UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

Monitoreo y gestión de la red universitaria utilizando el protocolo SNMP

TESIS
Para obtener el grado de
Ingeniero en Redes

PRESENTA
Iván Giovanni Olivera Montalvo

DIRECTOR DE TESIS
MSI. Rubén Enrique González Elixavide

ASESORES
Dr. Jaime Silverio Ortegón Aguilar
MTI. Vladimir Veniamin Cabañas Victoria
Dr. Freddy Ignacio Chan Puc
MTI. Melissa Blanqueto Estrada

Chetumal Quintana Roo, México, diciembre de 2013

UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

Trabajo de Tesis elaborado bajo supervisión del Comité de asesoría y aprobado como requisito parcial para obtener el grado de:

INGENIERO EN REDES

Comité de Trabajo de Tesis

Director: _____
MSI. Rubén Enrique González Elixavide

Asesor: _____
Dr. Jaime Silverio Ortegón Aguilar

Asesor: _____
MTI. Vladimir Veniamin Cabañas Victoria

Chetumal, Quintana Roo, México, Diciembre de 2013.

Agradecimientos

A mis padres:

Les agradezco a mis padres, Sr. Carlos Olivera Martínez y Sra. Francisca Montalvo Martín, todo el apoyo brindado durante todos los años que duraron mis estudios, por todas las facilidades, por nunca dejarme solo y estar ahí en las buenas y en las malas. Gracias por todos sus regaños y consejos, pero sobre todo por los ánimos para no tirar la toalla y poder llegar hasta aquí.

A mis profesores:

También quiero agradecer a todos los profesores que participaron en mi formación académica, sobre todo a los que participaron en la revisión de este trabajo de tesis, MTI. Vladimir Cabañas Victoria, Dr. Jaime Ortegón Aguilar y MSI. Rubén González Elixavide, grandes mentores a los que les agradezco todas sus enseñanzas, tiempo y paciencia.

A la Universidad de Quintana Roo

Así también quiero agradecer a la Universidad de Quintana Roo por el apoyo con la facilitación de los planos arquitectónicos de los edificios de la Universidad y la impresión de éste trabajo.

Un agradecimiento a Luis Fernando Mis, administrador de la red de datos universitaria, por todas las facilidades brindadas para la realización de este trabajo de tesis.

Dedicatoria

Este trabajo de tesis va dedicado a las dos personas que durante tantos años pusieron todos sus esfuerzos para que mi meta de ser un profesionista pudiera hacerse realidad, mis padres, Sr. Carlos Olivera Martínez y Sra. Francisca Montalvo Martín, quienes con trabajo, empeño y dedicación lograron darme estudios universitarios.

Mamá, papá, hoy puedo decirles con orgullo que todos sus esfuerzos no fueron en vano, que me tardé un poquito pero alcancé mi meta. Ojalá se sientan orgullosos de mi como yo me siento orgulloso de ustedes y ojalá la vida me los preste muchos años más para seguir compartiéndoles éxitos como este, por que este éxito es suyo.

Resumen

El Departamento de Cómputo y Telemática es el área responsable de mantener el correcto funcionamiento de las redes de telecomunicaciones en la Universidad de Quintana Roo, evitando el deterioro del rendimiento de la red y previniendo interrupciones en el servicio que afecten a los usuarios.

Sin embargo, carecen de una herramienta de monitoreo automatizada que notifique en tiempo real las fallas que día a día suceden en la red universitaria, que debido a su modernidad y a la cantidad de dispositivos y servicios, son difíciles de monitorear y gestionar.

Es por ello que la implementación de una herramienta de gestión de red en la Universidad de Quintana Roo unidad Chetumal es de suma importancia, volviéndose indispensable para el administrador de red.

Por todo lo anterior, el objetivo de este trabajo de tesis es el monitoreo y gestión de la red universitaria utilizando el protocolo SNMP, documentando un método de gestión de red con base en los requerimientos especificados por el administrador de red de la Universidad.

La herramienta elegida para realizar el trabajo de monitoreo y gestión de la red universitaria fue Nagios Core, una poderosa herramienta open source, que trabajando en conjunto con el protocolo SNMP, forman una excelente opción gracias al concepto gestor-agente con el que trabaja este protocolo.

De esta forma, este trabajo de tesis benefició enormemente al administrador de red mejorando el monitoreo y la gestión de los dispositivos, notificandole en tiempo real los distintos eventos que se llevan a cabo con los dispositivos de la red universitaria.

