detectar automáticamente fallas y retransmitir paquetes, los administradores tienen la tarea de detectar y corregir los problemas subyacentes porque las retransmisiones reducen el desempeño de todas las computadoras que comparten la red.

Sin embargo es el software como administración de red que permitirá al administrador supervisar y controlar los componentes; por ejemplo, investigar y determinar el funcionamiento de dispositivos como hosts, ruteadores, conmutadores, hub, Switches y Routers determinando su estado y obtener estadísticas sobre las redes a las que se conectan, también controlar tales dispositivos cambiando las rutas y configurando interfaces.

Puede parecer extraño que se empleen protocolos para la administración de redes, si a fin de cuentas, las fallas de los protocolos y del hardware pueden evitar que los paquetes viajen de un dispositivo a otro y hagan imposible el control de un dispositivo cuando ocurre una falla; sin embargo, en la práctica los protocolos que son empleados por el administrador de red se operan en el nivel de aplicación.

El Protocolo Sencillo de Administración de Redes SNMP es un protocolo de administración de redes estándar usado en Internet. Este protocolo, define la comunicación de un administrador con un agente, lo que significa que define el formato y el significado de los mensajes que intercambian el administrador y el agente. Es decir, en lugar de definir muchas operaciones, el SNMP utiliza el paradigma de obtención y almacenamiento, mas no define el grupo de variables que se pueden emplear. SNMP, en sus distintas versiones, es un conjunto de aplicaciones de gestión de red que emplea los servicios ofrecidos por TCP/IP y que ha llegado a convertirse en un estándar.

La evolución de las redes no fue prevista de la misma forma en las herramientas de gestión, al menos de forma unísona. Mientras los órganos de normalización procedían a diseñar complejos y completos sistemas de gestión de red, el modelo de gestión SNMP para redes TCP/IP ganaba adeptos entre fabricantes y usuarios por su sencillez.

Finalmente, en una evolución natural de las necesidades, ambos caminos se han encontrado, observando en las redes de gestión actuales una organización por capas, pero haciendo un uso imprescindible del protocolo SNMP (adaptando la estructura de la red de gestión a las necesidades de los agentes).

3.4. METODOLOGÍA DE DESARROLLO.

Cada organización es única, tiene su propia combinación exclusiva de recursos, en el caso de una entidad educativa no es diferente, ésta singularidad hace necesario que cada organización desarrolle sus propias especificaciones de su sistema de gestión de red, mediante una evaluación sistemática de su propio ambiente externo e interno y de su punto de vista, de acuerdo con sus propias necesidades únicas.

Por otra parte, la mejor manera de implementar un sistema de gestión de red es haciéndolo desde abajo hacia arriba; es decir, empezando en los niveles más bajos de la organización y progresivamente cubrir aplicaciones en los niveles superiores. Este enfoque asegura que se recogen datos al más bajo nivel de detalle proporcionándolos a los niveles más altos a medida que se necesitan.

No subestimar la inercia. Cualquier sistema posee inercia, es decir, resistencia a los cambios en su estado. Los sistemas de gestión no constituyen una excepción. Por esta razón, cuando se implementa una nueva tecnología administrativa es necesario considerar la tendencia natural de las personas de resistirse al cambio.

Lo que se propone hacer se compone de dos etapas:

1.- Análisis del entorno.

2.- Implantación del sistema de gestión.

Análisis del entorno.

El objetivo de ésta primera etapa es investigar acerca de las tecnologías que posee la institución educativa esto es observar y documentar los equipos que posee la institución y cómo son utilizados. Observar cómo se manejan los usuario del entorno de red, cuáles son las estrategias implícitas en el entorno con respecto al trabajo y al manejo de la información.

Lo que se procederá a hacer es reconocer el entorno y definir las aplicaciones usadas por cada usuario, con esto se podrá tener una visión general respecto de áreas y recursos que se van a gestionar en la infraestructura de red, de esta manera se creará un documento detallando los objetivos y procesos para asegurar el entorno de red, y llevar a cabo un plan de trabajo a seguir asignando recursos.

El siguiente paso es efectuar una inspección general sobre la institución educativa y sus bienes informáticos, además se tiene que obtener información del usuario respecto a las amenazas que existen en su entorno de trabajo, para con ello determinar las amenazas y analizar el impacto de las vulnerabilidades detectadas.

Lo que sigue es la planificación que comprende un análisis detallado de los puntos a proteger estudiando el entorno en distintos aspectos como: el físico, el lógico, y el de la institución, al término de ésta etapa se tendrá una idea mas clara de la infraestructura de red donde implementaremos el sistema de gestión de red.

La implantación del sistema de gestión.

Esta segunda etapa comprende la implantación de las técnicas que se eligieron en la etapa anterior, generando y desarrollando los modelos de análisis que forman parte del Plan de Aseguramiento y que servirán de ahí en adelante, durante toda la vida del entorno.

En la etapa de la implementación se llevará a cabo el Plan de Aseguramiento antes propuesto y las etapas de ajuste político y organizativo que se considere necesario. Aquí se empezará con la elaboración del levantamiento de activos, aquí se realiza el inventario de los bienes físicos y lógicos de la red a gestionar en la institución educativa, luego se clasifica la información según su grado de vulnerabilidad.

Desde aquí se realizara el método de seguridad donde se da inicio al proceso de aseguramiento del entorno de red comenzando con los requisitos, normativas que debe cumplir la institución educativa, para luego poder implantar el plan de aseguramiento donde se darán las medidas que se han planificado con anterioridad para todos los niveles el físico, lógico y el organizacional.

En base a las metodologías afines descritas, el paradigma del modelo en cascada, la metodología RUP y de acuerdo a la documentación de algunos proyectos implementados, básicamente en los elementos clave y en objetivos claros y alcanzables, a continuación de describe la Metodología para la Implantación de un Sistema de Gestión.

La metodología desarrollada tiene por objetivo guiar en la implantación de un Sistema de gestión, a través de la planificación del proyecto, definición de una visión y alcance claros y concisos, elaboración de un cronograma de trabajo para el control y seguimiento del proyecto, elaboración de un plan de riesgos que permita cumplir las fechas y tiempos establecidos en el cronograma de trabajo, y un involucramiento del nivel directivo para la toma de decisiones tempranas.

Otro de los aspectos parte de la metodología consistirá en revisar los procesos base de la institución educativa con la funcionalidad del sistema; así mismo se definirá la configuración y parametrización del sistema acorde a los requerimientos de usuario y se realizarán las respectivas pruebas de integridad a través de los usuarios finales; finalmente una vez cumplidas las fases anteriores el sistema de gestión estaría listo para empezar a monitorear la red.

A continuación se describen las fases que forman la metodología desarrollada.

Fase Inicio.- Tiene como objetivo principal, definir todas y cada una de las actividades para la creación y planificación del proyecto, esto es elaborar un documento de Visión y Alcance, un Cronograma de Trabajo basado en la métrica Puntos de Función, una Matriz de Riesgos, una Presentación del proyecto y una Carta de compromiso, documentos que permitan establecer un control y seguimiento adecuados al proyecto.

Fase Selección Sistema de Gestión de Red.- Consistirá en realizar un análisis de la funcionalidad de varios sistemas de gestión versus los requerimientos de usuario o especificaciones técnicas de cada una de las áreas involucradas, obteniéndose un sistema de gestión seleccionado.

Fase Mapeo sistema de Gestión.- Tiene por finalidad es revisar los procesos base del entorno para integrarlos a la funcionalidad del sistema de gestión con las mínimas adecuaciones que abarquen en un 80% o 90% los servicios y aplicaciones de los nodos gestionados.

Fase Configuración Sistema de Gestión de Red.- Tiene como propósito, realizar la configuración y parametrización del sistema de gestión, configurar si es necesario a los nodos de la red, realizar pruebas de cada una de las áreas del entorno y pruebas de integración entre ellas, a través de los usuarios funcionales.

Fase Implantación Sistema de Gestión de Red.- Una vez configurado y parametrizado el sistema de gestión, la fase denominada Implantación del sistema gestión tiene como ideal a la funcionalidad común de los nodos de red y a temas funcionales particulares, obteniendo la información deseada de mismos o a su vez solucionando los problemas de parametrización que se presenten.

3.5. INFRAESTRUCTURA GENERAL DE UNA RED PARA CAMPUS UNIVERSITARIO.

Las infraestructuras de red pueden variar en gran medida en términos de: el tamaño del área cubierta, la cantidad de usuarios conectados, y la cantidad y tipos de servicios disponibles.

Las universidades en sí mismas son espacios que deberían ser abiertos a la sociedad, sin embargo se muestran cerrados ante las necesidades del entorno. Paradójicamente a esta visualización general que se tienen hacia ellas.

Una red de campus universitario generalmente cubre una única área geográfica y proporciona servicios y aplicaciones a personas dentro de una estructura organizacional común, este tipo generalmente son de área local.

Una red LAN por lo general está administrada por un único departamento u organización, el control administrativo que rige las políticas de seguridad y control de acceso está implementado en niveles como:

- La cantidad y calidad de equipos disponibles para los estudiantes
- La cantidad y calidad de equipos disponibles para los funcionarios administrativos.
- Las condiciones de conexión de la red de comunicación a todos los edificios de la universidad, su velocidad, confiabilidad y soporte.
- El número de equipos conectados a Internet, para clases y conferencias virtuales.
- La conexión de la universidad a la red de Internet, respecto a la velocidad, confiabilidad y soporte.

La meta de una infraestructura de red es satisfacer los requerimientos inmediatos y futuros de los usuarios o nodos.

Las redes no pueden ser divididas en subredes basándose únicamente en el número de usuarios. La aparición de servidores capaces de ejecutar aplicaciones globales tiene también una incidencia directa en la carga de la red. Un tráfico elevado en la red global supone tener que emplear técnicas de enrutamiento y conmutación más eficaces.

Tradicionalmente, las redes de campus han colocado la logística y servicios básicos a nivel de red en el centro de la red, compartiendo el ancho de banda a nivel de usuario. Conforme el desarrollo tecnológico se va apoyando cada vez más en la red como herramienta de productividad, los servicios de red distribuidos y la conmutación van migrando hasta el nivel de puesto de trabajo. Dicho esto consideramos las siguientes características generales en una red de campus universitario.

Estándar

Ethernet es un estándar de redes de área local para computadores con acceso al medio por contienda CSMA/CD. CSMA/CD (Acceso Múltiple por Detección de Portadora con Detección de Colisiones), es una técnica usada en redes Ethernet para mejorar sus prestaciones. El nombre viene del concepto físico de ether. Ethernet define las características de cableado y señalización de nivel físico y los formatos de tramas de tramas de datos del nivel del enlace de datos del modelo OSI.

En una red Ethernet, cuando un dispositivo desea enviar datos a otro, puede abrir una ruta de comunicación hacia el otro dispositivo usando la dirección MAC. Cuando se envían datos desde un origen a través de una red, los datos transportan la dirección MAC del destino deseado. A medida que estos datos viajan a través de los medios de red, la NIC de cada dispositivo de la red verifica si la dirección MAC coincide con la dirección destino física que transporta el paquete de datos. Si no hay concordancia, la NIC descarta el paquete de datos.

Topología.

La topología lógica de una red es la forma en que los hosts se comunican a través del medio. Los dos tipos más comunes de topologías lógicas son broadcast y transmisión de tokens.

La **topología broadcast** simplemente significa que cada host envía sus datos hacia todos los demás hosts del medio de red. Las estaciones no siguen ningún orden para utilizar la red, el orden es el primero que entra, el primero que se sirve. Esta es la forma en que funciona Ethernet.

Medio físico.

Cable de categoría 6, o Cat 6 (ANSI/TIA/EIA-568-B.2-1) es un estándar de cables para Gigabit Ethernet y otros protocolos de redes que es retrocompatible con los estándares de categoría 5/5e y categoría 3. La categoría 6 posee características y especificaciones para crosstalk y ruido. El estándar de cable es utilizable para 10BASE-T, 100BASE-TX Y 1000BASE-TX (Gigabit Ethernet). Alcanza frecuencias de hasta 250 MHz en cada par y una velocidad de 1Gbps.

Topología Física.

El término topología puede definirse como el "estudio de la ubicación". La topología es objeto de estudio en las matemáticas, donde los "mapas" de nodos (puntos) y los enlaces (líneas) a menudo forman patrones.

La topología en estrella extendida tiene una topología en estrella central, en la que cada uno de los nodos finales actúa como el centro de su propia topología en estrella. La ventaja de esto es que el cableado es más corto y limita la cantidad de dispositivos que se deben interconectar con cualquier nodo central. La topología en estrella extendida es sumamente jerárquica, y busca que la información se mantenga local.

Dispositivos de red.

Los dispositivos y los medios son los elementos físicos de la red. El hardware es generalmente el componente visible de la plataforma de red.

Los dispositivos de interconexión de redes y de red se dividen en cuatro categorías: repetidores, puentes, encaminadores y pasarelas. Cada uno de los cuatro tipos interactúa en diferentes niveles del modelo OSI, los repetidores actúan sólo sobre los componentes eléctricos de una señal y sólo son activos en el nivel físico. Los puentes utilizan protocolos de direccionamiento y pueden afectar al control de una única red, la mayoría son activos en el nivel de enlace de datos. Los encaminadores ofrecen enlaces entre dos redes diferentes del mismo tipo por lo que están en el nivel de red, por último las pasarelas proporcionan servicios de traducción entre redes y son activas en todos los niveles. Cada tipo es también activo en los niveles inferiores a aquel en que sea en mayor parte activo.

La administración de datos mientras fluyen en la red es función de los dispositivos de red, los procesos que se ejecutan el los dispositivos de red realizan las siguientes funciones: regenerar y retransmitir señales, mantener información sobre qué rutas existen a través de la red, notificar a otros dispositivos errores y fallas de la comunicación.

Dispositivos de usuario final.

Los dispositivos más comunes y con los que el usuario está más familiarizado se denominan dispositivos finales, estos dispositivos constituyen la interfaz entre la red humana y la red de comunicación subyacente. Algunos ejemplos de dispositivos finales son: estaciones de trabajo, servidores, impresoras de red, teléfonos IP, etc.

En el contexto de la red, los dispositivos finales se denominan host. Un dispositivo host puede ser origen o el destino de un mensaje transmitido a través de red. Hoy en día un host puede funcionar como un cliente, como un servidor o como ambos, el software instalado en el host determina qué rol representa en la red.

Los servidores son host que tienen software instalado que les permite proporcionar información y servicios a otros host de la red.

Los clientes son host que tienen software instalado que les permite solicitar y mostrar la información obtenida del servidor.

Las infraestructuras de red de campus universitario pueden variar en gran medida en términos de:

(1) Tamaño de área cubierta.

(2) Cantidad de usuarios.

(3) Cantidad y tipos de servicios disponibles.

Una red de campus universitario generalmente cubre una única área geográfica y proporciona servicios y aplicaciones a personas dentro de una estructura organizacional común. Este tipo de red se denomina red de área local. Una LAN por lo general está administrada por una organización única, el control administrativo que rige las políticas de seguridad y control de acceso está implementado en el nivel de red.

3.6. REQUERIMIENTOS.

Monitoreo informático (o monitorización), refiere al flujo de información que se genera desde y hacia la estructura informática (en sentido amplio, contemplando hardware, software e infraestructura), con el objeto de relevar el estado en el que se encuentran los distintos parámetros operativos, con la intención de alimentar diversos procesos.

Existen tipos de monitoreo: manual y remoto.

El monitoreo manual es más frecuente de lo que podría pensarse. De hecho, es el mecanismo más habitual. En este, uno o varios operadores, revisan parámetros que consideran relevantes de la infraestructura de red, e intentan detectar condiciones no deseadas para luego poder proceder a la toma de acción.

Habitualmente este modelo es extremadamente costoso en términos de esfuerzo (horas-hombre), ya que el tiempo insumido se repite, en la medida que no se tomen acciones para automatizarlo.

En el monitoreo automático, se elaboran instrumentos informáticos para efectuar el control, que deben considerar básicamente 3 aspectos:

- Como ejecutar el control (puede ser en forma manual, o automática mediante schedulers[19]).
- Como obtendrá el control la información deseada (una vez disparado).
- Como reportará los resultados.

El segundo de estos puntos es el que habitualmente recibe una mayor atención. Si bien es seguramente el más importante de los tres (sin él los otros dos no tienen sentido), es de suma importancia conseguir respuestas efectivas para los otros aspectos.

En el monitoreo automático, por estar estrechamente ligado a la noción de repetición del control, es fundamental la revisión y ajuste de las herramientas utilizadas para asegurar la efectividad a lo largo del tiempo.

19 *El planificador es un componente funcional de los sistemas operativos, su función es repartir el tiempo disponible de un microprocesador entre todos los procesos que están disponibles para su ejecución.*

Cuando se cumplen con estos objetivos, los recursos de operación ven aliviada su carga de tareas repetitivas y se pueden reasignar a otras de mayor valor.

El monitoreo remoto ocurre cuando para el control de un determinado servicio de la infraestructura de red, toda la ejecución del software de control ocurre sin utilizar recursos del equipamiento monitoreado.

En contraposición, en el monitoreo local, se involucran recursos del equipo a monitorear para la ejecución de software de control.

Esta distinción entre ambas modalidades, tiene implicaciones sobre el significado y la interpretación que deben asignarse a un control; y debe ser tenida en cuenta a la hora de diseñar un procedimiento de monitoreo. Mediante monitoreo local, podemos tener la posibilidad de relevar diversos parámetros y conocer en profundidad las causas de un mal funcionamiento cuando este ocurra. Estas son las ventajas que se obtienen con un monitoreo local (o interno).

Sin embargo, con un monitoreo remoto, a pesar de limitarse el acceso a información de detalle; podemos conocer como se percibe el servicio monitoreado, desde un punto externo al propio servidor. Debe considerarse que si ambos controles generarán un log con los resultados de sus ejecuciones, en los equipamientos donde se ejecutan, ante una pérdida de conectividad del nodo (con el resto del mundo), obtendríamos un escenario en donde se registra dicha caída en el log del monitoreo remoto, pero no se detectan caídas en el log local.

El monitoreo de red involucra muchas actividades incluyendo búsqueda de fuentes de interferencia, detección e identificación de transmisores o nodos nuevos, desconocidos, localización de emisores y monitoreo de emisiones a largo plazo para verificar cumplimiento de las políticas de seguridad y gestión de red.

Cada una de estas actividades tiene su propio flujo de trabajo característico. Para hacer la operación lo más simple posible para el usuario y para asegurar un trabajo eficiente y libre de errores, los flujos de trabajo individuales son implementados usando una serie de requerimientos de información de gestión tales como: monitoreo de servicios, monitoreo de logs, notificaciones, etc.

3.6.1. MONITOREO DE SERVICIOS.

La finalidad de una red es que los usuarios de los sistemas informáticos de una entidad educativa puedan hacer un mejor uso de los mismos mejorando de este modo el rendimiento global de la entidad. Así las organizaciones obtienen una serie de ventajas del uso de las redes en sus entornos de trabajo, como pueden ser:

- Mayor facilidad de comunicación.
- Mejora de la competitividad.
- Mejora de la dinámica de grupo.
- Reducción del presupuesto para proceso de datos.
- Reducción de los costos de proceso por usuario.
- Mejoras en la administración de los programas.
- Mejoras en la integridad de los datos.
- Mejora en los tiempos de respuesta.
- Flexibilidad en el proceso de datos.
- Mayor variedad de programas.
- Mayor facilidad de uso. Mejor seguridad.

Para que todo esto sea posible, la red debe prestar una serie de servicios a sus usuarios, como son: accesos, ficheros, impresión, correo, información, etc.

Para la prestación de los servicios de red se requiere que existan equipos en la red con capacidad para actuar como servidores. Los servidores y servicios de red se basan en los sistemas operativos de red.

Un sistema operativo de red es un conjunto de programas que permiten y controlan el uso de dispositivos de red por múltiples usuarios. Estos programas interceptan las peticiones de servicio de los usuarios y las dirigen a los equipos servidores adecuados. Por ello, el sistema operativo de red, le permite a ésta ofrecer capacidades de multiproceso y multiusuario. Según la forma de interacción de los programas en la red, existen dos formas de arquitectura lógica:

Cliente-servidor.

Este es un modelo de proceso en el que las tareas se reparten entre programas que se ejecutan en el servidor y otros en la estación de trabajo del usuario. En una red cualquier equipo puede ser el servidor o el cliente. El cliente es la entidad que solicita la realización de una tarea, el servidor es quien la realiza en nombre del cliente. Este es el caso de aplicaciones de acceso a bases de datos, en las cuales las estaciones ejecutan las tareas del interfaz de usuario (pantallas de entrada de datos o consultas, listados, etc.) y el servidor realiza las actualizaciones y recuperaciones de datos en la base.