Índice de contenido

Índice de Figuras

Índice de Tablas

CAPÍTULO 1

CAPÍTULO 1 – Introducción

El Departamento de Cómputo y Telemática –DCT, adscrito a la Dirección de Informática de la Universidad de Quintana Roo, es el área responsable de mantener el correcto funcionamiento de las redes de telecomunicaciones en la Universidad. Una de las prioridades de esta área es evitar el deterioro del rendimiento de la red o prevenir interrupciones en el servicio que afecten a los usuarios. Sin embargo, al carecer de un monitoreo automatizado de los dispositivos de comunicaciones, de servidores y de servicios, conlleva a que muchas de las problemáticas en la red universitaria sean detectadas por los usuarios finales y no por el administrador de la red, lo que genera malestar entre los mismos usuarios y proyecta una mala imagen del Departamento de Cómputo y Telemática.

Pocos son los dispositivos de comunicaciones que son monitorizados en tiempo real en la Universidad y si alguno de ellos presentara algún inconveniente o alteración en su funcionamiento o configuración, éstos generan una alerta pero que no es enviada al administrador de la red universitaria.

Además de las dificultades para la realización del análisis de la red, se suman el presupuestal y el humano. Generalmente la estrategia utilizada por el DCT para la implementación de nuevas tecnologías, en este caso de software que ayuden a la gestión de redes, es primeramente la evaluación de aquellas opciones que ofrece el software *open source*, sin embargo este tipo de productos, a pesar de ser funcionales, requiere habilidades técnicas adicionales por personal especializado.

Justificación

La implementación de un sistema de monitoreo de red para el control de dispositivos y de servicios, ha ganado suma importancia, volviéndose indispensable para los administradores de red, esto debido a la complejidad en la estructura de las redes de datos modernas que manejan numerosos dispositivos como servidores, switches y routers y gran cantidad de servicios como DHCP, SSH, FTP, HTTP entre otros.

Un sistema de monitoreo de red es un software especializado que permite visualizar de manera remota los detalles de los distintos dispositivos y servicios que estén funcionando en la red, esto a través de un panel de monitoreo que muestra el estado del dispositivo, del componente o del servicio en ejecución, y genera alertas en caso de que sea detectada alguna falla, sobrecarga de algún sistema o cambio en la configuración.

Así también, este tipo de aplicaciones brinda herramientas tales como mapas lógicos que ayudan al administrador de la red a tener un panorama gráfico de la estructura interna de la red, lo que le permite generar reportes con los cuales puede tomar decisiones con base a estadísticas de uso.

Existen aplicaciones *open source* disponibles en el mercado que permiten a los administradores de red gestionar muchas de estas tareas de manera práctica, sin embargo tienen un costo muy alto y no accesible para la mayoría de las instituciones. Varias de estas aplicaciones cuentan con una versión gratuita que aunque es completamente funcional, cuenta con limitaciones que no vuelven práctica la administración de un sistema de monitoreo de red.

Debido a las limitaciones en precio y en practicidad, es necesario el desarrollo e implementación de un software que facilite de manera integral la administración de la versión gratuita de este tipo de software.

Objetivo General

- Monitorear y gestionar la red universitaria utilizando el protocolo SNMP.

Objetivos particulares

- Definir el método de monitoreo,
- Definir los diagramas físicos de red,
- Establecer los criterios de monitoreo,
- Definir los dispositivos y servicios a monitorear,
- Instalar y configurar la estación de gestión de red,
- Desarrollar una aplicación que permita la generación de archivos de configuración,
- Configurar los dispositivos y servicios a monitorear,
- Generar estadísticas de uso,
- Recomendar acciones y estrategias para mejorar el rendimiento de la red.

Alcance

- Se implementará una herramienta open source para el monitoreo de dispositivos de la red universitaria,
- Los dispositivos de red que se van a monitorear, están ubicados en la Universidad de Quintana Roo, unidad Chetumal y serán definidos por el administrador de la red universitaria,
- Se configurará la herramienta para cada dispositivo de red que se vaya a monitorear,

- Deberá generar estadísticas de uso de los dispositivos asignados por el administrador de la red universitaria,
- Deberá generar alarmas de acuerdo a los parámetros que establezca el administrador de la red universitaria,
- Se desarrollará una aplicación que genere archivos con los parámetros por default o personalizado para el monitoreo de cada dispositivo, así como los servicios de red que ofrece,
- Se creará un plan de mejora para la red universitaria considerando los datos obtenidos.

Metodología

Tipo de investigación:

- Descriptiva

Para esta investigación, se obtuvo una entrevista con el administrador de la red de la Universidad de Quintana Roo. El administrador describió las dificultades que tiene para gestionar los dispositivos de comunicaciones centrales y de los servidores de la red universitaria, por lo que se definió qué dispositivos, servicios y servidores deben de ser monitoreados de forma constante. Para tal problemática, se establecieron algunas de las características que debería cumplir la aplicación que realizaría estas tareas.

- Experimental

Para esta investigación se utilizarán algunos de los dispositivos en producción de la red institucional como son routers, switches, access points y servidores, que serán configurados en un entorno real de acuerdo a la topología presentada por la Universidad de Quintana Roo.

Método utilizado:

- Método empírico.

Objeto:

- Red universitaria.

Medio:

- Referencias electrónicas.
- Pruebas con dispositivos dentro de la red universitaria.
- Recopilación de información bibliográfica.

CAPÍTULO 2

CAPÍTULO 2 – Marco Teórico/Contextual

Contexto

La Universidad de Quintana Roo es el centro académico en su tipo más joven del país. Su creación responde a un viejo anhelo de los quintanarroenses de contar con un centro de educación superior para formar profesionales en las áreas sociales, las humanidades, las ciencias básicas y las áreas tecnológicas de mayor demanda y consumo en esta época de alta competitividad (UQRoo, Historia).

Su creación hizo acopio de las invaluables experiencias acumuladas en los últimos setenta años de la educación superior y se incorporaron innovadores conceptos con objeto de convertirla en una universidad de excelencia en México y la Cuenca del Caribe (UQRoo, Historia).

La infraestructura de la Universidad de Quintana Roo (UQRoo) incorpora adelantos tecnológicos en áreas sustantivas, como telecomunicaciones basadas en redes de fibra óptica e inalámbricas (UQRoo, Infraestructura y servicios) debido a que las redes de telecomunicaciones se han convertido en elementos esenciales en las actividades de las personas que laboran y estudian en la institución, utilizando servicios de voz, datos y vídeo.

La Universidad de Quintana Roo está ubicada en la ciudad de Chetumal, Quintana Roo, México sobre la Av. Boulevard Bahía entre Ignacio Comonfort y Pucté en la colonia del Bosque (ver Figura 1). Debido al gran número de usuarios, entre estudiantes, profesores y administrativos, surge la necesidad de hacer que los servicios proporcionados por la red sean confiables, que sea posible detectar fallas rápidamente, monitorear su desempeño, utilizar eficientemente los recursos

de red, administrar la seguridad, entre otras. Es decir, surge la necesidad de gestionar la red de telecomunicaciones universitaria.

Figura 1. Mapa ubicación de la Universidad de Quintana Roo

Gestión de la red

La gestión de la red es la faceta que se ocupa de controlar el funcionamiento y el mantenimiento de la misma. Para ello se utiliza un conjunto de protocolos y técnicas que conjuntamente pueden garantizar el funcionamiento del sistema y el acoplamiento del mismo a las necesidades de funcionamiento diario de los organismos que las utilizan (Sánchez, 2000).

Los sistemas de gestión de red están diseñados para ver a la red como una arquitectura unificada, con direcciones y etiquetas asignadas a cada punto. De esos puntos (computadoras en general) se reciben o se extraen, por medio, generalmente de protocolos específicos, información de una manera regular que permite tener una fotografía casi permanente del funcionamiento general de todo el sistema (Sánchez, 2000).

En los sistemas de gestión de red se deben contemplar los siguientes aspectos:

- Actividades que permitan a los gestores de red la planificación, organización, supervisión, control y contabilidad para el uso de los servicios de red.
- Habilidad para ser capaces de escalar el sistema cuando las demandas así lo requieran.
- Técnicas para poder anticiparse, en la medida de lo posible, a los funcionamientos incorrectos que se puedan dar en la red.

Aunque todos los protocolos de red especifican modelos para facilitar su gestión, los modelos habitualmente utilizados son el modelo OSI y el modelo TCP/IP. En éste capítulo se explicará el funcionamiento de los mismos. Como se puede observar, ambos modelos tienen diferencias estructurales básicas, ya que si bien el modelo OSI pretende plantear la gestión de red de forma completa y jerárquica, resulta complicado de implementar por su complejidad (Sánchez, 2000).

Sin embargo, el esquema de gestión TCP/IP se centra en la simplicidad y la provisión, tratando de posibilitar de la forma más sencilla desde el punto de vista de costo económico y de carga para el funcionamiento de las máquinas (Sánchez, 2000).