En este tipo de redes, las estaciones no se comunican entre sí.

Las ventajas de este modelo incluyen:

- Incremento en la productividad.
- Control o reducción de costos al compartir recursos.
- Facilidad de administración, al concentrarse el trabajo en los servidores.
- Facilidad de adaptación.

Redes de pares (*peer-to-peer*).

Este modelo permite la comunicación entre usuarios (estaciones) directamente sin tener que pasar por un equipo central para la transferencia. Las principales ventajas de este modelo son:

- Sencillez y facilidad de instalación, administración y uso.
- Flexibilidad. Cualquier estación puede ser un servidor y puede cambiar de papel, de proveedor a usuario según los servicios.

Los servicios de acceso a la red comprenden tanto la verificación de la identidad del usuario para determinar cuáles son los recursos de la misma que puede utilizar, como servicios para permitir la conexión de usuarios de la red desde lugares remotos.

Control de acceso.

Para el control de acceso, el usuario debe identificarse conectando con un **servidor** en el cual se autentifica por medio de un nombre de usuario y una clave de acceso. Si ambos son correctos, el usuario puede conectarse a la red.

Acceso remoto.

En este caso, la red de la institución está conectada con redes públicas que permiten la conexión de estaciones de trabajo situadas en lugares distantes. Dependiendo del método utilizado para establecer la conexión el usuario podrá acceder a unos u otros recursos.

3.6.2. MONITOREO DE LOGS.

Los logs de eventos permiten a los administradores que revisen el historial reciente de un servidor o de un dispositivo de red y observar tendencias, fallas sucesos y otra información crítica para el campus universitario. En tiempo real pueden brindar indicadores de infecciones por troyanos y malware en equipos de redes. Los logs de eventos también almacenan pruebas potencialmente valiosas para el análisis "forense". Tras un incidente de seguridad en la red, los logs de eventos almacenan toda la información sobre dicho incidente; como sucedió, cuándo, y en el último caso las claves para prevenir que vuelva ocurrir.

Dado que puede brindar tanto como una defensa de primera línea, como los elementos necesarios para un análisis forense, el log de eventos es un componente clave de la seguridad de la red en la actualidad.

El poder monitorear los logs de eventos da al administrador de red una ventaja considerable para la identificación temprana de amenazas, algo que es mejor investigar los hechos que suceden. Una estrategia sólida de registro de eventos es la clave para tener un panorama completo del plan de seguridad de red en cualquier infraestructura de red. La presencia de monitoreo de eventos es la estrategia de que ayuda a distinguir un plan proactivo de uno reactivo. Las amenazas más serias a la seguridad de la red son internas y por o general se originan en la misma red, la causa puede ser un usuario molesto.

Cuando es externo, probablemente se trate también de los mismos gusanos o virus que atacan a una red doméstica, los equipos que combaten este tipo de amenazas son de gran ayuda, sin embargo un software de administración de logs de eventos puede ser tan o incluso más efectivo para defender la red. De hecho, una estrategia de administración de eventos es más efectiva para combatir ataque internos.

Rastrear los ingresos equivocados de contraseña, los accesos a archivos y carpetas, y comparar los inicios y cierres de sesión exitosos contra los fallidos, todas estas funciones pueden manejarse con facilidad mediante una estrategia de mantenimiento de logs integral.

A medida que la infraestructura de redes va creciendo y evolucionando en complejidad, la necesidad de contar con un sistema racional de análisis de datos es fundamentas para las operaciones diarias.

3.6.3. MONITOREO DE UPS.

Un UPS es un Sistema Ininterrumpido de Energía, conjunto de baterías y estabilizador de voltaje conectados al computador, que detecta pequeñas fluctuaciones eléctricas o cortes de energía, entregando electricidad propia de sus baterías. Estas tienen en promedio, dependiendo del consumo, una autonomía de servicio de 30 minutos.

UPS significa en inglés Uninterruptible Power Supply.

Los UPS suelen conectarse a la alimentación de los hosts, permitiendo usarlas varios minutos en el caso de que se produzca un corte eléctrico. Algunos UPS también ofrecen aplicaciones que se encargan de realizar ciertos procedimientos automáticamente para los casos en que el usuario no esté y se corte el suministro eléctrico.

El monitoreo de nuestro UPS es una gran herramienta en el uso cotidiano de la infraestructura de red, pues nos puede dar detalles con gran exactitud sobre el estado actual de nuestro UPS, por ejemplo indicándonos el estado de carga del UPS, en caso de tener una sobrecarga no será necesario tener que decodificar los sonidos que emite nuestro UPS, sino bastará con ir a la aplicación de monitoreo y

esta indicará si el UPS está sobrecargado midiéndolo en porcentajes de 0 a 100%, con esto se ahorra mucho trabajo y costes, incluso prolongando el tiempo de vida útil del UPS.

3.3.4. ENVÍO DE NOTIFICACIONES

Las notificaciones se derivan de eventos, el objetivo es notificar a al administrador o administradores cuando se genera un evento que coincide con determinados criterios. Las alertas ayudan a los administradores a monitorear servidores y procesos importantes de la red sin perder mucho tiempo revisando gráficos e informes. Existen dos mecanismos de notificaciones de alertas en la aplicación: notificaciones vía SMS al teléfono móvil y notificaciones vía email.

Hoy en día existen herramientas que permiten ejecutar un programa automáticamente cuando se genere una alerta y crear sus propios recursos de notificaciones, como RSS y Twitter. Notificaciones de traps SNMP es uno de los ejemplos de programas ejecutados.

Notificaciones vía email

EventLog Analyzer es un ejemplo, notifica a los operadores vía correo cuando se dispara una alerta. Las notificaciones vía correo instantáneas ayudan al departamento de monitoreo y administración de red a identificar y resolver los problemas más rápidamente.

Notificaciones de correo seguro.

Se pretende asegurar el envío de correos, mediante la configurar la autenticación segura de correos utilizando soporte para envío de notificaciones utilizando cuentas de Gmail (TLS).

Notificaciones vía SMS.

Consiste en configurar la herramienta de monitoreo para que notifique a los operadores vía SMS a sus teléfonos móviles cuando se dispara una alerta. Las notificaciones vía correo instantáneas ayudan a los administradores de red móviles a identificar los problemas más rápidamente y dedicarse a resolverlos.

Notificaciones de traps SNMP.

Puede configurar la herramienta de monitoreo para que notifique a los operadores enviando un trap SNMP cuando se dispara una alerta. Es posible reenviar el trap SNMP a cualquier aplicación de administración de red o activos.

3.6.5. REQUERIMIENTOS ADICIONALES.

En la gestión de red en general se tienen requerimientos adicionales a los ya expuestos para prepararse y ocuparse del mal manejo y del uso indebido de la información de un campus universitario. Logran esta meta, recopilando la información de una gran variedad de fuentes de la infraestructura de red y analizando la información que contribuye a los síntomas de los problemas de seguridad de la misma, y permiten que el usuario especifique las respuestas en tiempo real a las violaciones.

El objetivo es monitorear activamente los sistemas operativos y el tráfico de red, con el objeto de detectar ataques y violaciones a la seguridad, además de:

Vigilar y analizar la actividad de los usuarios y del sistema.

- Revisar las configuraciones del sistema y de las vulnerabilidades.
- Evaluar la integridad de los archivos críticos del sistema y de los datos.
- Reconocimiento de los modelos de la actividad que reflejan ataques conocidos.
- Análisis estadístico para los modelos anormales de la actividad.
- Gerencia del rastro de intervención del sistema operativo, con el reconocimiento de las violaciones de la actividad del usuario respecto a la política establecida.
- Vigilar el cumplimiento de políticas y procedimientos establecidos dentro de la institución.

La combinación de estas características hace que sea más fácil la gestión de red, y vigilar la intervención y la evaluación de sus sistemas y redes.

La meta es proporcionar una indicación de un potencial o de un ataque verdadero. Un ataque o una intrusión es un acontecimiento transitorio, mientras que una vulnerabilidad representa una exposición, que lleva el potencial para un ataque o una intrusión. La diferencia entre un ataque y una vulnerabilidad, entonces, es que un ataque existe en un momento determinado, mientras que una vulnerabilidad existe independientemente de la época de la observación. Otra manera de pensar en esto es que un ataque es una tentativa de explotar una vulnerabilidad (o en algunos casos, una vulnerabilidad percibida).

Una intrusión, explota una vulnerabilidad específica y debe ser detectada cuanto antes, después de que comience. Por esta razón, las herramientas de gestión de red deben de ejecutarse con más frecuencia que los exploradores de vulnerabilidad. Los sistemas de gestión de red examinan el sistema o la actividad de la red para encontrar eventuales intrusiones o ataques posibles.

En el monitoreo de una infraestructura de red se requiere tratar las siguientes cuestiones de gestión, sin importar en que mecanismo se basen:

- Debe ejecutarse continuamente sin la supervisión humana. El sistema debe ser bastante confiable y permitir que se ejecute en el fondo del sistema que es observado. Sin embargo, no debe ser un "rectángulo negro". Es decir, sus funcionamientos internos deben ser observables desde el exterior.
- Debe ser tolerante a fallos, en el sentido de que debe mantenerse ante un fallo del sistema, además no debe de poder reiniciar el sistema.
- Debe resistir el cambio. El sistema puede vigilarse para asegurarse de que no ha sido alterado.
- Debe imponer los gastos mínimos para el sistema.
- Debe observar desviaciones del comportamiento normal.
- Debe ser adaptado fácilmente al sistema en cuestión. Cada sistema tiene un diverso modelo de uso, y el mecanismo de la defensa debe adaptarse fácilmente a estos modelos.

- Debe hacer frente a comportamiento del sistema que cambia en un cierto periodo de tiempo, mientras que se están agregando las nuevas aplicaciones.

Algunos sistemas de gestión proporcionan ciertas características adicionales, incluyendo: la instalación automática de correcciones lógicas al software, instalación y operación de los servidores que registran la información de intrusos.

Los tipos de errores que probablemente puedan ocurrir en un sistema de gestión de red, se pueden categorizar cuidadosamente como:

- Positivo falso.
- Negativa falsa.
- Errores de cambio.

Un positivo falso ocurre cuando el sistema de gestión clasifica una acción como anómala (una intrusión posible) cuando es una acción legítima. Una negativa falsa ocurre cuando ha ocurrido una acción intrusa real pero el sistema permite que pase como no intruso. Un error de cambio, ocurre cuando un intruso modifica la operación del detector de la intrusión para forzar a que ocurran negativas falsas. Los errores positivos falsos conducirán a los usuarios y/o nodos de la red a no hacer caso de su salida, pues clasificará acciones legítimas como intrusiones. Las ocurrencias de este tipo de error se deben reducir al mínimo (puede no ser posible eliminarlas totalmente), para proporcionar la información útil a los operadores. Si muchos positivos falsos se generan también, los operadores vendrán no hacer caso de la salida del sistema en un cierto plazo, que puede conducir a una intrusión real que es detectada pero no hecha caso por los usuarios.

Un error negativo falso ocurre cuando procede una acción aunque es una intrusión. Los errores negativos falsos son más serios que errores positivos falsos porque dan un sentido engañoso de la seguridad. Permitiendo que todas las acciones procedan, una acción sospechosa no será traída a la atención del administrador de red. El sistema de gestión ahora es un defecto, pues la seguridad del sistema es menor que la que era antes de que el sistema de gestión fuera instalado.

Los errores de cambio son más complejos Un intruso podría utilizar conocimientos sobre los mecanismos internos de un sistema de gestión para alterar su operación, permitiendo posiblemente que el comportamiento anómalo proceda. El intruso podría entonces violar los apremios operacionales de la seguridad del sistema. Esto se puede descubrir por el administrador de red que examina los registros del software de gestión, pero parecería que el sistema de gestión todavía trabaja correctamente.

3.7 ESTUDIO COMPARATIVO DE LOS SISTEMAS DE GESTIÓN DE ACUERDO A LOS REQUERIMIENTOS DEL TIPO DE RED SELECCIONADO.

Hay tres valores técnicos fundamentales a la hora de elegir un sistema de monitorización adecuado para nuestro entorno de red, independientemente del precio o facilidad de instalación y de utilización. Estos tres valores son:

1. Forma de presentar los datos, las alarmas y gráficos para su estudio. Estos han de ser lo más eficientes posible y ofrecer una idea de los problemas de un solo vistazo.
2. Ubicación, distancia entre equipos y tipo de conexión (velocidad y rendimiento). A más distancia y cantidad de equipos, así como con conexiones lentas, es conveniente utilizar agentes locales que reporten a un servidor central.
3. Sistemas Operativos que se monitorizarán. Es más sencillo monitorizar únicamente máquinas basadas en Linux, aunque en la mayoría de los casos es fundamental hacerlo con Windows y conveniente utilizar WMI, (además de SNMP).

Los entornos de red cada vez son más diversos en cuanto a los sistemas operativos de cada unos de los hosts que pertenecen al entorno, los sistemas de gestión basados en arquitecturas de software libre han demostrado ser más eficientes y flexibles para administrar entornos con diferentes sistemas operativos. En nuestro caso optaremos por considerar herramientas de libre distribución.

3.7.1. SELECCIÓN DEL SISTEMA DE GESTIÓN.

Zenoss está ganando conversos a lo largo y ancho del globo. Zenoss incluye una impresionante lista de funcionalidades que parece crecer cada mes.

Zenoss soporta la monitorización y gestión de tecnologías como SNMP, WMI, ping, análisis de puertos y monitorización basada en ssh. SNMP es el estándar de facto para la obtención de información sobre redes, y casi todos los dispositivos de red computacionales lo soportan.

A los dispositivos que no usan SNMP o WMI, o que están fuera del alcance de las herramientas de monitorización convencionales, les podemos realizar pruebas de red limitadas mediante una monitorización basada en ping o en análisis de puertos.

La monitorización a través de ssh permite a Zenoss conectarse a la máquina y determinar su estado mediante la ejecución de comandos. Zenoss ofrece varias vías para la comunicación de información a través de la red, la primera opción es la interfaz web.

La primera aplicación interna, sub-aplicación o módulo, es el denominado **Administración y Configuración de la Base de Datos**. Desde aquí el administrador o encargado de la implementación de Zenoss, podrá hacer las configuraciones iníciales, registrar los equipos, redes, herramientas y hasta software a monitorear. Se podrá exportar e importar datos, elegir las configuraciones deseadas, entre otras muchas opciones más. Asimismo, hay que destacar que, Zenoss en las primera aplicación open source en implementar uno de estos módulos.

Herramientas como la de Monitoreo de Red, que se diseño estrictamente para trabajar en el análisis de las actividades de una red en la organización.

Se podrá realizar evaluaciones de acuerdo a las asignaciones de las IP de los equipos, de las identificaciones en la red, u otras características. También podremos verificar los recursos con los que cada una de las estaciones afiliadas a la red cuenta, y verificar cómo se está compartiendo la información.

Otro de los puntos clave de Zenoss es la integración de una herramienta de detección de tecnología nueva, si un sistema instalado en una de las estaciones sin autorización, o la derivación de información de la empresa sin autorización; gracias a este sistema se podrá detectar automáticamente cualquier variación en la red.

Una de las grandes herramientas de Zenoss es el Dashboard Configuration. Esta herramienta permite identificar a cada uno de los equipos, recursos y dispositivos tecnológicos de la organización. Provee de datos de ubicación, hora de conexión, entre otros de suma importancia. Las posibilidades de esto son impresionantes.

Para ejemplificar lo anterior, con Zenoss, y gracias a la configuración previa; se podrá acceder a la información de ubicación de equipos y su hora de conexión automáticamente. Esto es realmente útil, pues permite poner en contacto a las unidades de la entidad educativa, a cualquier hora y en cualquier lugar. El propósito de la herramienta de localización o Dashboard; Zenoss permite integración con Google Maps, permitiendo localizar gráficamente en los mapas que ofrece Google, a las unidades y dispositivos tecnológicos fuera de la empresa. Existen gran variedad de aplicaciones y características internas adicionales.

Al ser una herramienta muy potente y versátil, hablar de cada uno de sus componentes sería muy largo; por ello solo hemos descrito alguna de las mas interesantes y con mayor impacto distintivo dentro del mercado de aplicaciones para el monitoreo de tecnología.

Zenoss ofrece muchas posibilidades y recursos más, y se constituye en otra de las prometedoras opciones de código libre que se ofrecen a las instituciones. Su plataforma está dirigida a empresas pequeñas y medianas, pues les permite ahorrar costos en materia de monitoreo de tecnología.

A su vez, Zenoss permite a estas empresas, la posibilidad de incorporar a sus procesos y sistemas de control, una herramienta que, si no es hoy, será mañana muy necesaria en las empresas instituciones modernas.

3.7.2. VENTAJAS Y DESVENTAJAS.

Zenoss es un producto de vigilancia y seguimiento para una red informática y de supervisión de infraestructuras de red. Puede gestionar la configuración, salud, rendimiento de dispositivos, servidores y aplicaciones. Todo esto a través de un único paquete de integrado de software. Ofrece monitorización de dispositivos y servicios en la red (SNMP, HTTP, POP3, etc.), recursos hardware y detecta automáticamente nuevos recursos en la red y cambios en su configuración. Realiza notificaciones y alertas basados en un conjunto de reglas. Es un producto multiplataforma para soporte en clientes, incluyendo: Linux y Windows.

Para ser instalado como servidor soporta distribuciones:

- Linux: Red Hat, CentOS, Fedora, Debian, Ubuntu, OpenSUSE, SUSE.
- Mac OS X v10.5 y v10.6
- Windows (Requiere VMWare Player y la aplicación virtual Zenoss).

Para la consola o interfaz web necesita:

Firefox 3.6.x, 4, 5 o Internet Explorer 7, 8, 9.

Adobe Flash Player.

Zenoss utiliza una tecnología sin agentes (SNMP, SSH, Telnet y WMI) y se inicia con una CMBD (Base de datos de la Gestión de Configuración), la cual contiene detalles relevantes de cada elemento, generando a partir de esta la administración de fallos, notificaciones, alertas y tareas de remediación a fallos. Y además con un amplio inventario de cada recurso. Una vez que se descubre la infraestructura, comienza a monitorizar el rendimiento de cada dispositivo. Posteriormente, ofrece la gestión de eventos, automatización de alarmas e informes. Por tanto, los principales niveles o áreas del núcleo sistema son:

- Descubrimiento y Configuración.
- Rendimiento y Disponibilidad.
- Fallos y gestión de Eventos.
- Alertas y remedios.

- Generación de Informes.

La arquitectura del sistema viene separada y escalonada en cuatro partes principales:

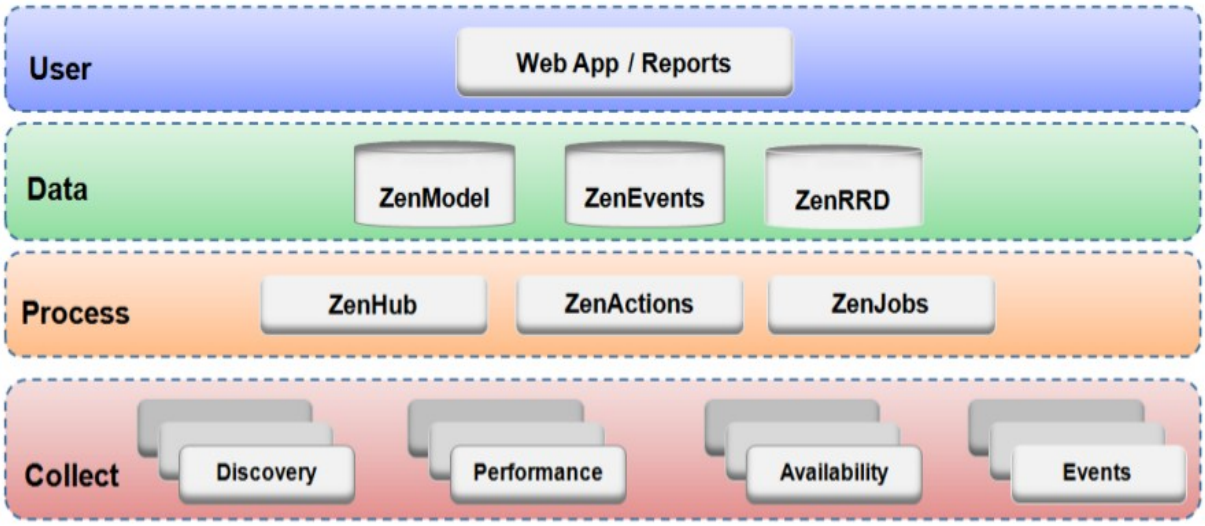


Figura 3.2. ARQUITECTURA DE ZENOSS.