Modelo OSI

El modelo OSI (Open System Interconection, o interconexión de sistemas abiertos) tiene un tanto de enigmático. Diseñado en su origen con el propósito de permitir que existieran protocolos independientes de los proveedores y de eliminar las pilas

de protocolos monolíticas, este modelo apenas se usa hoy para tales fines (Hill, 2002).

Sin embargo aún conserva un uso importante: es una de las mejores herramientas de que se dispone en la actualidad para describir y catalogar las complejas series de interacciones que tienen lugar en el diseño de redes. Dado que la mayoría de las pilas de protocolos utilizadas actualmente como TCP/IP fueron diseñadas a partir de modelos diferentes, muchos de los protocolos de estas pilas no se adaptan exactamente al modelo OSI, lo que es fuente de bastantes confusiones. Lo fundamental es mirar el modelo OSI cómo lo que verdaderamente es: una herramienta para enseñar y describir cómo tienen lugar las operaciones en una red (ver Figura 2) (Hill, 2002).

Figura 2. Modelo de referencia OSI (Hablemos del modelo OSI Open System Interconexion)

En la Tabla 1 se describen de manera general, las funciones de cada una de las capas del modelo de referencia OSI (Hill, 2002).

Tabla 1. Descripción de las capas del Modelo OSI

Capa	Función
Aplicación (Capa 7)	Esta capa es responsable de la comunicación directa con la propia aplicación. Permite escribir las aplicaciones con poco código de red. En vez de ello, la aplicación informa al protocolo de la capa de aplicación de lo que necesita, y es responsabilidad de dicha capa de aplicación traducir la petición a algo que la pila de protocolos sea capaz de entender.
Presentación (Capa 6)	Esta capa es responsable de todo lo relacionado con el formateo de un paquete: compresión, encriptación, decodificación y correspondencia de caracteres. Si se recibe, por ejemplo, un e-mail y el texto está encriptado, será un problema de la capa de presentación.
Sesión (Capa 5)	Esta capa es la responsable de las conexiones, o sesiones, entre dos puntos extremos (normalmente, aplicaciones). Asegura que la aplicación del otro extremo tenga configurados los parámetros correctos para establecer una aplicación bidireccional con la aplicación fuente.
Transporte (Capa 4)	Esta capa proporciona comunicación entre distintos programas de aplicación. Según el protocolo de que se trate, puede ser responsable de la detección y recuperación de errores, del establecimiento y la terminación de sesiones en la capa de transporte, del multiplexado, de la fragmentación y del control de flujo.
Red (Capa 3)	Esta capa es responsable principalmente del direccionamiento lógico y la determinación de rutas, o enrutamiento, entre agrupaciones de direcciones lógicas.
Enlace de datos (Capa 2)	Esta capa es responsable del direccionamiento físico y del control de la Network Interface Card (NIC, tarjeta de interfaz de red). Según el protocolo de que se trate, puede realizar también el control de flujo. Esta capa añade además la FCS, que ofrece cierta capacidad de detección de errores.
Física (Capa 1)	La más simple de todas las capas, sencillamente gestiona las características físicas de la conexión de red: cableado, conectores y cualquier otra cosa que sea puramente física. Esta capa es responsable asimismo de la conversión de bits y bytes (unos y ceros) a una representación física (impulsos eléctricos, ondas o señales ópticas), y de la reconversión de estas representaciones en bits en el lado de la recepción.

Modelo TCP/IP

TCP/IP es un protocolo que fue desarrollado en 1972 por el Departamento de Defensa de los Estados Unidos. El nombre TCP/IP proviene de dos de los protocolos más importantes de la familia de protocolos de Internet, el Transmission Control Protocol (TCP) y el Internet Protocol (IP) (Raya, 1997).

El protocolo TCP/IP transfiere datos mediante el ensamblaje de datos en paquetes. Cada paquete comienza con una cabecera que contiene información de control seguida de los datos. El Internet Protocol (IP), es un protocolo de nivel de red de OSI, permite a las aplicaciones ejecutarse de forma transparente sobre las redes interconectadas. De esta forma, las aplicaciones no necesitan conocer que hardware está siendo utilizado en la red, por lo que la misma aplicación puede ejecutarse en una topología Ethernet, Token-Ring o X.25 (Raya, 1997).

La principal virtud de TCP/IP es que está diseñado para enlazar dispositivos de diferentes tipos, incluyendo PC, servidores, routers y switches, que ejecuten sistemas operativos distintos sobre redes de área local y redes de área extensa, y por tanto permite la conexión de equipos distantes geográficamente (Raya, 1997). Las funcionalidades de las capas del modelo TCP/IP (ver Figura 3) están descritas en la Tabla 2.

Figura 3. Modelo TCP/IP (TCP/IP)

Tabla 2. Descripción de las capas del modelo TPC/IP *(TCP/IP)*

Capa	Función
Aplicación (Capa 4)	Esta es la capa más alta dentro de la estructura jerárquica del protocolo TCP/IP, e incluye las aplicaciones y procesos con los que intercambia datos la capa de transporte. TCP/IP tiene en esta capa protocolos que soportan servicios de conexión remota, correo electrónico y transferencia de archivos.
Transporte (Capa 3)	En esta capa se encuentran definidos el protocolo TCP y el protocolo UDP (User Datagram Protocol). TCP permite enviar los datos de un extremo a otro de la conexión con la posibilidad de detectar errores y corregirlos. UDP, por el contrario, reduce al máximo la cantidad de información incluida en la cabecera de cada datagrama, ganando con ello rapidez a costa de sacrificar la fiabilidad en la transmisión de datos.
Internet (Capa 2)	La capa Internet se encuentra justo encima de la capa de acceso a red. En este nivel el protocolo IP es el gran protagonista. El protocolo IP se ha diseñado para redes de paquetes conmutados no orientadas a conexión. Para el protocolo IP un datagrama es el formato que debe tener un paquete de datos en la capa de red.
Acceso a red (Capa 1)	IP en una trama que pueda ser transmitida por la red, siendo en una inmensa mayoría de redes LAN una trama Ethernet. Otra función importante de esta capa es la de asociar las direcciones lógicas IP a direcciones físicas de los dispositivos adaptadores de red (NIC).

Las diferencias entre el modelo OSI y modelo TCP/IP se pueden apreciar de mejor manera en la imagen comparativa de la Figura 4.

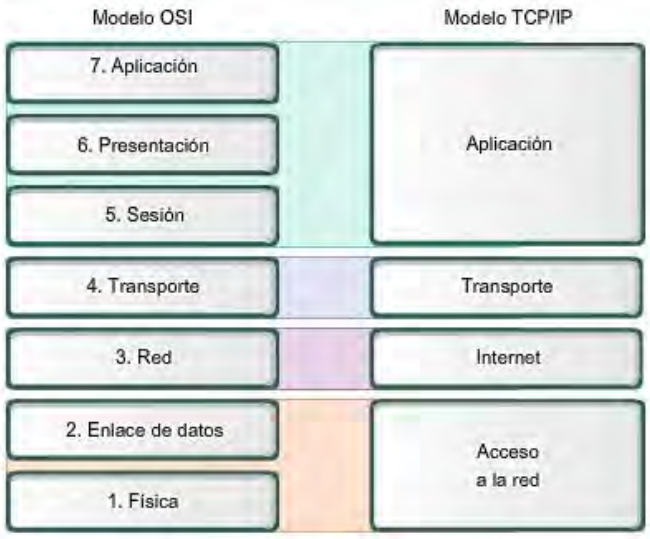

Figura 4. Comparativa entre el modelo OSI y TCP/IP (Fundamentos de redes de datos)

Administrador de la red

El administrador de red es la persona responsable de supervisar y controlar el hardware y software de una red local. El administrador trabaja en la detección y corrección de problemas que hacen ineficiente o imposible la comunicación y en la eliminación de las condiciones que pudieran llegar a provocar problemas nuevamente. Ya que tanto las fallas de hardware o de software pueden generar problemas y el administrador de red debe supervisar ambos (Comer, 1997).

La administración de red puede ser difícil por dos razones

1. La mayoría de las redes locales son heterogéneas, esto quiere decir que la red local consta de hardware y software de diferentes compañías.
2. Los dispositivos de red en las redes locales no se encuentran precisamente en el mismo punto geográfico.

Por lo tanto, es necesario utilizar un sistema que permita centralizar el monitoreo de los dispositivos de red en un sólo punto geográfico.

Este trabajo describe un sistema de gestión centralizado para la Universidad de Quintana Roo, de acuerdo con las funciones de gestión especificadas por el administrador de la red universitaria. El protocolo de gestión utilizado es SNMP (Simple Network Management Protocol).