La capa de usuario está construida alrededor de la interfaz o aplicación web e interactúa con la capa de datos para traducir la información y mostrarla al usuario. Dicha capa de datos, recopila la información y configuración y la almacena en tres bases de datos separadas:

- ZenRRD: Utiliza la herramienta RRDtool.
- ZenModel: Es el modelo de configuración del núcleo, que comprende los dispositivos, sus componentes, grupos y lugares.
- ZenEvents: Almacena los datos de eventos en una base de datos MySQL.

La capa de procesos gestiona la comunicación entre la capa de datos y la capa de colección y ejecuta periódicamente trabajos generados por el usuario (ZenActions y ZenJobs). Utiliza la herramienta Twisted PB para las comunicaciones. Por último, la capa de colección está formada por servicios o demonios que llevan a cabo funciones como la recopilación de información en máquinas remotas, disponibilidad (fallos de PING) y rendimiento (infracciones en los umbrales), los cuales son devueltos a través de ZenHub al sistema de eventos.

Combina programación propia y tecnologías de código abierto, con las cuales consigue integrar su software al completo. Por ejemplo, en el núcleo del sistema realiza tareas como el Modelado del Sistema, que le permite entender el entorno en el que opera, basado en el concepto de herencia de lenguajes de programación. Se puede citar algunas de las tecnologías utilizadas, como por ejemplo:

Zope: Aplicación web orientado a objetos. Está escrito en el lenguaje de programación Python. Es utilizado para la edición de contenidos, personalizaciones básicas y aporta ventajas respecto a lugares web compuestos por archivos de texto plano.

Python: Lenguaje de programación de alto nivel diseñado en 1991 por Guido van Rossum. Es un lenguaje multiparadigma (permite crear programas con más de un estilo de programación), ya que soporta programación orientado a objetos, programación imperativa (basado en estados y sentencias, variables globales, como en la programación o implementación hardware de las Máquinas de Turing) y en menor medida, programación funcional (basado en funciones aritméticas: Entrada -> Subrutina -> Salida). Es un lenguaje interpretado (ejecutado por un intérprete que convierte el lenguaje fuente en código máquina).

Net-SNMP: Protocolo de monitorización que recolecta información sobre el estado de los sistemas.

RRDtool: Es una herramienta ya mencionada y utilizada por otros productos de monitorización. Trabaja y tiene como objetivo la creación de gráficas y guarda registros temporales de datos. Una de sus principales características es que no crece con el paso del tiempo.

MySQL: Motor y gestor de base de datos relacional multihilo y multiusuario popularmente conocido.

Twisted PB: Es un framework de red para la programación dirigida por eventos escrito en Python. Soporta varias arquitecturas (TCP, UDP, SSL, IP, etc.) y protocolos (HTTP, XMPP, NNTP, SSH, etc.). Los usuarios pueden escribir pequeños callbacks (retrollamadas) para realizar tareas complejas.

Zenoss posee una comunidad “Zenoss Core Comunnity” la cual dispone de un repositorio de plugins llamado ZenPacks, con los cuales los miembros de la comunidad pueden extender las funcionalidades de Zenoss Core. Además, **el software soporta el formato de plugins de Nagios**.

Para la visualización y control total de la aplicación aporta una interfaz o Consola Web, la cual permite manejar el estado y situación de la infraestructura de red. Se puede personalizar por distintos roles para usuario y se puede integrar con Google Maps para visualizar problemas geográficamente., en el caso de redes distribuidas.

De lo expuesto anteriormente podemos resumir como **principales ventajas:**

(1) Fácil de instalar.

(2) Soporta plugins de herramientas poderosas para el monitoreo de redes como: Nagios y Cacti.

(3) Es una aplicación de gestión multiplataforma, muy importante para el tipo de infraestructuras de red que existen hoy en día.

(4) Utiliza una tecnología de gestión de red sin agentes, esto facilita la instalación de la aplicación, permite la escalabilidad y actualización de los equipos de red sin ningún trabajo extra.

(5) Existe amplia información y soporte.

(6) Versatilidad para crear scripts escritos por el propio administrador, para desarrollar una gestión de red a medida.

(7) Seguridad, la capacidad de monitorear de forma segura a través de vario niveles protegidos por contraseñas.

Las desventajas:

(1) Al no utilizar tecnología con agentes en los clientes, requiere una configuración previa en su instalación del protocolo SNMP en cada uno de las máquinas a monitorizar siguiendo un procedimiento distinto según la versión o tipo de sistema operativo.

(2) Necesita la instalación de paquetes adicionales ZenPacks para monitorización de servicios básicos como HTTP o FTP, información del sistema operativo y algunos recursos hardware como obtener información de la CPU. Con lo cual, la instalación puede no llegar a ser suficiente, y necesita una puesta a punto para cumplir funcionalidades básicas.

(3) La instalación de la herramienta en el equipo host es rápida, pero no cada configuración del cliente desde la consola web. Por ejemplo, hay que asignarle una plantilla o template adecuada o personalizada para que monitorice lo que necesitamos de dicho dispositivo.

(4) Necesita de la aplicación externa VMplayer para funcionar en sistemas operativos de Microsoft Windows.

3.8. ESTUDIO DE LAS SOLUCIONES A LOS REQUERIMIENTOS CON EL SISTEMA SELECCIONADO.

Los requerimientos básicamente dependerán de cada entorno de red y su infraestructura. En esta sección se hace una simple enumeración de los puntos principales del mismo para establecer una mínima información de contexto.

En general los requerimientos recomendados por los creadores de la herramienta, para un entorno de red conformado hasta por 250 nodos o dispositivos, un servidor de con una memoria de mínimo 4 GB en RAM, con un procesador de 4 núcleos y un disco duro con una capacidad de almacenamiento de 300GB.

En cuanto al software necesario tenemos:

- Oracle Java.
- RRDTools.
- MySQL.

Los puertos que deberían habilitarse en el cortafuegos.

PUERTO	PROTOCOLO	DESCRIPCIÓN
11211	TCP/UDP	memcached
8080	TCP	Interface WEB
514	UDP	Syslog
162	UDP	SNMP traps
25	TCP	Zenmail

En cuanto a los host de la red, sabemos que la herramienta es multiplataforma.

CAPITULO 4. INSTALACIÓN Y PRUEBAS DE FUNCIONAMIENTO – DEMO.

4.1. INTRODUCCIÓN.

En ésta sección se realizaran los trabajos de instalación y configuración de la aplicación de monitoreo ZENOSS, para ello vamos a necesitar: Centos, VMWare Player.

CENTOS.

El Community ENTerprise Operating System, también conocido como CentOS, es una alternativa libre a los caros sistemas empresariales proporcionados por empresas como Red Hat, SUSE y Mandriva.

Un sistema operativo para la empresa no está diseñado para el usuario que busca “lo último de lo último” en software, con gráficos espectaculares, los últimos kernels, montones de juegos y otras características superfluas. Muchas distribuciones GNU/Linux cubren la demanda de “lo último de lo último”. Estas distribuciones se lanzan cada 6 meses más o menos, y normalmente requieren un trabajo constante de actualización debido a que el soporte va desapareciendo gradualmente con cada versión nueva que aparece. Estas distribuciones con “lo último de lo último” tienen generalmente un ciclo de lanzamiento de 6 meses y un ciclo de soporte de entre 12 y 18 meses.

Los sistemas operativos empresariales normalmente tienen un precio elevado, y su coste económico puede ser importante. Muchos de ellos, con un año de actualizaciones y soporte telefónico, pueden costar entre 300 y 2.500 dólares por año y servidor. Los planes más caros tienen sus ventajas, como tiempos de respuesta menores y más horas de soporte telefónico. La aparición de los sistemas operativos empresariales dio al usuario otra opción. Éstos podían ahora elegir entre:

1. Una distribución GNU/Linux convencional, gratuita (o de bajo coste), con ciclos de lanzamiento y soporte cortos.

2. Un sistema operativo empresarial de elevado precio, con ciclos de lanzamiento y soporte largos.

CentOS es un proyecto de mayor envergadura y más elaborado que la mayoría de los demás proyectos recompilados. El equipo de CentOS tiene 11 desarrolladores y su trabajo está disponible desde más de 70 mirrors por todo el mundo. CentOS se encuentra disponible en tres distribuciones principales: CentO-3, CentO-4 y CentOS-5, CentOS-6. Soporta las arquitecturas x86, x86_64, S390, S390x, IA64, sparc, ppc, ppc64 y alpha. (La mayoría de sus rivales soporta sólo x86 y x86_64).

Este enorme trabajo de los desarrolladores de todo el mundo ha hecho de CentOS un sistema operativo completamente funcional que ocupa un hueco muy importante en el panorama Linux. En la última encuesta de netcraft.com se estima que CentOS se ejecuta en cerca de 100.000 servidores Web. Esto lo sitúa dentro de las 8 distribuciones GNU/ Linux con más servidores Web desplegado. Además, es la única distribución empresarial gratuita de la encuesta. CENTOS está dentro del top 20 en el ranking de distribuciones GNU/Linux y BSD, la posición más alta de un proyecto recompilado empresarial.

Se puede usar CENTOS para cualquiera de las tareas que, de otra manera, se tendría que asignar a soluciones empresariales comerciales. CENTOS puede reemplazar a los servidores comerciales existentes en el mercado. El selecto software de CentOS hace de esta la herramienta perfecta para las aplicaciones de servidor. Podemos usar CentOS como servidor Web, servidor de correo, servidor de bases de datos o servidor de aplicaciones. CentOS incorpora todas las sofisticadas funcionalidades de compatibilidad con Windows incluidas en Red Hat Enterprise Linux. Se puede usar CentOS como controlador de dominios primarios o secundarios, o como servidor de clientes Windows basado en Samba y SMB. CentOS es también un sistema de escritorio Linux plenamente funcional. Se pueden encontrar la mayoría de las herramientas de escritorio más populares, como OpenOffice.org 1.1.2, Mozilla 1.7.12, Firefox 1.0.7, Evolution 2.0.2, Gaim 1.3.1-0.el4.3, X-chat 2.4.0, Konqueror 3.3.

Ya sea trabajando en un servidor empresarial, en un servidor para la oficina o incluso en un sistema común de escritorio, se encontrará en CentOS una distribución estable, de alto rendimiento, fácil de administrar y de utilizar.

VMWARE PLAYER

VMware Player es un programa de virtualización gratuito de VMware, que es la forma más fácil de ejecutar múltiples sistemas operativos al mismo tiempo en su PC. Con su interfaz fácil de usar, VMware Player lo hace sin esfuerzo para que cualquier persona pueda probar cualquier sistema operativo sin tener que poner en riesgo tu información o tus archivos tratando de particionar tu disco y hacer dual boot.

La plataforma de virtualización de VMware se basa en una arquitectura preparada para la empresa. Puede utilizar un software para transformar o “virtualizar” los recursos de hardware de un ordenador, incluidos CPU, RAM, disco duro y controlador de red, con el fin de crear una máquina virtual completamente funcional que puede ejecutar su propio sistema operativo y aplicaciones de la misma forma que lo hace un ordenador “real”.

Cada máquina virtual contiene un sistema completo, con lo que se eliminan los posibles conflictos. La virtualización de VMware inserta directamente una capa ligera de software en el hardware del ordenador o en el sistema operativo host. Contiene un monitor de máquina virtual o “hipervisor” que asigna los recursos de hardware de manera dinámica y transparente. Varios sistemas operativos se ejecutan de manera simultánea en el mismo ordenador físico y comparten recursos de hardware entre sí. Al encapsular la máquina entera (incluida la CPU, la memoria, el sistema operativo y los dispositivos de red), una máquina virtual es totalmente compatible con los sistemas operativos, las aplicaciones y los controladores de dispositivos estándar. Puede ejecutar con toda seguridad varios sistemas operativos y aplicaciones al mismo tiempo en un solo ordenador; cada uno de ellos tendrá acceso a los recursos que necesite cuando los necesite.

VMware ha introducido los primeros productos de virtualización comercializados de forma gratuita para usuarios sin experiencia en virtualización. En junio de 2006, VMware ha presentado VMware Infrastructure 3, el primer paquete completo de virtualización de infraestructuras del sector que ofrece amplias capacidades de virtualización, gestión, optimización de recursos, disponibilidad de aplicaciones y automatización operativa en una oferta integrada.

Virtualizar permite reducir los costes de tecnologías informáticas y aumentar la eficacia, el uso y la flexibilidad de los activos existentes. En todo el mundo, organizaciones de todos los tamaños se benefician de la virtualización de VMware. Miles de organizaciones utilizan soluciones de virtualización de VMware. La arquitectura de infraestructura virtual de VMware permite a las empresas reducir los costes gracias al aumento de la eficiencia, la flexibilidad y la capacidad de respuesta. La gestión de una infraestructura virtual permite a la tecnología de la información conectar y gestionar rápidamente los recursos en función de las necesidades de la empresa.

La infraestructura virtual permite a las organizaciones de IT lograr lo siguiente:

- Índices de utilización del 60 al 80% para servidores x86, frente al 5 a 15% actual.
- Suministrar nuevas aplicaciones en décimas de segundos, no en días.
- Medir los tiempos de respuesta a solicitudes de cambio en minutos.
- Realizar el mantenimiento del hardware sin pérdida de servicio y sin esperar a las ventanas de mantenimiento.

4.2. CARACTERÍSTICAS.

Zenoss es un producto único que ofrece un servicio en el mundo real, híbrido que abarca la infraestructura física, virtual y cloud-based.

Las funciones clave que conforman los servicios de Zenoss incluyen:

- Gestión de Eventos.
- Análisis y optimización.
- Gestión de Recursos.

Gestión de eventos.

Las empresas y los proveedores de servicio y las necesidades de una nueva clase de solución de tecnología de información, han convertido en operaciones que ofrece escalable, automatizado y en tiempo real garantía de servicio y análisis de todo el

entorno de cloud híbrido completo. Las operaciones deben ir más allá de las estadísticas de dispositivo de nivel de tiempo de actividad y la disponibilidad general y ser capaz de responder a las preguntas e inquietudes formuladas por los administradores de red.

Con Zenoss, las operaciones de gestión de red son cada vez mayores por la aparición de dispositivos físicos y virtuales (como los servicios en lugar de puntos de datos individuales). En escala, la gestión del nivel de servicio es uno de los mayores retos que tiene planteados. Zenoss elimina las conjeturas de saber cuándo un evento en la infraestructura de red, como un fallo del disco, pone los servicios críticos en riesgo y permite una respuesta proactiva ante los usuarios del servicio y los clientes se vean afectados en el entorno.

Análisis y optimización.

Un factor crítico de éxito para operar una infraestructura de red dinámica a gran escala es la capacidad de tomar decisiones de planificación a corto y largo plazo. Nube operadores se están dando cuenta que hay un sin fin de preguntas para resolver.

- ¿Mis servicios que satisfagan las necesidades de mis clientes? Si no, ¿dónde está el problema?
- ¿Es esta una tendencia que tengo que dirigirme?
- ¿Es este cliente como otros clientes?
- ¿Cómo puedo ser más eficiente?
- ¿Cuándo tengo que comprar más hardware, y dónde puedo exprimir más la utilización?

Con Zenoss, los operadores de infraestructuras de nube se puede obtener acceso a una capacidad unificada, análisis avanzados que ofrece una visión inmediata de las tendencias de uso en todas las capas de la infraestructura de red y su entorno, incluidos dispositivos de almacenamiento, servidores, máquinas virtuales,

aplicaciones y servicios cloud. Esta idea es fundamental, ya que permite a los administradores de red determinar las tendencias del consumo, la utilización de optimizar la infraestructura de red, las necesidades de capacidad de pronóstico y cobran por sus servicios.

Zenoss aprovecha el modelo de relación unificada del entorno de red completo. Esta basado en objetos y es un poderoso modelo de gestión con el cual se construirán y mantendrá de forma automática toda la información acerca de la gestión de la red, Zenoss para analizar e informar sobre todos los dispositivos en el entorno de red y sus relaciones como por ejemplo: redes, servidores, dispositivos virtuales, software y aplicaciones, dispositivos personalizados, UPS y sensores de temperatura.

Gestión de recursos.

En el corazón de Zenoss es un modelo unificado del entorno de red completo. Zenoss se basa en un modelo de gestión de gran alcance basado en objetos que se construye y se mantiene de forma automática. Todos los dispositivos en el entorno.

4.3. SISTEMA DE GESTIÓN Y MONITOREO.

4.3.1. REQUERIMIENTOS DEL ORDENADOR.

Los requisitos mínimos recomendados, teniendo en cuenta los efectos de un servidor, deberían permitir la instalación de: Un sistema operativo anfitrión, un software de virtualización, un gestor de red.

- Procesador con arquitectura de 64 bits.
- Memoria RAM 2GB.
- Disco duro 20 GB.
- Tarjeta gráfica y monitor capaz de soportar una resolución de 1027x768.
- Lector de DVD.
- Puerto USB.

- Conexión a internet.

4.3.2. INSTALACIÓN DEL SOFTWARE.

En las secciones anteriores se ha dado una explicación amplia del software que usaremos para instalar la aplicación de gestión de red ZENOSS.

Cómo instalar VMWare PLAYER.

Para empezar con la instalación partiremos del hecho que el sistema operativo anfitrión ya fue previamente instalado y configurado, en el caso de el presente trabajo de investigación se uso UBUNTU en su versión 12,04 por su versatilidad y de fácil instalación y su compatibilidad con la mayoría de periféricos existentes en el mercado.

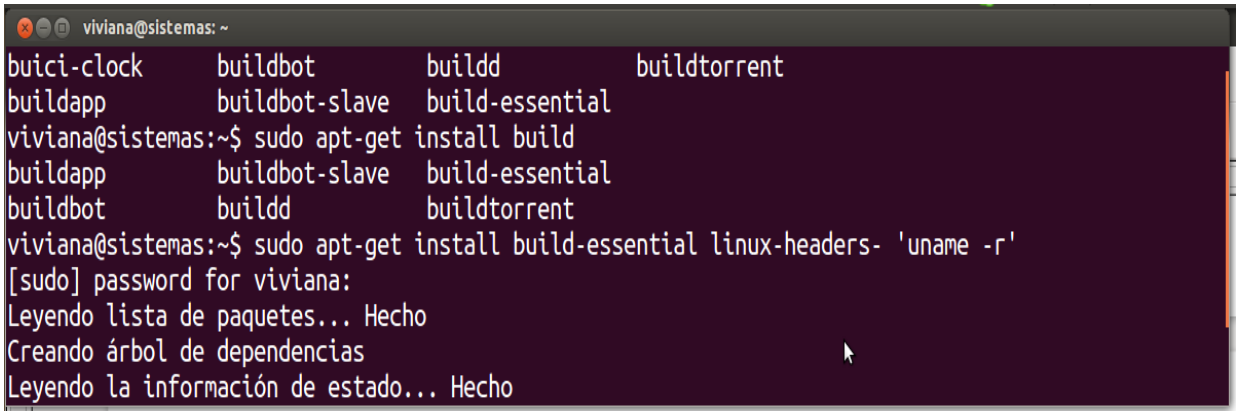
1.- Como primer paso se deben descargar los instaladores de la página oficial.



Figura 4.1. Descargando VMWARE PLAYER.

Escogemos la opción Vmware-Player-5.0.1-894247.bundle, descargamos y guardamos los instaladores.

2.- Abrimos un terminal actualizamos el repositorio y descargamos los header del kernel, para ello abrir un terminal y digitar los siguientes comandos:



3.- Moverse al directorio donde se encuentra los ejecutables y digitar

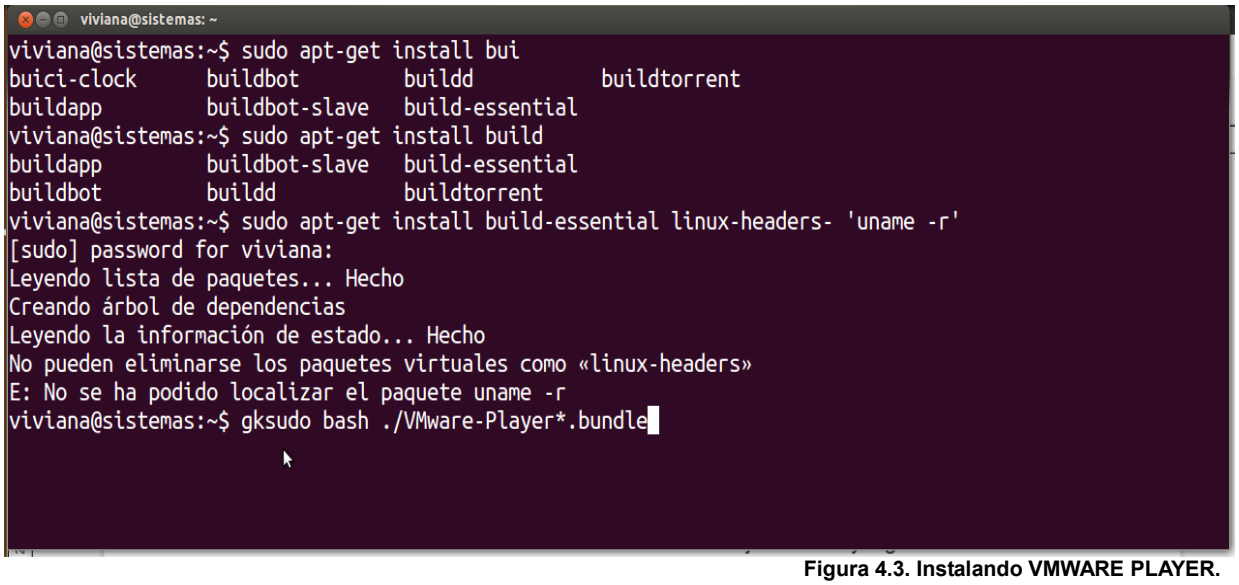


Figura 4.3. Instalando VMWARE PLAYER.

Con ello estaría finalizada la instalación de VMware Player.

4.- Una vez instalado el VMware Player procedemos a crear una máquina virtual para instalar el software de gestión de red.

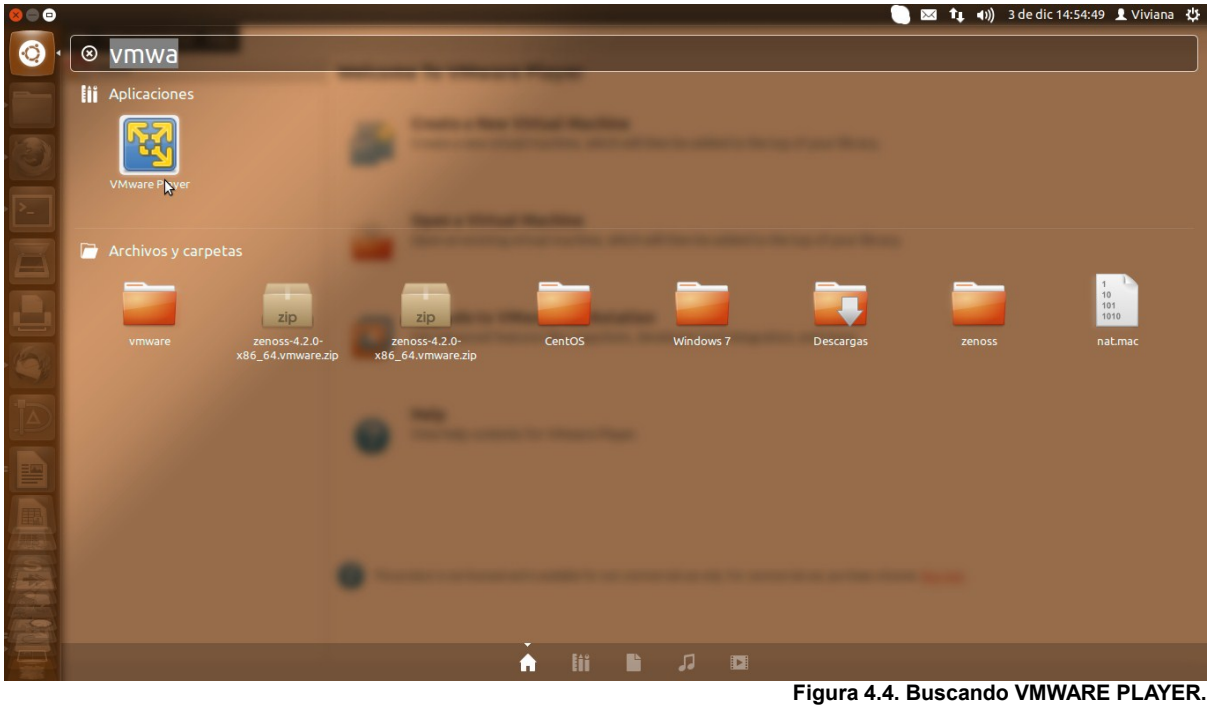


Figura 4.4. Buscando VMWARE PLAYER.

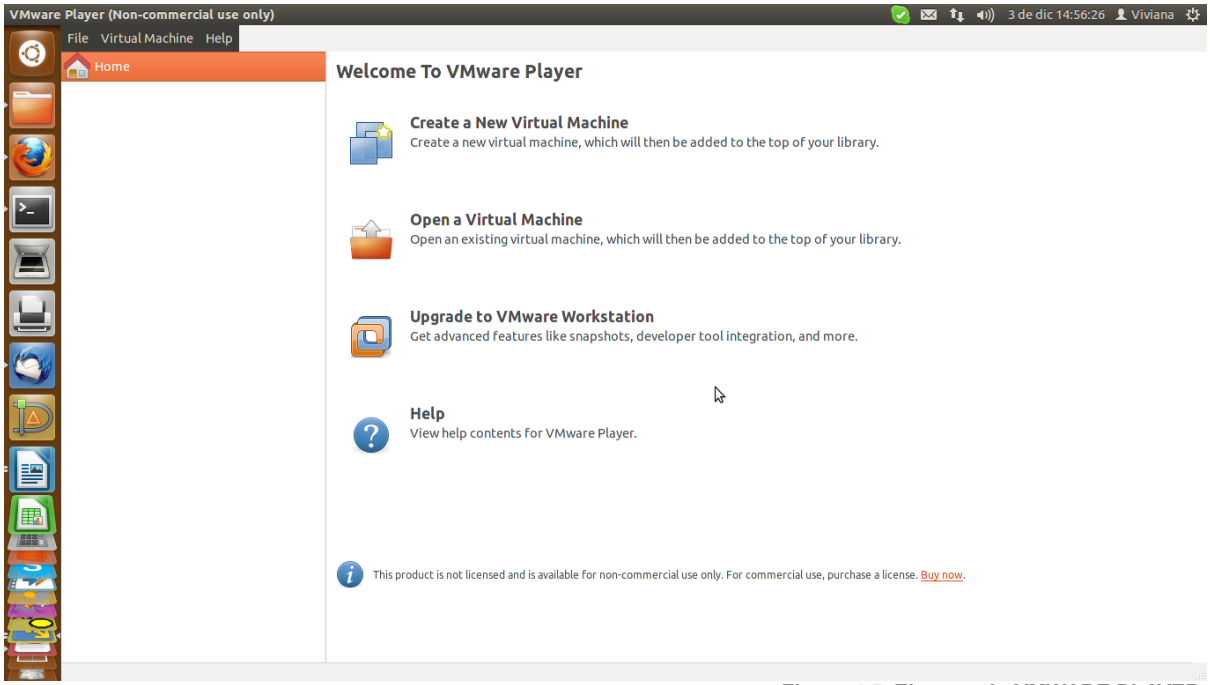


Figura 4.5. Ejecutando VMWARE PLAYER.

5.- Procedemos a crear la máquina virtual donde se instala ZENOSS.

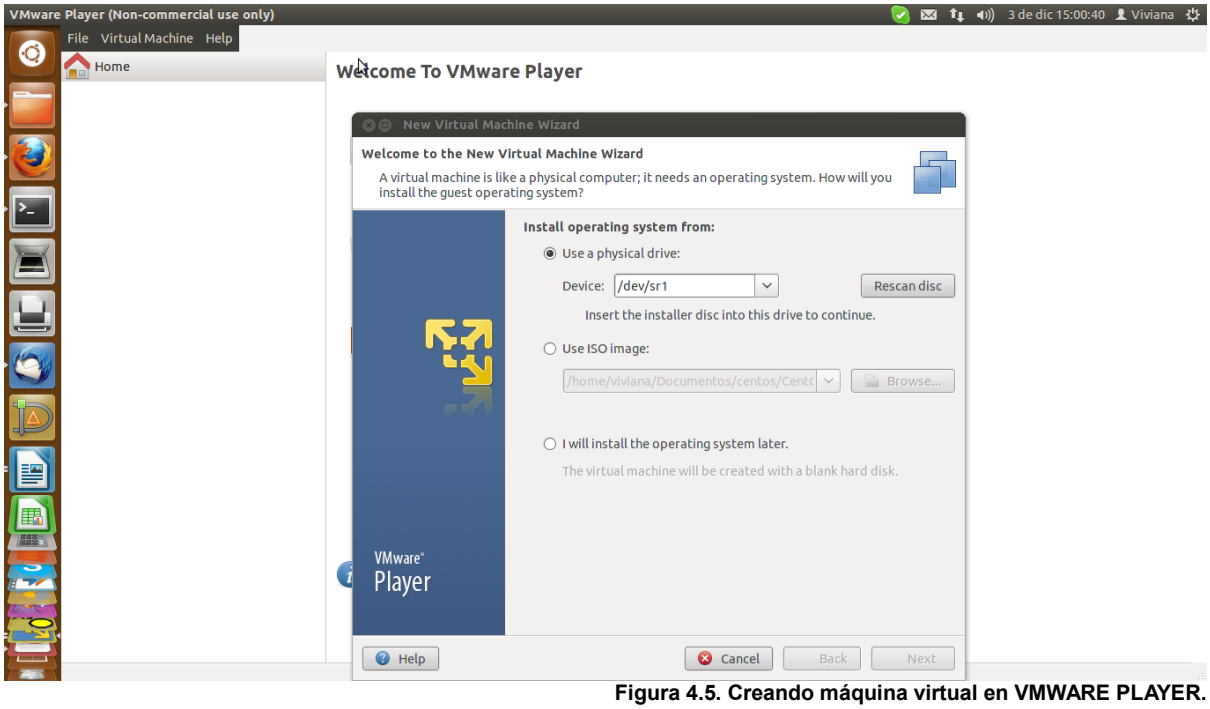


Figura 4.5. Creando máquina virtual en VMWARE PLAYER.

6.- En éste punto debemos tener a la mano los instaladores de Zenoss para continuar con la creación de la máquina virtual, a continuación explicamos cómo hacerlo.

Abrimos el sitio WEB sourceforget.net y buscamos Zenoss:

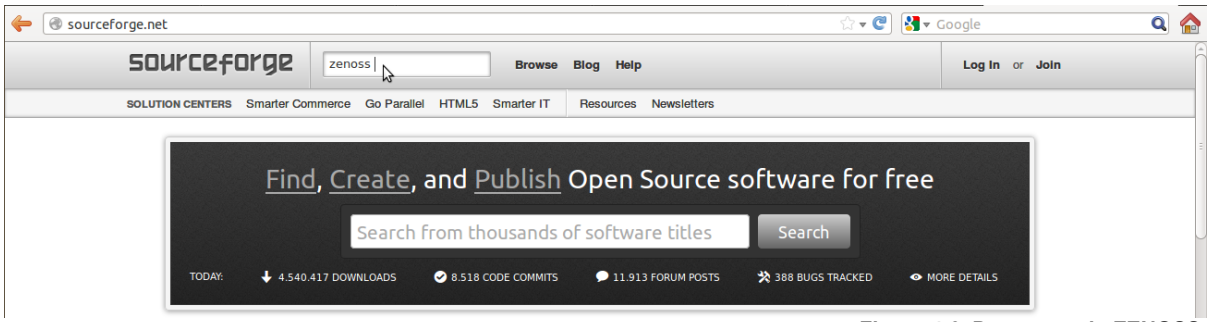


Figura 4.6. Descargando ZENOSS.

6.- De el siguiente listado escogemos la opción zenoss-4.2.0-x86_64.vmware.zip.

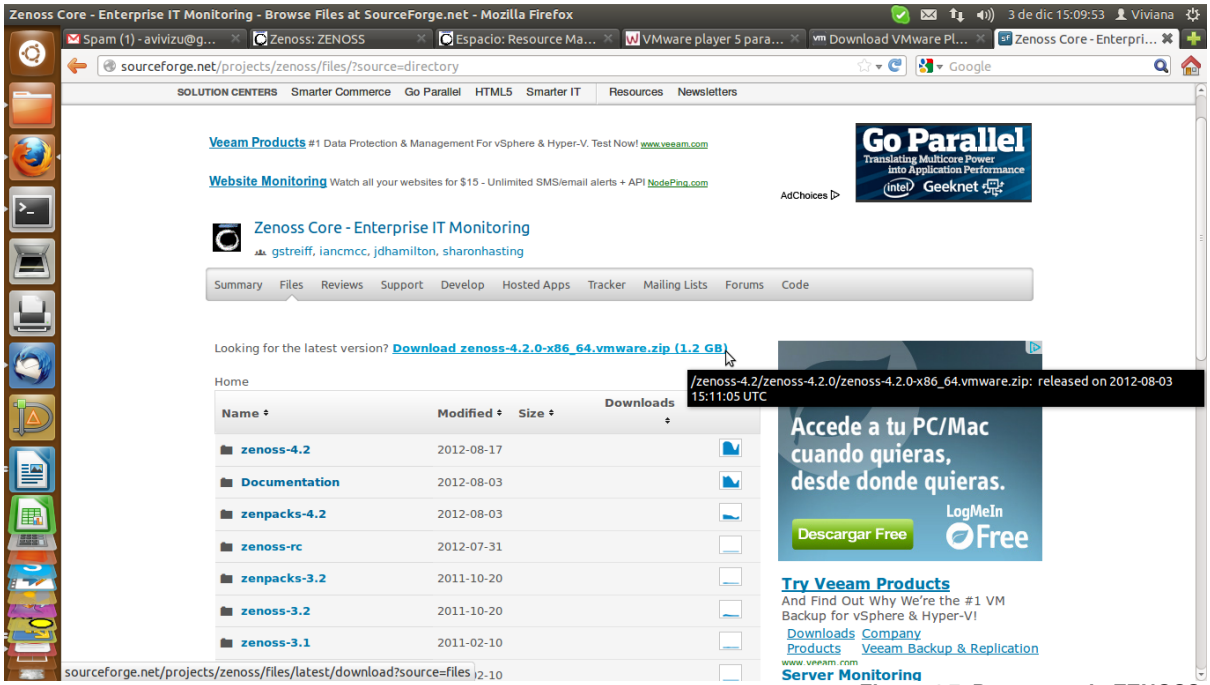


Figura 4.7. Descargando ZENOSS.

7.- Luego de descargar el archivo anterior buscamos en la ubicación adecuado y continuamos con la creación de la máquina virtual.

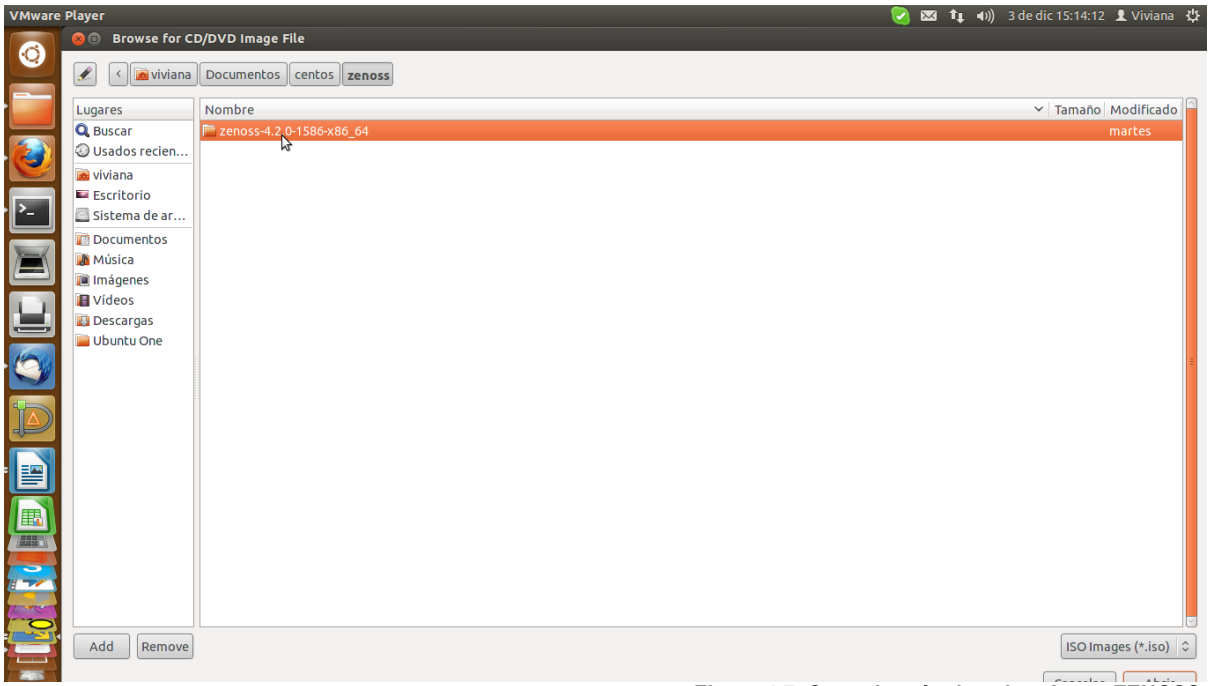


Figura 4.7. Creando máquina virtual para ZENOSS.

8.- En éste punto únicamente hay que abrir la máquina virtual de Zenoss del archivo desempaquetado.

9.- Ejecutamos la máquina virtual seleccionada en el paso anterior.

10.- A partir de aquí se instalará la máquina virtual con la aplicación de gestión de red ZENOSS "embebida" en un sistema operativo CENTOS 5.4 con todos los servicios y plugins listos para empezar el monitoreo y gestión de una infraestructura de red.

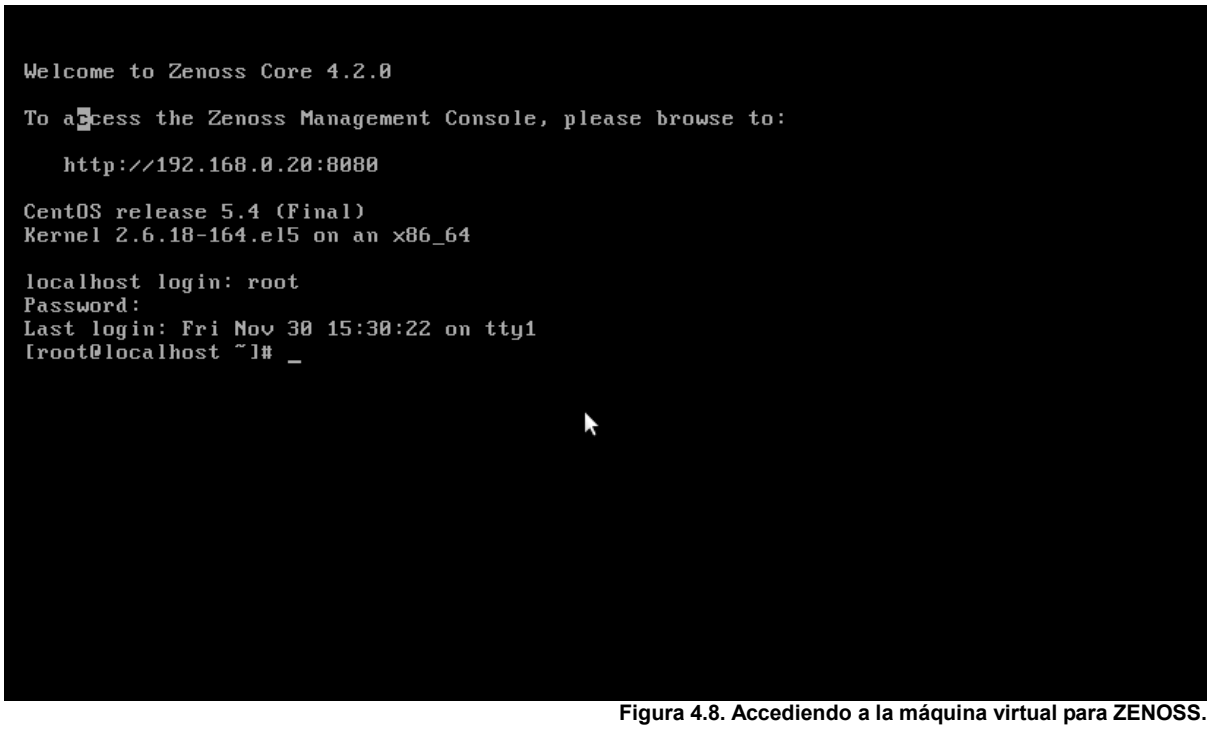


Figura 4.8. Accediendo a la máquina virtual para ZENOSS.

11.- Acceder al sistema operativo.

Para acceder al sistema operativo de la máquina virtual CENTOS se deben usar:

Usuario: root.

Contraseña: zenoss.