SNMP

Este protocolo, es un marco de trabajo para gestionar los dispositivos en una red que utiliza el conjunto de protocolos TCP/IP. Ofrece un conjunto de operaciones fundamentales para monitorizar y mantener una red (Forouzan, 2002). El funcionamiento de este protocolo es muy simple, pues se basa en el concepto gestor-agente (ver Figura 5).

Figura 5. Concepto gestor-agente (Gestión de redes)

Gestor

Un gestor o una estación de gestión, es una estación que ejecuta un cliente de SNMP. Una estación gestionada, denominada agente, es un dispositivo que ejecuta el servidor de SNMP. La gestión se realiza a través de una sencilla interacción entre el gestor y el agente (Forouzan, 2002).

Agente

El agente almacena información sobre prestaciones en una base de datos denominada MIB (Management Information Base). El gestor tiene acceso a los valores de esta base de datos, la cual puede leer y comparar los valores de estas dos variables para actualizar los datos a mostrar.

Cada agente crea su propia MIB con base en el dispositivo en el que esté instalado. Los objetos en la MIB se clasificarán en ocho grupos: sistema, interfaz, traducción de direcciones, ip, icmp, tcp, udp, y egp. Estos grupos se encuentran bajo el objeto mib en el árbol de identificadores de objetos. Cada grupo tiene variables definidas y/o tablas.

MIB

Una MIB (Management Information Base) es una colección de objetos almacenados por el agente. Los objetos son parámetros que identifican cada componente del dispositivo mediante un valor numérico denominado OID (Object Identifier), que puede ser actualizado por el agente o pedido por una fuente externa, como un gestor (Hucaby, 2002).

Las MIB están estructuradas de acuerdo al lenguaje que usa SNMP en el modulo de las MIB que está basada en el lenguaje de la Sintaxis de Notación Abstracta Uno (ANS.1) (Hucaby, 2002) y es completamente jerárquica (ver Figura 6).