Como se explicó en capítulos anteriores ésta herramienta es totalmente administrable vía web, al término de la instalación nos arrojará los parámetros de conexión, en éste caso es: http://192.168.0.20:8080.

En resumen la instalación se resume a:

Previamente se requiere tener preparado el sistema operativo anfitrión de VMWare PLAYER.

1.- Como primer paso se deben descargar los instaladores de la página oficial VMWare PLAYER.

2.- Instalar VMWare PLAYER.

3.- Crear una máquina virtual.

4.- Instalar el servidor de ZENOSS en la máquina virtual.

5.- Acceder a la aplicación de gestión vía web con esta aplicación http://192.168.0.20:8080.

4.3.3. CONFIGURACIÓN.

La configuración de la herramienta es totalmente intuitiva ya que tiene una interfaz muy amigable.

Como primer paso hay que configurar el agente SNMP en uno de los clientes a ser gestionados por ZENOSS.

4.3.3.1. CONFIGURACIÓN BÁSICA.

Configuración del agente SNMP en un sistema operativo Windows.

A continuación detallaremos los pasos a seguir para configurar de manera adecuada el agente en uno de los clientes de la infraestructura de red para el caso en que el cliente tenga como sistema operativo Windows.

1.- Primero hay que verificar que el agente esté instalado en el sistema operativo, para ello iremos al panel de control, y verificamos en componentes del sistema que el servicio esté instalado como se ve en la siguiente figura.

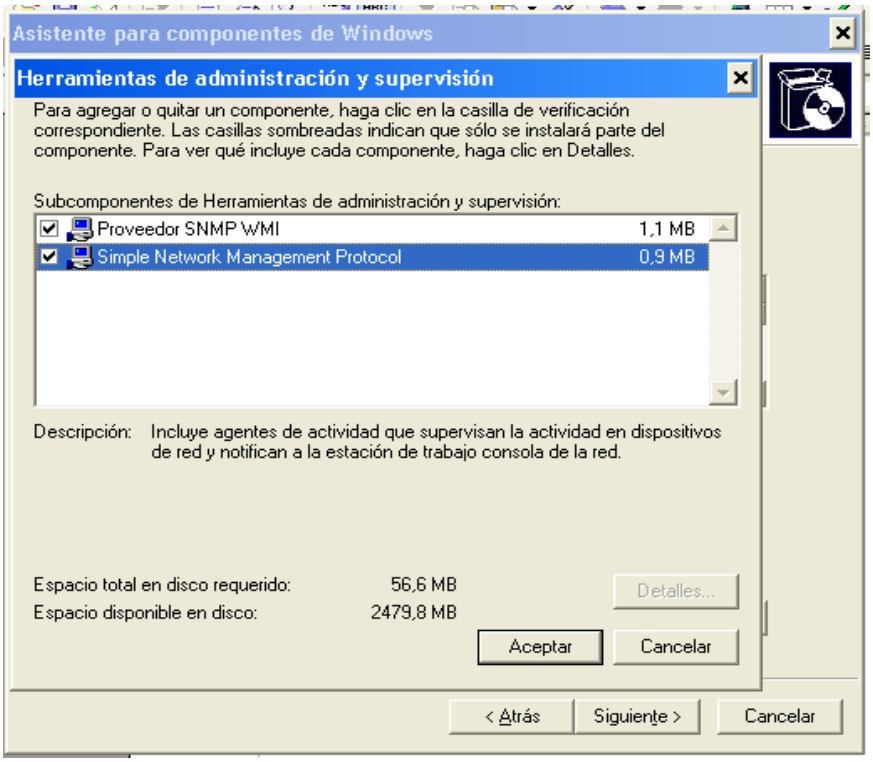


Figura 4.9-1. Instalando agente SNMP - WINDOWS

2.- Si el agente no está instalado debe instalarse para el efecto el sistema operativo pedirá el disco del sistema.

Una vez instalado chequeamos que las dependencias estén correctamente activadas.

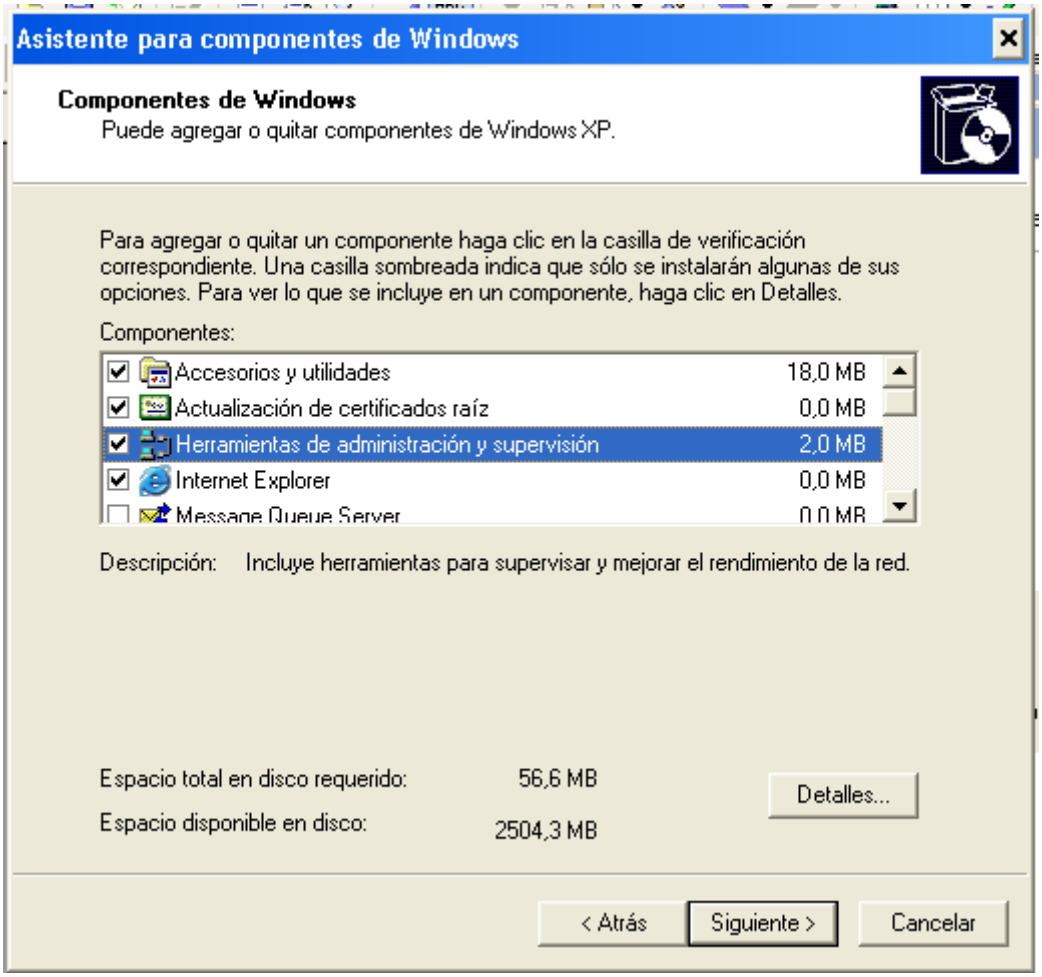


Figura 4.9-2. Instalando agente SNMP - WINDOWS

3.- El siguiente paso es configurar el agente, para ello nos vamos a mi PC y con clic derecho escoger la opción de Administración, con lo que se despliega la siguiente pantalla.

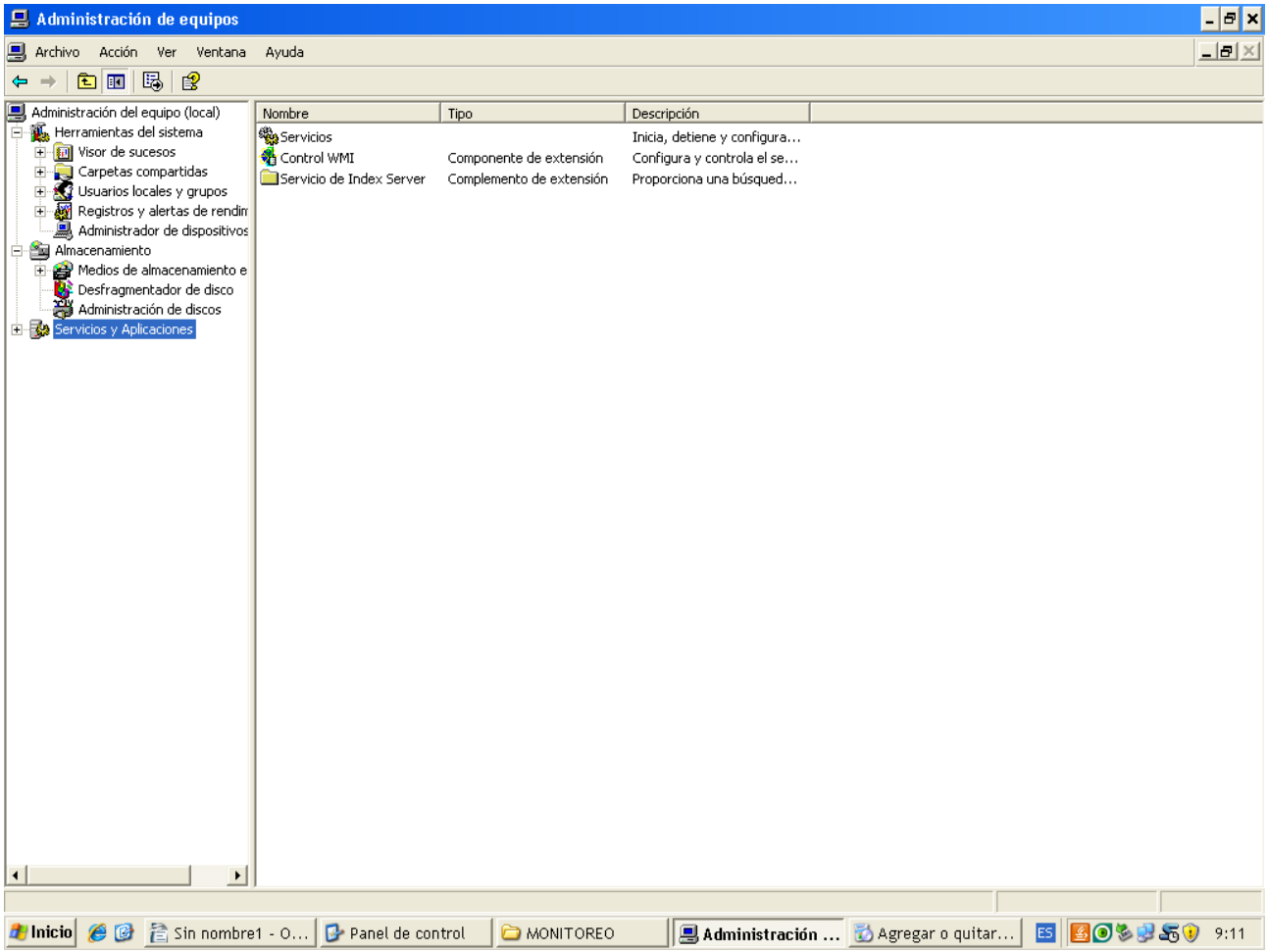


Figura 4.10-1. Configurando agente SNMP - WINDOWS

Nos vamos a la sección de servicios y aplicaciones, a continuación ingresamos a la pestaña del servicio SNMP accediendo con doble clic, tal como se ve en la siguiente figura.

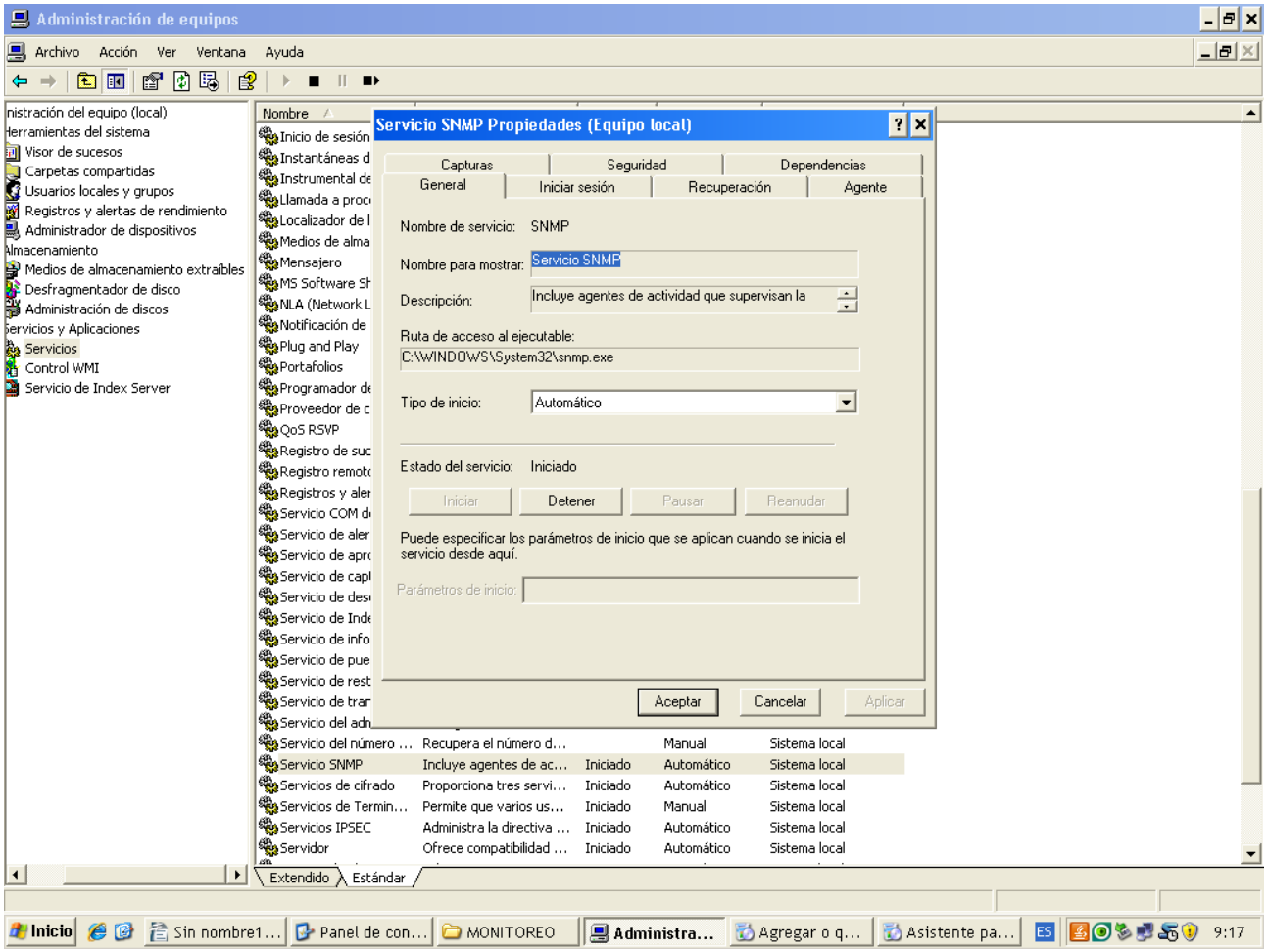


Figura 4.10-2. Configurando agente SNMP - WINDOWS

En la pestaña general se debe configurar para que el servicio inicie de forma automática, luego en la pestaña de seguridad, configurar el nombre de la comunidad y los atributos de la comunidad, es decir:



Figura 4.10-3. Configurando agente SNMP - WINDOWS

Nombres de comunidad aceptados: public.

Derechos: solo lectura.

En la misma ventana, nos dirigimos a la siguiente sección y activamos la opción: aceptar paquetes SNMP de cualquier HOST, la configuración debe quedar como se muestra en la siguiente figura:

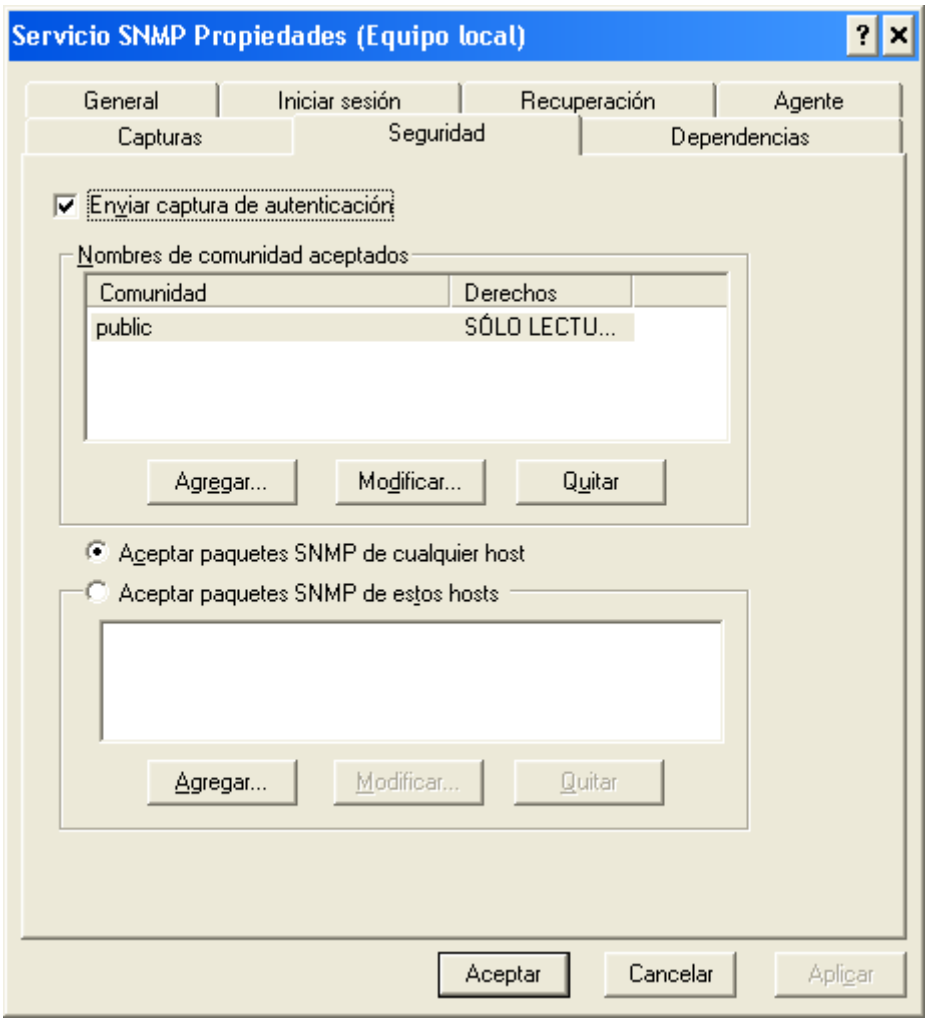


Figura 4.10-4. Configurando agente SNMP - WINDOWS

Lo siguiente es la configuración del agente. Nos dirigimos a la pestaña “agente” y en la sección de servicio activamos todas las casillas esto es: Físico, Aplicaciones, Vínculo de datos y subred, Internet, De un extremo a otro.

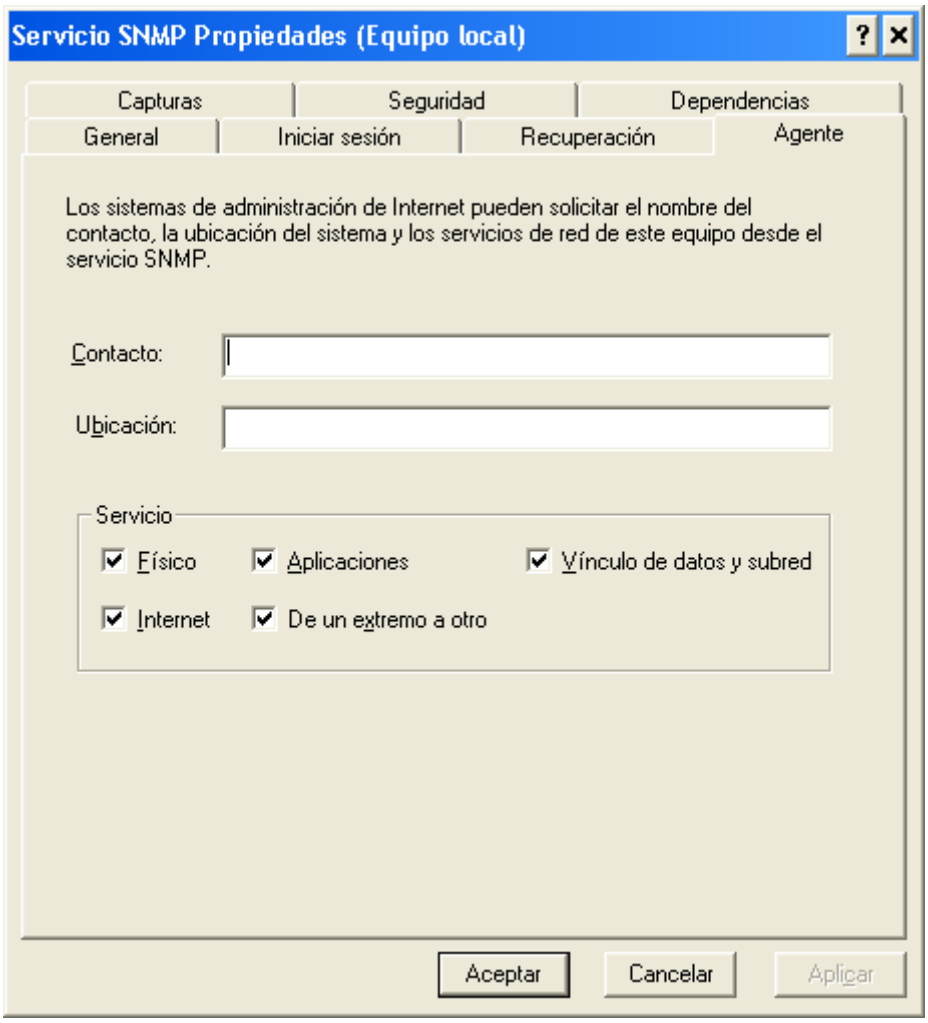


Figura 4.10-5. Configurando agente SNMP - WINDOWS

Configuración del agente SNMP en un sistema operativo Linux.