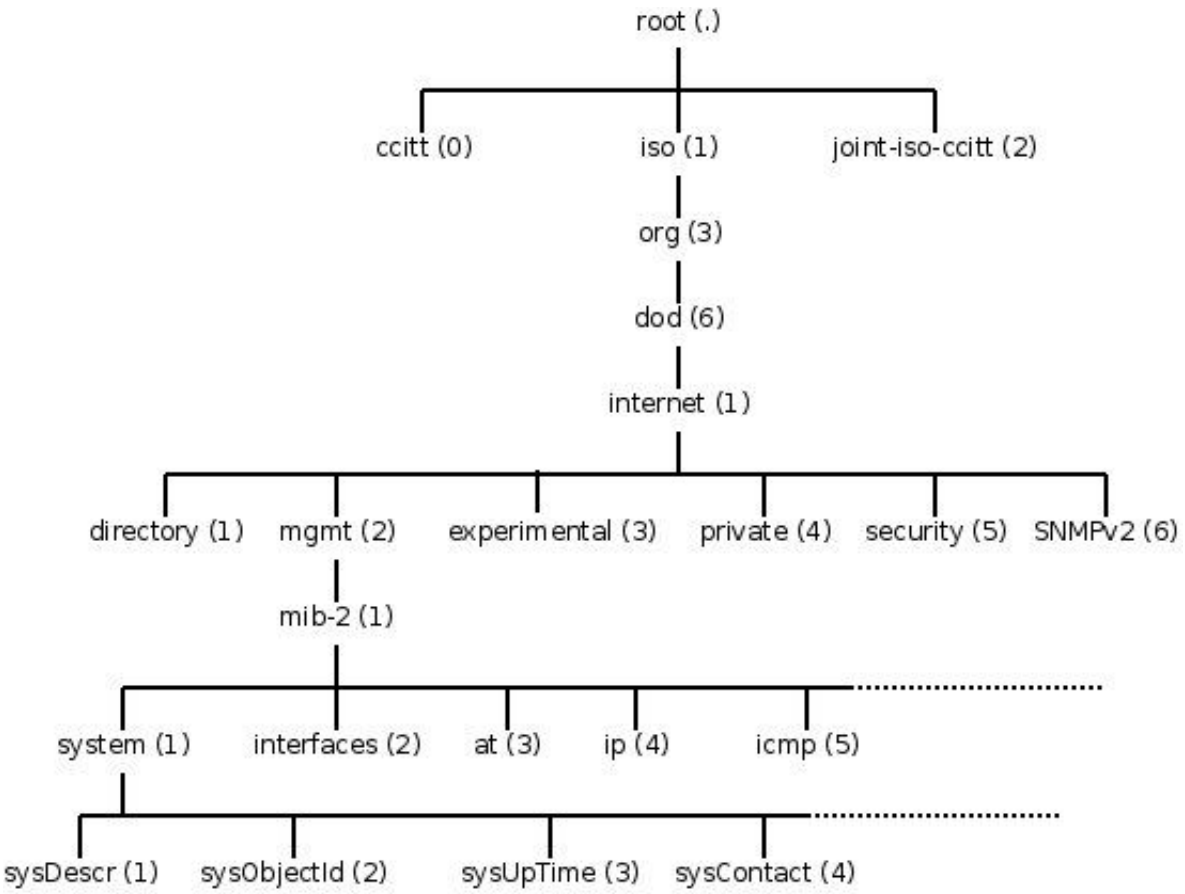

Figura 6. Estructura de una MIB-II (Gestión de redes)

A continuación, en la Tabla 3, se listan las ventajas y desventajas de utilizar el protocolo SNMP (empresas).

Tabla 3. Ventajas y desventajas de SNMP

Ventajas	Desventajas
Es un protocolo simple, con MIBs	han salido nuevas versiones SNMP V2 y V3.
Nuevos) que han mejorado las limitaciones de SNMP contra CMIP.	La
cho muy popular en el mercado	
Es posible dispositivo gestionado.	MIBs propietarios originan problemas de interoperabilidad.
agrupar variables relacionadas (ISO, Internet, Management).	usados para clasificar y agrupar variables.
mediante agentes.	
–	El uso de

Versiones de SNMP

Versión 1: Surge en el año de 1990 como primera versión, no posee seguridad solo se basa en comunidades (FIEC).

Versión 2: Se publica 1996 como un nuevo estándar. Los cambios fundamentalmente es en la mejora de las prestaciones de intercambio de información de gestión y la implementación de seguridad (FIEC).

Versión 3: Sigue el mismo formato que la versión 2, pero añade una serie de capacidades de seguridad y un marco que hace posible su uso junto con las PDUs de SNMPv.2 con mayor seguridad y administración (FIEC).

CAPÍTULO 3

CAPÍTULO 3 – Desarrollo

Este capítulo presenta un método de monitoreo de red, en el cual la primera fase es realizar el diagrama físico correspondiente a la red de datos universitaria, para definir los dispositivos estratégicos a monitorear junto con los servicios que ofrecen. Para ello, se llevó a cabo una entrevista previa con el administrador de la red universitaria para determinar la ubicación, el tipo de dispositivos y los servicios a monitorear, así como las herramientas para llevar a cabo dicha tarea.

Ubicación física de los dispositivos dentro de los edificios de la UQRoo

Las siguientes figuras son los planos arquitectónicos de los edificios de la UQRoo, en ellos se encuentran marcadas las ubicaciones de los diferentes dispositivos de red dentro de los edificios, dispositivos que son críticos para brindar a los estudiantes, profesores y administrativos, la conectividad y acceso a los diferentes servicios de la red universitaria e Internet, servicios que son necesarios para llevar a cabo diariamente sus actividades académicas y administrativas.

Estos planos fueron proporcionados por el departamento de Servicios Generales de la Universidad de Quintana Roo.