A continuación detallaremos los pasos a seguir para configurar de manera adecuada el agente en uno de los clientes de la infraestructura de red para el caso en que el cliente tenga como sistema operativo Linux.

1.- Como primer paso hay que instalar el agente, abrimos una ventana de comandos y procedemos a instalar.

$ sudo apt-get install snmp snmpd

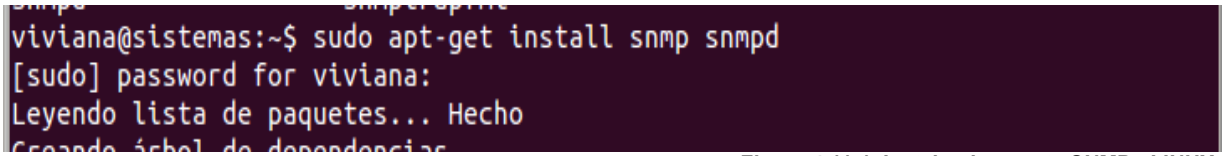


Figura 4.11-1. Instalando agente SNMP - LINUX

Esto nos creará los archivos de configuración en la ruta /etc/snmp/

2.- Modificar el archivo de configuración del agente, y con esto poder enviar la información y/o capturas del agente al gestor.

Lo primero es parar el servicio.

$ sudo /etc/init.d/snmpd stop

Luego en el terminal digitar:

$ cd /etc/snmp

$ sudo gedit snmpd.conf



Figura 4.11-2. Instalando agente SNMP – LINUX

3.- El archivo de configuración está dividido en tres partes.

En la primera se debe dejar el archivo configurado de tal manera en que el agente escuche por todas las interfaces de la máquina y no únicamente por la de loopback.

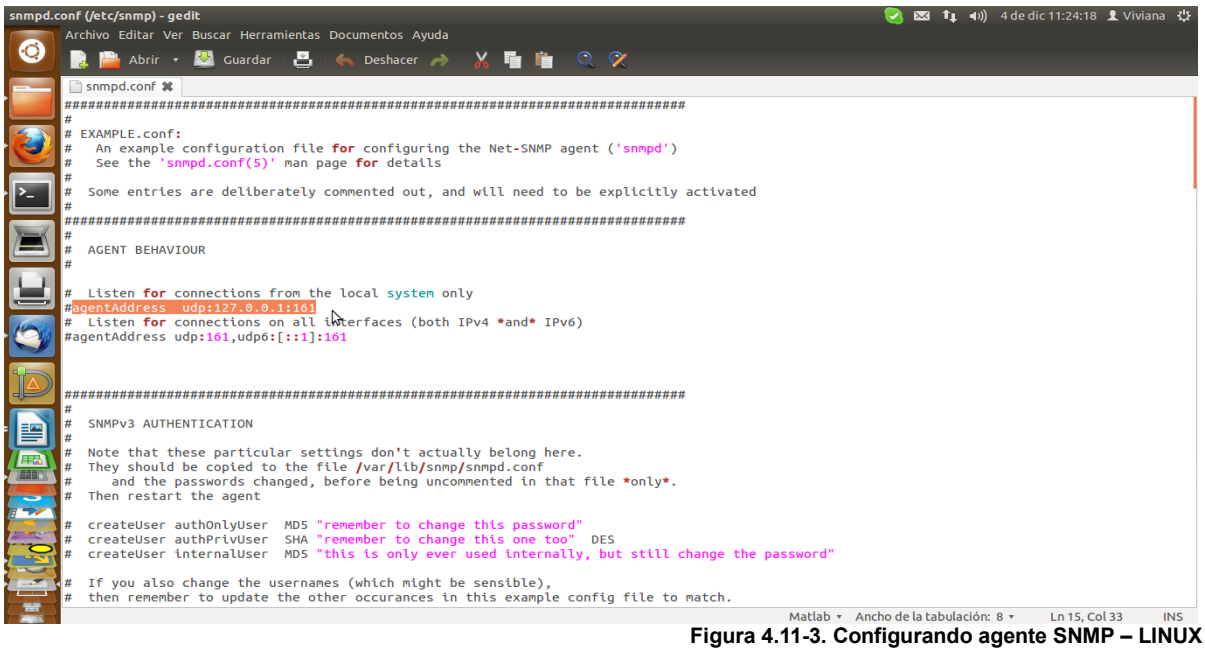


Figura 4.11-3. Configurando agente SNMP – LINUX

En la segunda parte hay que crear la comunidad y el entorno de red.

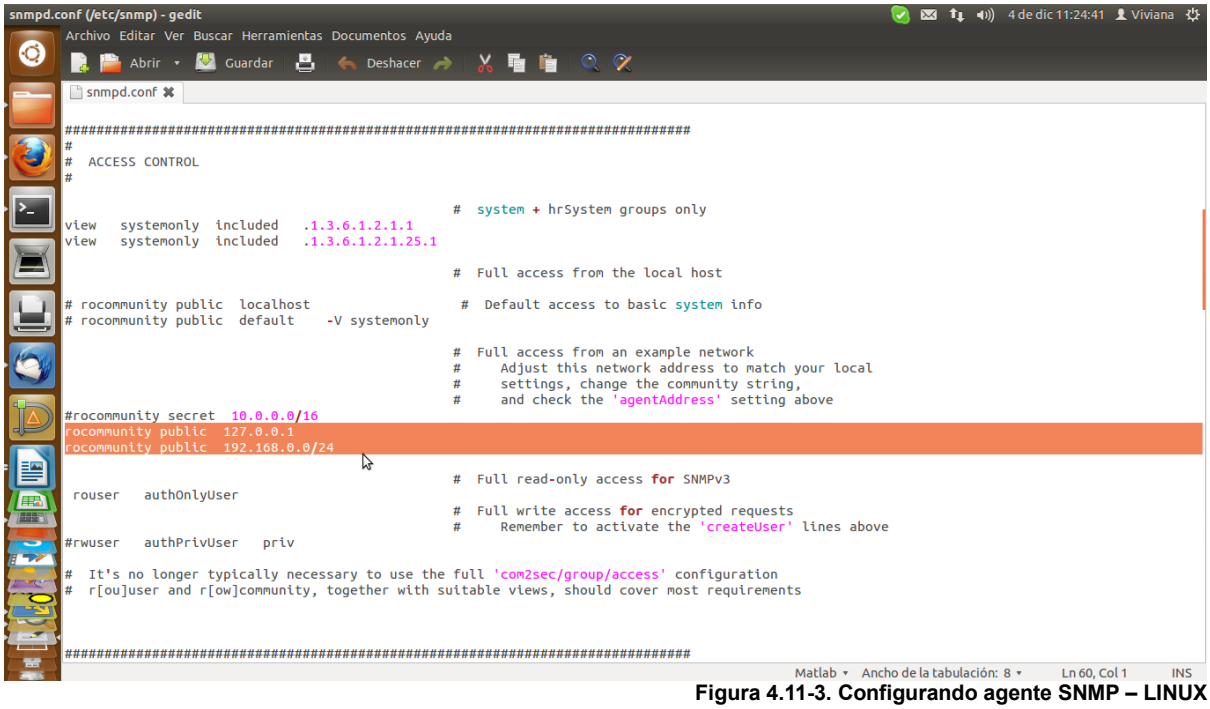


Figura 4.11-3. Configurando agente SNMP – LINUX

En la tercera parte hay que activar el monitoreo con la versión de protocolo.

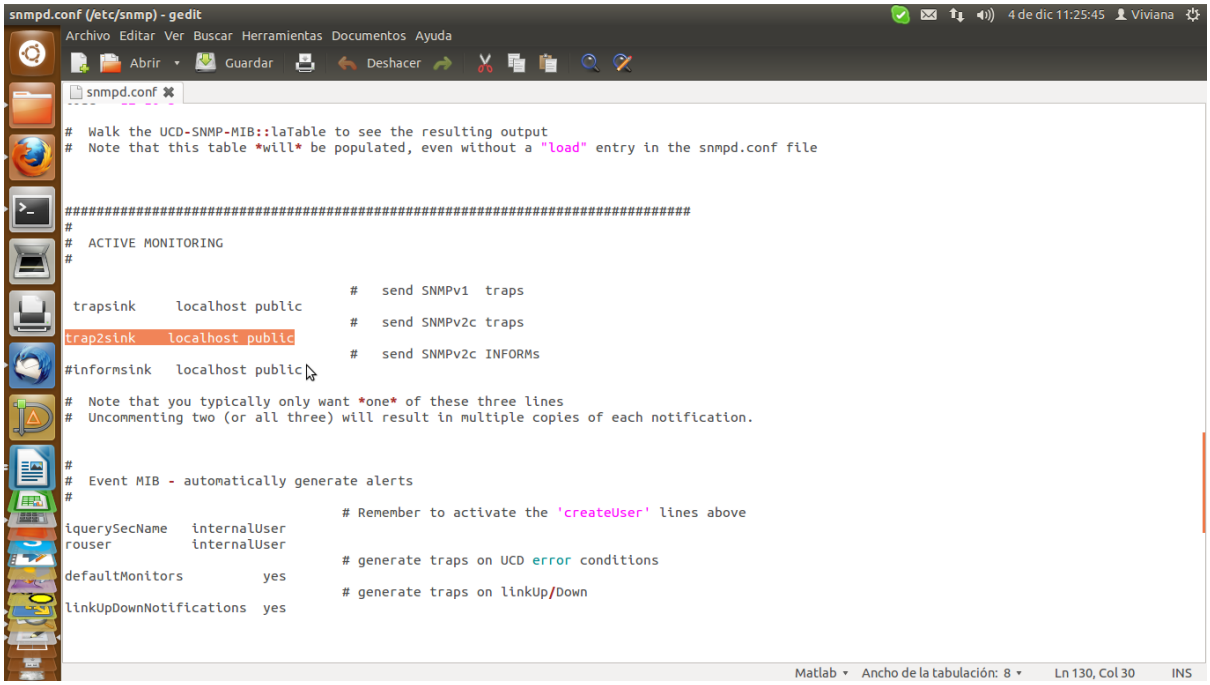


Figura 4.11-4. Configurando agente SNMP – LINUX

Guardamos el archivo y reiniciamos el servicio.



Figura 4.11-5. Configurando agente SNMP – LINUX

Con ello la configuración en linux está terminada.

4.3.3.2. CONFIGURACIÓN ESPECÍFICA.

La configuración específica en lo que tiene que ver a la aplicación de monitoreo empieza por especificar los parámetros de red en el sistema base de ZENOSS, a continuación detallamos los pasos a seguir.

1.- En la consola de administración de máquinas virtuales accedemos al sistema CENTOS como se ve en la siguiente pantalla, el usuario es root, y la contraseña es zenoss.

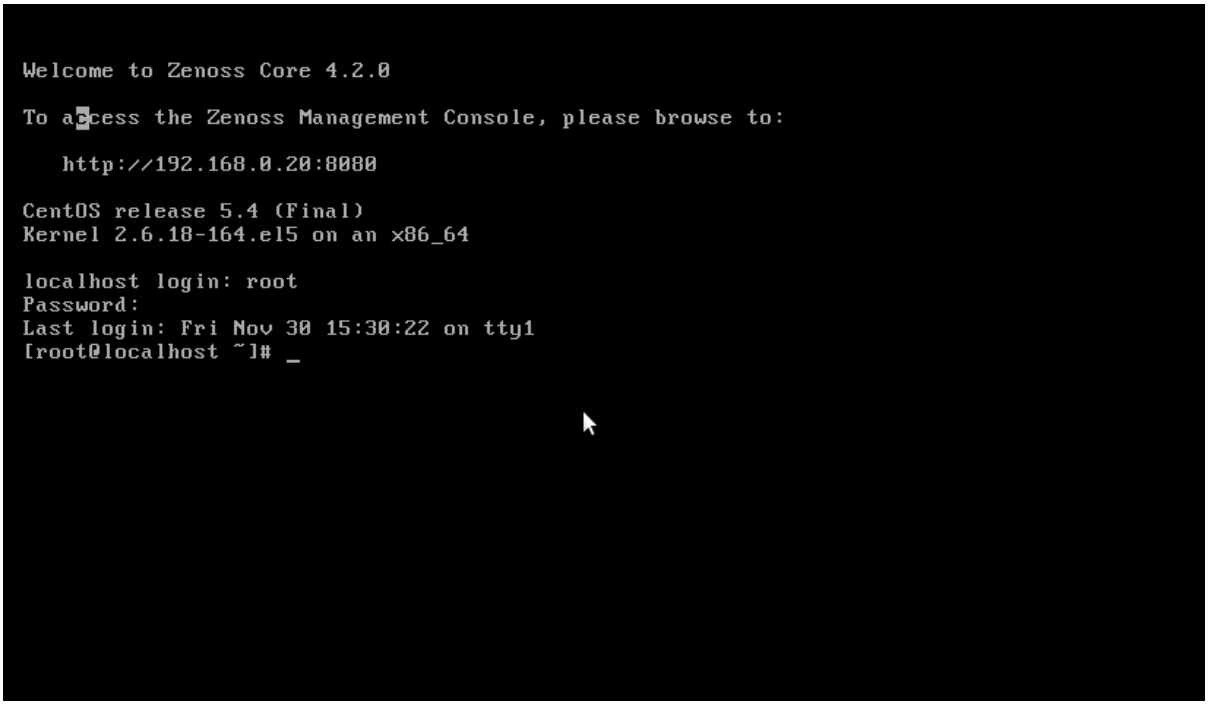


Figura 4.11-5. Configuraciones de red – CENTOS

Una vez en el sistema nos dirigimos a /etc/sysconfig/network-scripts/, debe modificarse con cualquier editor de textos, y configurar los parámetros de red de acuerdo al entorno que se va a monitorear con ZENOSS.

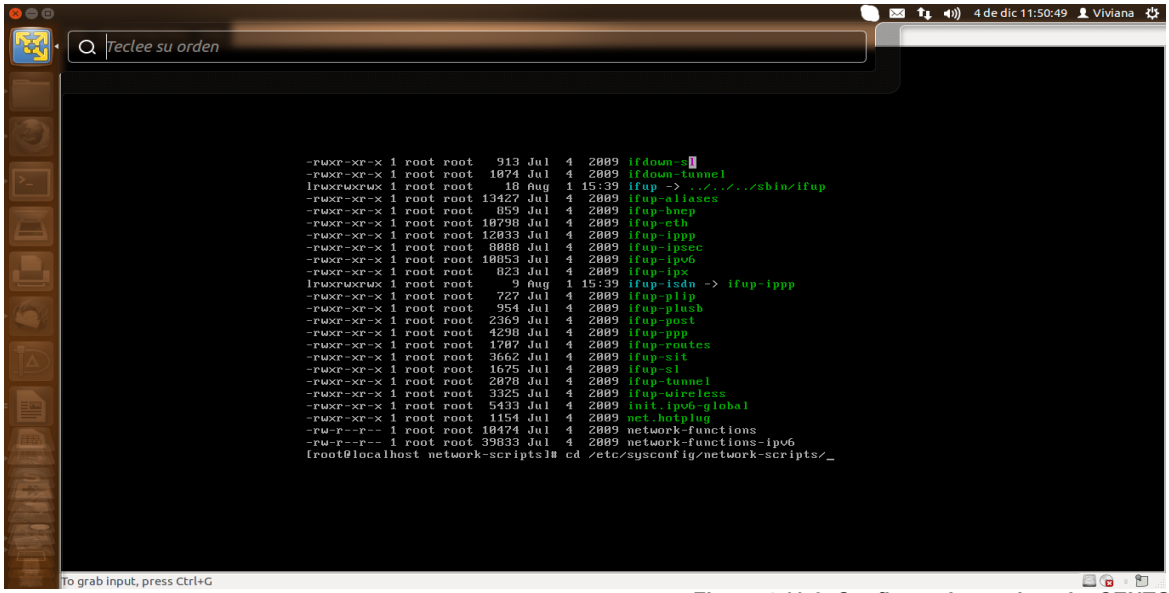


Figura 4.11-6. Configuraciones de red – CENTOS

Localizar el archivo de configuración ifcfg-eth0, y configurar de acuerdo al entorno de red, la dirección IP, la máscara de red, etc.

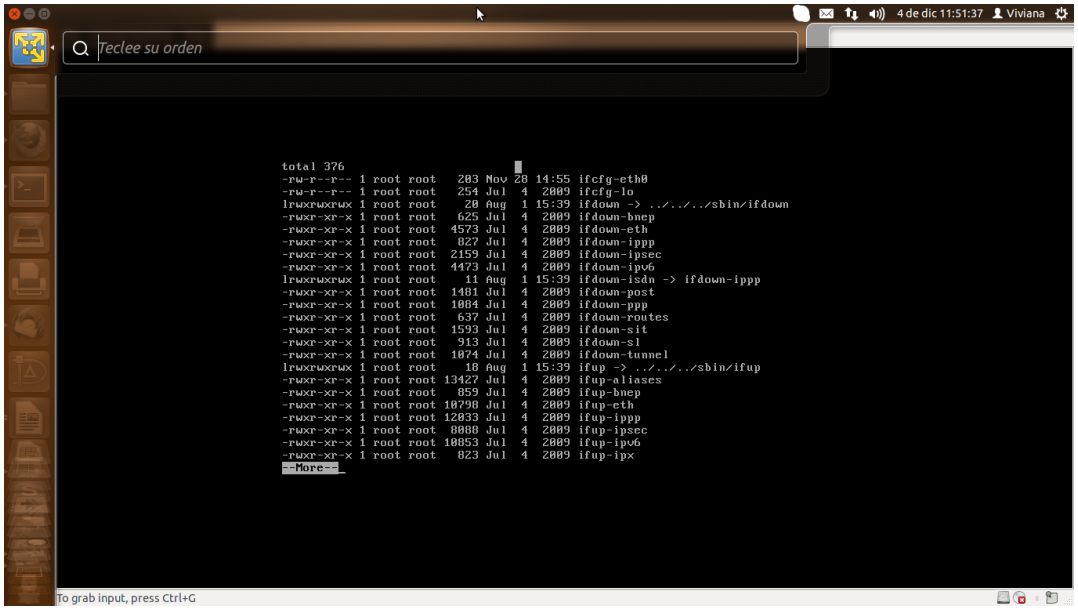


Figura 4.11-7. Configuraciones de red – CENTOS

La configuración para el entorno de prueba considerado para este demo quedaría de la siguiente forma.

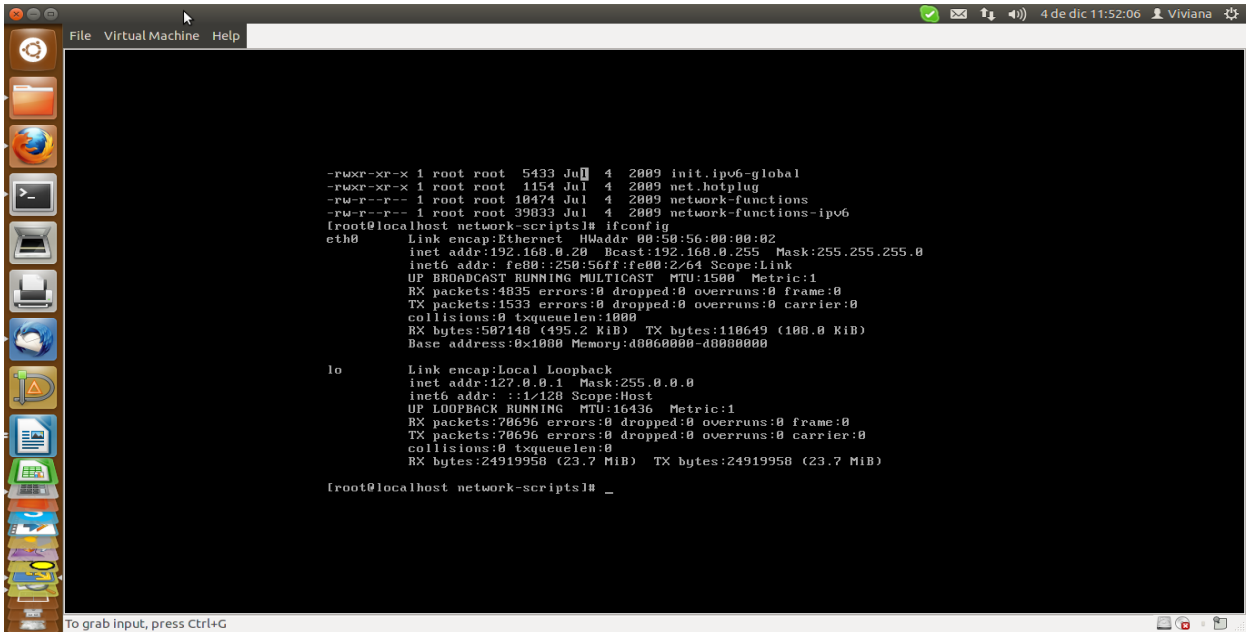


Figura 4.11-8. Configuraciones de red – CENTOS

Los parámetros anteriores son proporcionados por el administrador de red, o bien definidos de acuerdo a la planificación previamente establecida. El administrador deberá proporcionar una dirección IP y una máscara de red.

Ahora estamos listos para ingresar a la consola de administración de ZENOSS.



Figura 4.11-8. Configuraciones – ZENOSS

El usuario y la contraseña es zenoss, luego nos desplegara la pantalla principal de ZENOSS, como vemos es muy intuitiva.

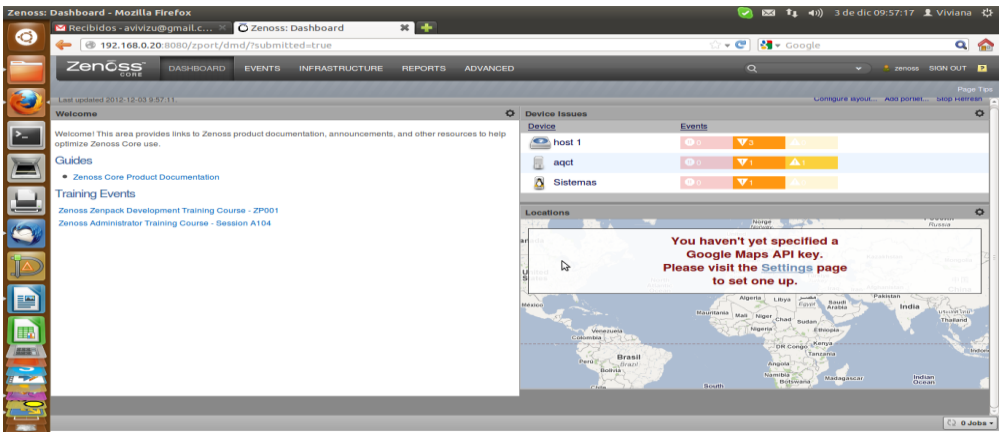


Figura 4.11-9. Pantalla principal – ZENOSS

Vamos a la pestaña INFRAESTRUCTURE en la opción NETWORKS. Lo primero que debe hacerse es descubrir el entorno de red, la herramienta lo hace sola, hay que establecer la red y la mascara, con esta información ZENOSS hace un sondeo de la red en búsqueda de nodos activos.

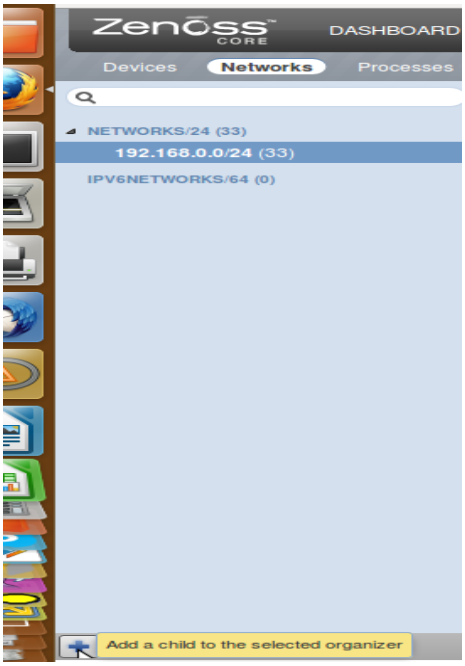


Figura 4.11-10. Descubriendo el entorno de red – ZENOSS

Ingresamos la red a descubrir junto con su máscara de red.

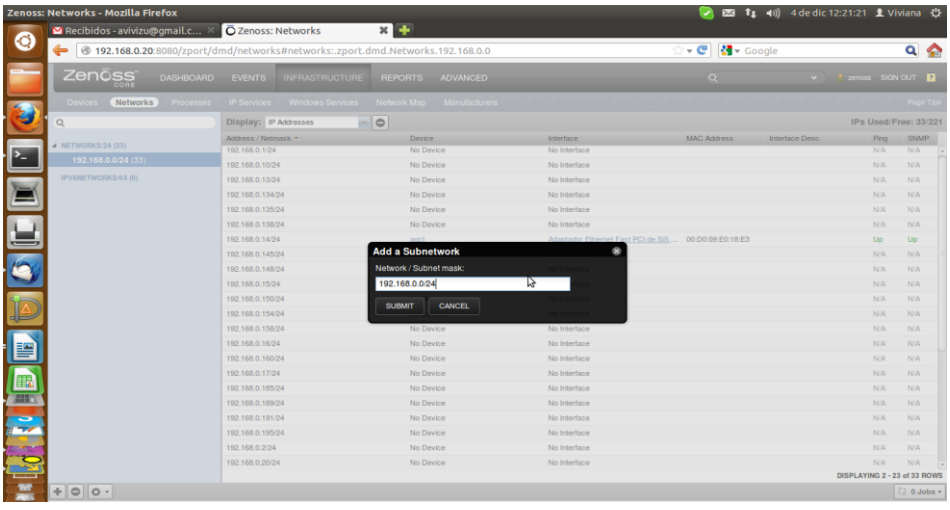


Figura 4.11-11. Descubriendo el entorno de red – ZENOSS

La herramienta despliega en pantalla todos los nodos descubiertos.

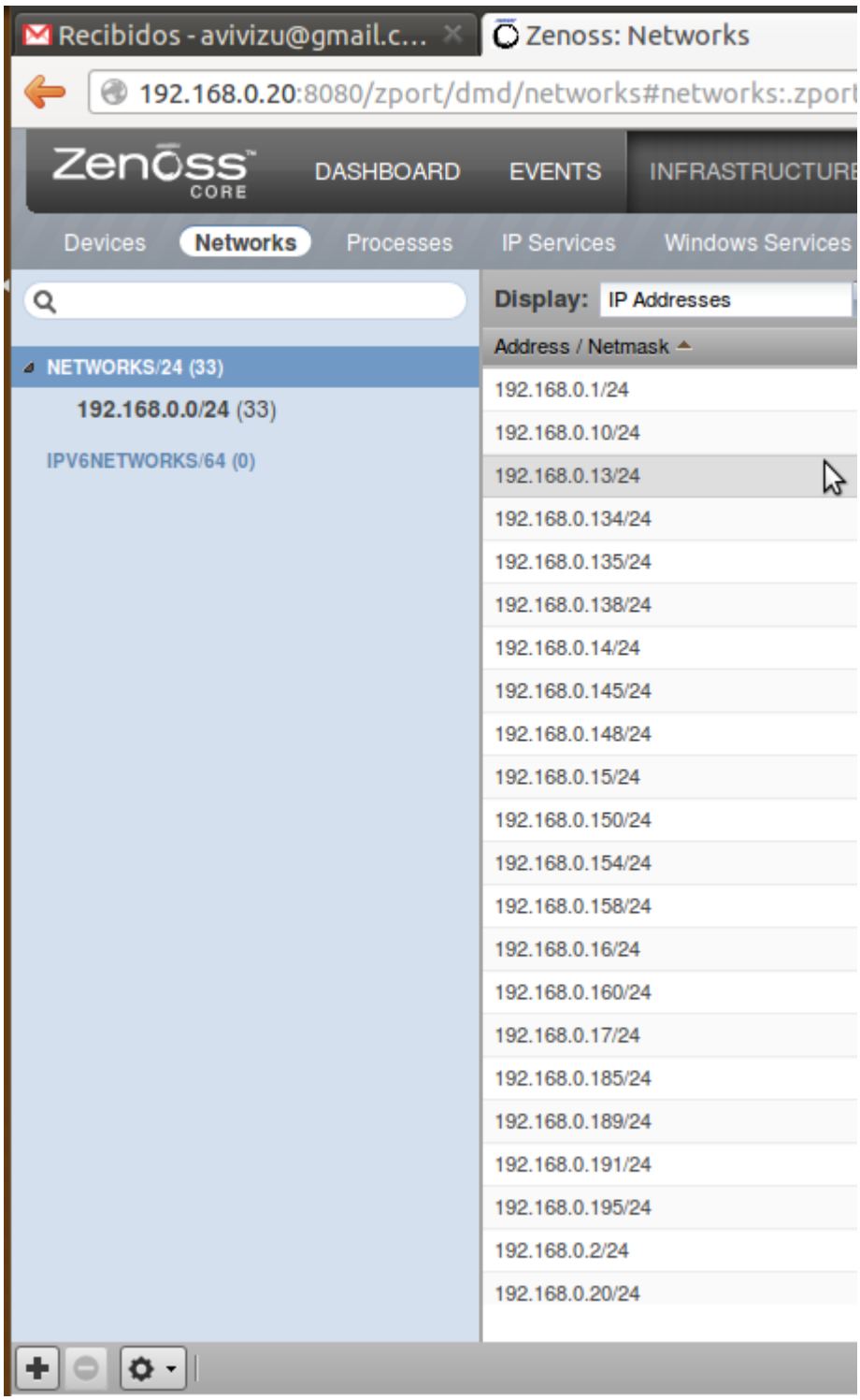


Figura 4.11-12. Descubriendo el entorno de red – ZENOSS

Como vemos en éste demo nuestro en nuestro entorno fueron descubiertos 33 nodos.

4.3.3.3. MONITOREO.

Para el monitoreo vamos a la pestaña de dispositivos donde ZENOSS mostrara todas y cada una de las características del nodo que se necesite monitorear por ejemplo.

Vamos a nuestro entorno demo al nodo con dirección IP 192.168.0.14, de lo que podemos ver.

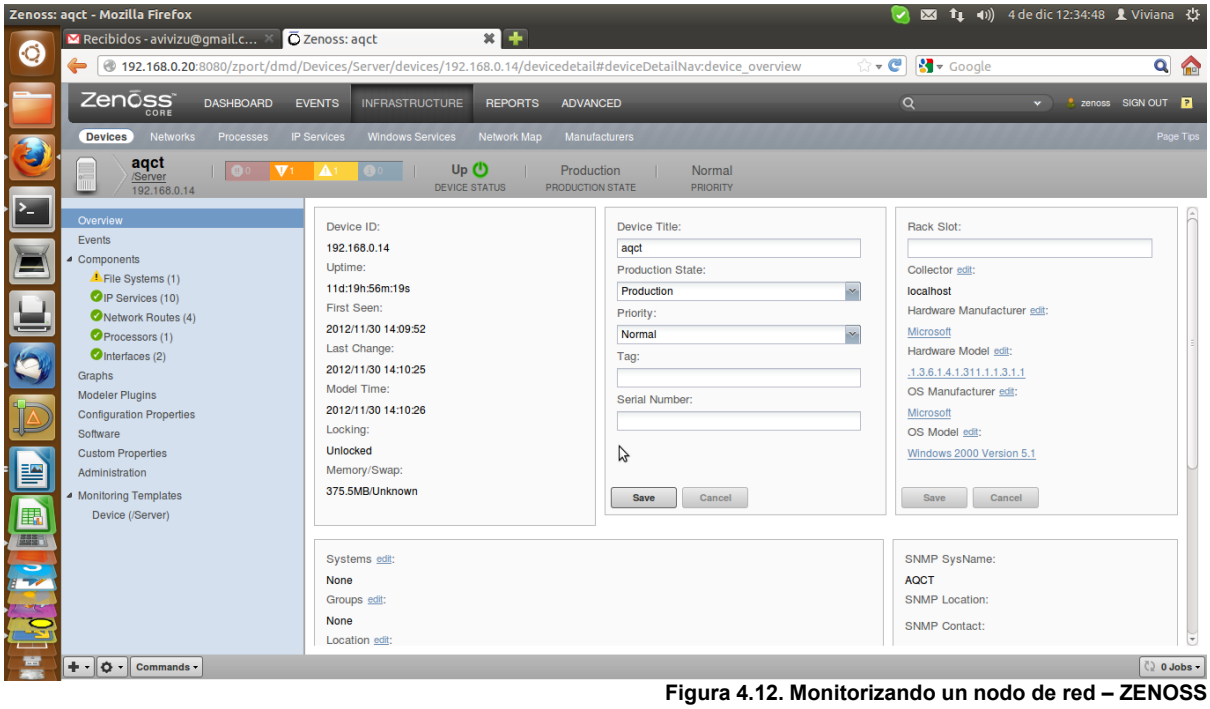


Figura 4.12. Monitorizando un nodo de red – ZENOSS

Como vemos se visualiza información detallada acerca del nodo en cuestión como por ejemplo: dirección IP, fechas de actualización, y memoria.

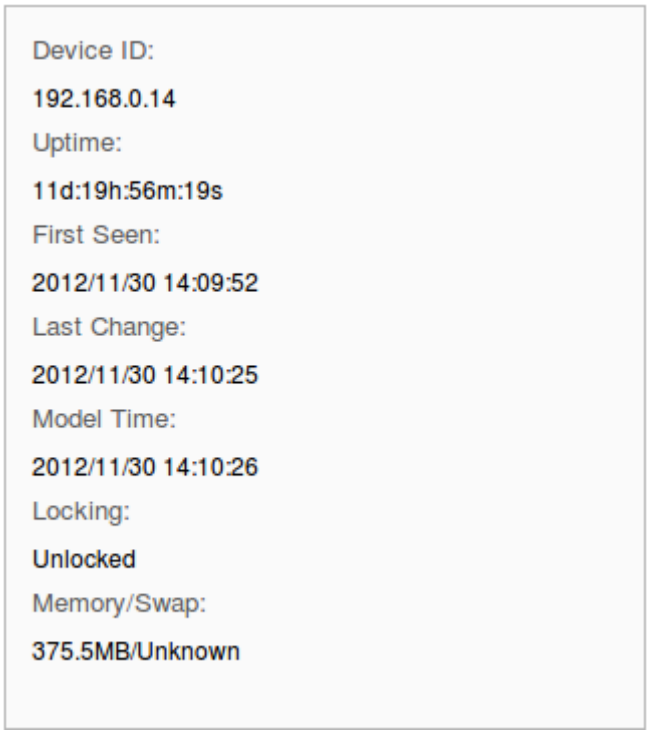


Figura 4.12-1. Monitorizando un nodo de red – ZENOSS

También se pude visualizar información acerca del sistema operativo del nodo y versión.

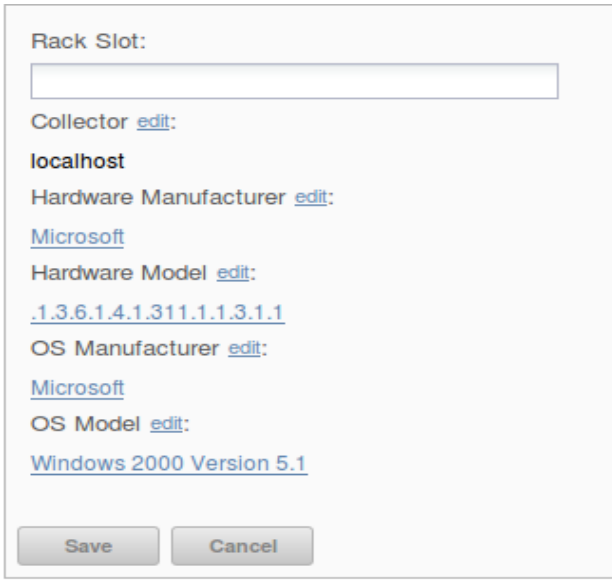


Figura 4.12-2. Monitorizando un nodo de red – ZENOSS

Como vemos la herramienta de monitoreo es muy completa y potente, tal es así que podemos visualizar información en tiempo real flujo de información y/o paquetes enviados y recibidos por cada una de las interfaces de red que posea el nodo en cuestión.

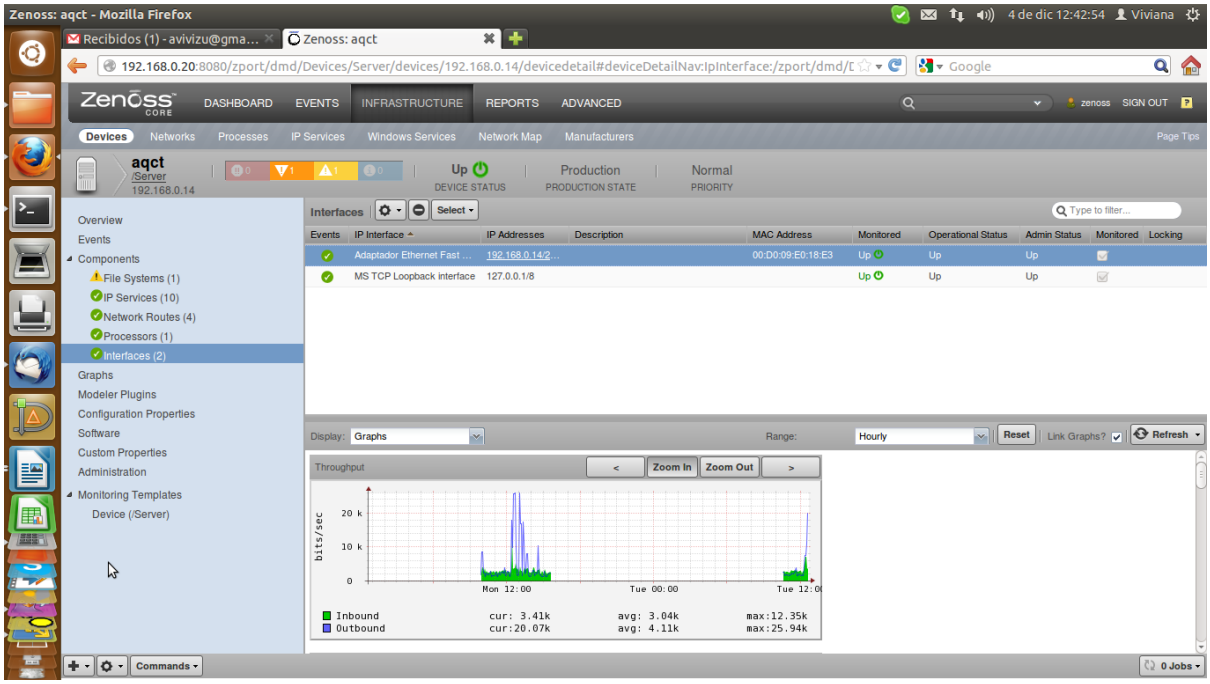


Figura 4.12-3. Monitorizando un nodo de red – ZENOSS

Como vemos en la figura anterior las gráficas de con picos de flujos de carga, son muy importantes a la hora de administrar un entorno de red y controlar el ancho de banda o flujos inadecuados de información.

Además ZENOSS gestiona y almacena las bitácoras de actualización de software en el nodo.

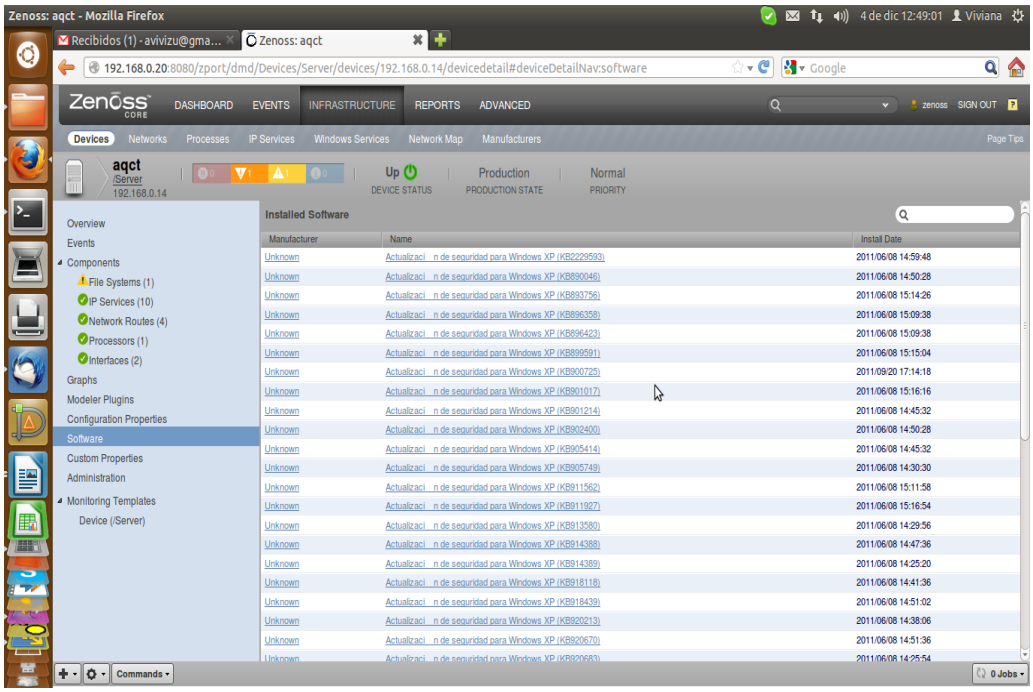


Figura 4.12-4. Monitorizando un nodo de red – ZENOSS

Además ZENOSS cuenta con las herramientas básicas de monitoreo y control para cada uno de los nodos que hacen parte del entorno de red, tales como: ping, trace, etc.

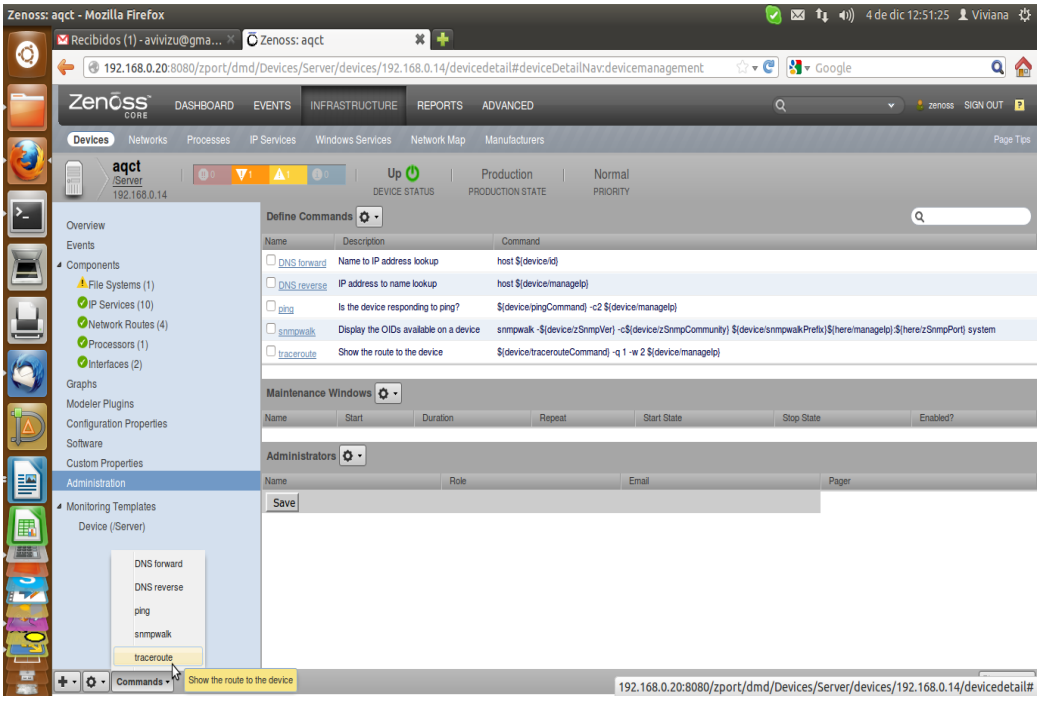


Figura 4.12-5. Monitorizando un nodo de red – ZENOSS

Hemos detallado las herramientas y opciones más importantes con las que cuenta ZENOSS para monitorear y gestionar una red, como hemos visto ZENOSS es una herramienta de vanguardia muy poderosa adaptable a cualquier entorno de red.

4.3.3.4. ALERTAS.

En cuanto a las alertas de red ZENOSS notifica alertas de todo tipo en rutas que podemos mencionar; cuando un host o nodo a dejado de funcionar o esta “down”,

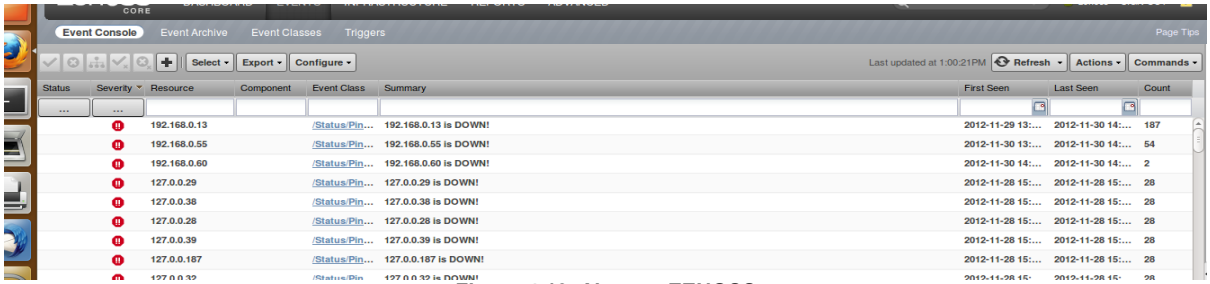


Figura 4.13. Alertas– ZENOSS

Y cada una de las alertas puede llegar al correo del administrador vía SMTP. Para el efecto ha y que configurar en la pestaña de configuraciones avanzadas.

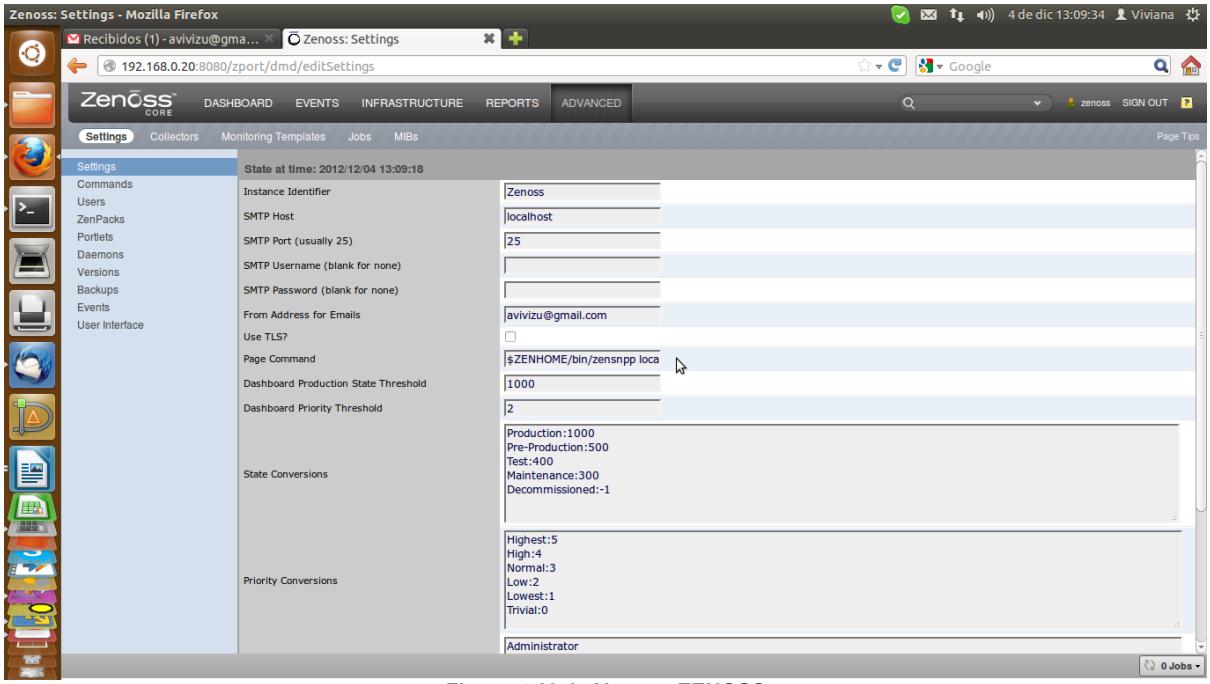


Figura 4.13-1. Alertas– ZENOSS

Inclusive si la red está distribuida existes “zenpack” que permiten administrar redes distribuidas o geográficamente distantes.

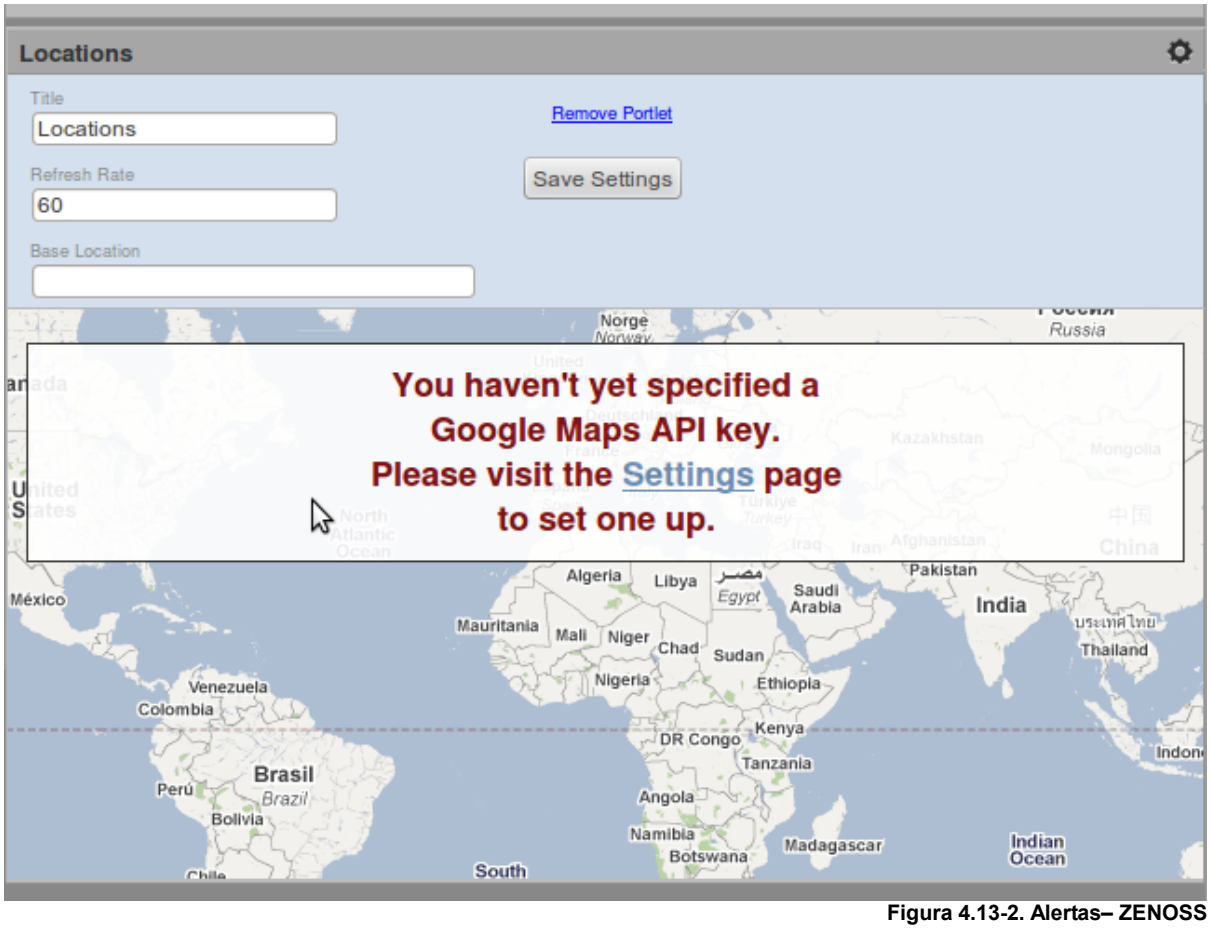


Figura 4.13-2. Alertas– ZENOSS

Como vemos las opciones de administración para la gestión de un entorno de red con ZENOSS son realmente muy extensas.

4.4. PRUEBAS DE FUNCIONAMIENTO.

4.4.1. POSIBLES FALLAS.

ZENOSS depende de que haya una buena configuración inicial, tal como se ha detallado en el presente documento, en cuanto a las fallas más comunes podemos mencionar: inadecuada configuración en los parámetros de red tanto en el gestor como en el gestionado.

Los datos evaluados son tiempo de respuesta y disponibilidad, la eficiencia del estado de los enlaces, tiempos de subida.

No se puede determinar el nombre del dispositivo o host, cuando éste se encuentre en los siguientes casos:

(a) Sistema Operativo Windows y protocolo NetBIOS deshabilitado,

(b) Dispositivos administrables sin configuración SNMP, y

(c) Hosts LINUX con servicio SNMP apagado.

Ésta información no se puede determinar, debido a que se envían paquetes de exploración que necesitan de estos servicios para obtener los resultados correspondientes. De él o los dispositivos que se encuentren en ésta situación, el reporte de los resultados acerca de ellos será mínimo.

Para el Monitor de Tráfico, si el usuario no sabe de la utilización de un proxy y si éste es o no transparente, el análisis de tráfico HTTP se lo realiza a través del puerto 80, además si los números de puerto asignados originalmente a las aplicaciones HTTP, FTP, SMTP y SNMP fueron cambiados en el host donde se ejecuta la aplicación, el Monitoreo de Tráfico por puertos no entregará los resultados adecuados.

La gestión de redes con ZENOSS básicamente describe el uso de la infraestructura de red en busca de componentes defectuosos o con comportamiento inadecuado, o lentos, etc., para luego informar al administrador mediante correo electrónico, u otras alarmas. Es un subconjunto de funciones de la administración de redes.

CAPITULO 5. RECOMENDACIONES Y CONCLUSIONES.

5.1. RECOMENDACIONES.

- El principal problema de LINUX y sus aplicaciones, es la dificultad de configuración.

- ZENOSS tiene una interfaz de configuración gráfica, que permite un sencillo control de todas las funcionalidades de la aplicación.
  La principal ventaja de la ZENOSS es su integración. Unir en un mismo paquete, funcionalidades como administración de ancho de banda, monitor de dispositivos y monitor de tráfico.

- ZENOSS es considerado como una de los herramientas más eficientes para gestión de red, si no el más popular sistema de monitorización de red de código abierto disponible, es un sistema es bastante completo para las necesidades actuales de cualquier infraestructura de red y las que
  puedan emerger a corto plazo, sin embargo se le pueden incluir nuevas características, como trabajos a futuro.

- Entre las bondades principales que pudimos apreciar tenemos: determinar el estatus de un nodo en la red, software de monitoreo puede enviar periódicamente mensajes mediante SMTP.

- Para poder establecer una buena política de uso de ancho de banda se recomienda realizar un seguimiento del mismo. ZENOSS provee un historial detallado del tráfico cursado en la red, permitiendo establecerse con estos datos una política de consumo del ancho de banda, basada en argumentos reales.

- Con los datos del ancho de banda que se dispone en la red LAN, con ZENOSS se dispone de una herramienta para ajustar el consumo de ancho de banda de acuerdo a parámetros tales como: IP fuente, IP destino y tipo de protocolo.

- No es recomendable la utilización de un único host como servidor para diferentes aplicaciones (FTP, MAIL, DNS, WEB, etc.). Esto, para evitar que todo el tráfico sea dirigido hacia un solo host y éste se vea congestionado por la cantidad de información que debe manejar.

- Para la administración de la aplicación ZENOSS, requiere que el usuario tenga un mínimo conocimiento de los conceptos básicos del manejo y administración de red en entornos Linux.

5.2. CONCLUSIONES.

- La administración de red tiene por objetivo proporcionar herramientas automatizadas y manuales de administración al usuario de red, para que éste pueda detectar posibles fallas o degradaciones en el desempeño de la misma. Le permite contar con estrategias de administración para optimizar la infraestructura existente y mejorar el rendimiento de aplicaciones y servicios.

- Muchas instituciones mantienen estructuras de comunicaciones complejas, debido a la necesidad de mantenerse comunicados con sus filiales; por lo que precisan de una buena administración de red que permita un mejor manejo y control de los elementos que la conforman.

- Una buena herramienta para gestión de redes debe ser fácil de instalar y usar. ZENOSS cuenta con las siguientes funcionalidades:

- Administración remota a través de navegador web.
- Notificaciones sobre fallos a través de correo electrónico.
- Amplia selección de sensores a través de sus zenpacks.
- Posibilidad de monitorear varios sitios con una sola instalación.
- Soporte de todos los métodos comunes de adquisición de datos de utilización SNMP.

- Se logró conseguir una monitorización efectiva, ZENOSS supervisa los signos vitales de la red: **disponibilidad, velocidad y actividad.**

- El monitoreo de la disponibilidad de red comprueba si los servicios ofrecidos están en funcionamiento y si tantos los usuarios internos como externos pueden acceder a ellos. Incluye el monitoreo de, servidores de correo electrónico, y conexiones de Internet.

- Pudimos constatar que ZENOSS monitoreo el ancho de banda y la velocidad de red evitando por ejemplo que páginas web y servicios de red pierdan visitantes debido a páginas, ficheros o imágenes que tardan mucho en cargar.

- ZENOSS evalúa las cargas que los equipos de red tienen que sostener y para ver las tendencias de utilización.

- La interfaz gráfica presenta la opción de acceder a reportes para el control de tráfico, así como también ZENOSS cuenta la opción de ir observando las estadísticas que guardan cada una de nodos de acuerdo al número de paquetes que cursan por cada una de sus interfaces.

- ZENOSS monitorea los recursos de la red para conocer su estatus en tiempo real y continuamente actualiza su base de datos con nueva información, como cambios en la red. ZENOSS también sirve de soporte para identificar la causa raíz de los problemas en el entorno de red y reducir significativamente

el tiempo utilizado para resolverlos.

- Cuando ocurre un problema, ZENOSS guía al operador a través del mapa de topología de la red, al dispositivo que presenta el problema. El administrador de la red puede inmediatamente ver la data de otros dispositivos y sistemas impactados.

- Los mapas de la red son generados automáticamente y administrados por ZENOSS. A medida que se producen cambios en la red, ZENOSS actualiza la base de datos de la topología de la red y los mapas sin intervención manual, ahorrando tiempo y esfuerzo y reduciendo las tareas administrativas.

- Dentro del Monitoreo de dispositivos, los resultados son obtenidos y presentados de manera automática, se puedan desplegar los resultados en el espacio determinado para ello.

- Se facilita la interpretación de los resultados del Monitoreo de dispositivos a través de páginas ubicadas dentro de la misma ventana tanto para entornos Windows y/o LINUX, Dispositivos Administrables, etc.

BIBLIOGRAFÍA.

http://es.wikipedia.org/wiki/

http://www.ramonmillan.com

http://es.scribd.com/doc/71082471/Monitoreo-Y-Gestion-de-Red

http://www.mcgraw-hill.es

http://wiki.ehas.org/

http://es.wikipedia.org/

ftp://ftp.eitf.org

http://nagioses.blogspot.com/

http://exchange.nagios.org/

http://community.zenoss.org/

http://centos.pop.com.br/6.3/isos/i386/

http://www.aplicacionesempresariales.com/

http://www.linux-magazine.es

https://my.vmware.com/

http://www.zenoss.com/

Morris S, “Network Management, MIBs and MPLS:
Principles, Desing and Implementation”, Addison Wesley.

PONTIFICIA UNIVERSIDAD DE PERÚ - “DISEÑO E IMPLEMENTACIÓN DEL CENTRO DE OPERACIÓN Y GESTIÓN DE LA RED ACADÉMICA PERUANA EN SOFTWARE LIBRE”.

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL - “INSTALACIÓN Y CONFIGURACIÓN DE SOFTWARE OPEN SOURCE PARA MONITOREAR EL SERVICIO Y LA CARGA DE UN SISTEMA ASTERISK”