Ubicación física de los dispositivos dentro del edificio A

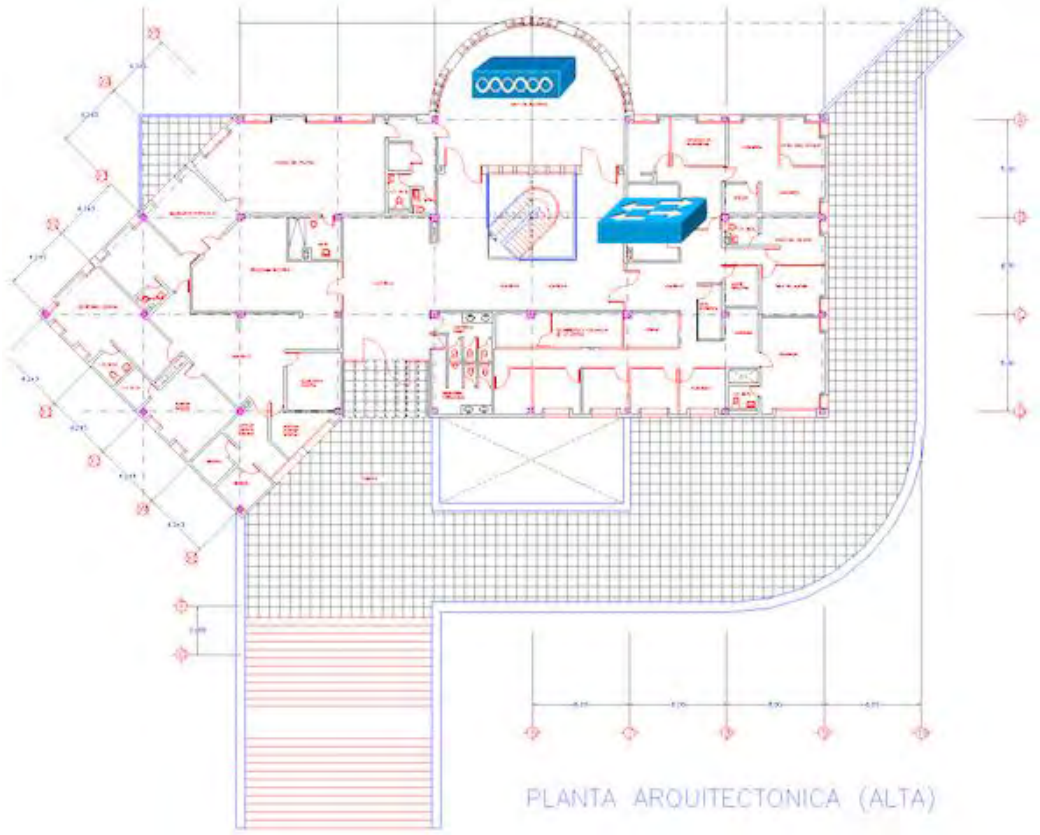

Figura 7. Ubicación física de los dispositivos dentro del edificio A

Ubicación física de los dispositivos dentro del edificio B

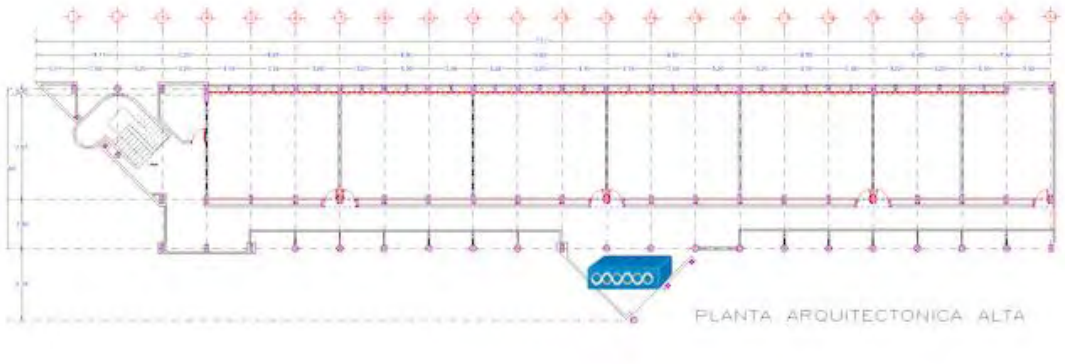

Figura 8. Ubicación física de los dispositivos dentro del edificio B

Ubicación física de los dispositivos dentro del edificio C

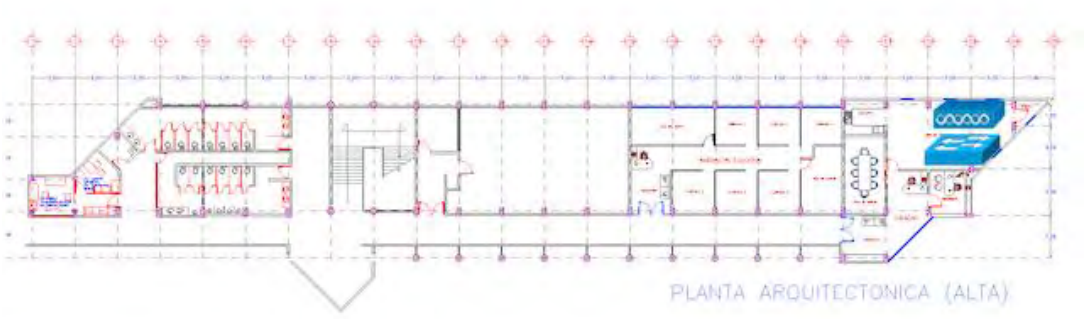

Figura 9. Ubicación física de los dispositivos dentro del edificio C

Ubicación física de los dispositivos dentro del edificio D

Figura 10. Ubicación física de los dispositivos dentro del edificio D

Ubicación física de los dispositivos dentro del edificio E

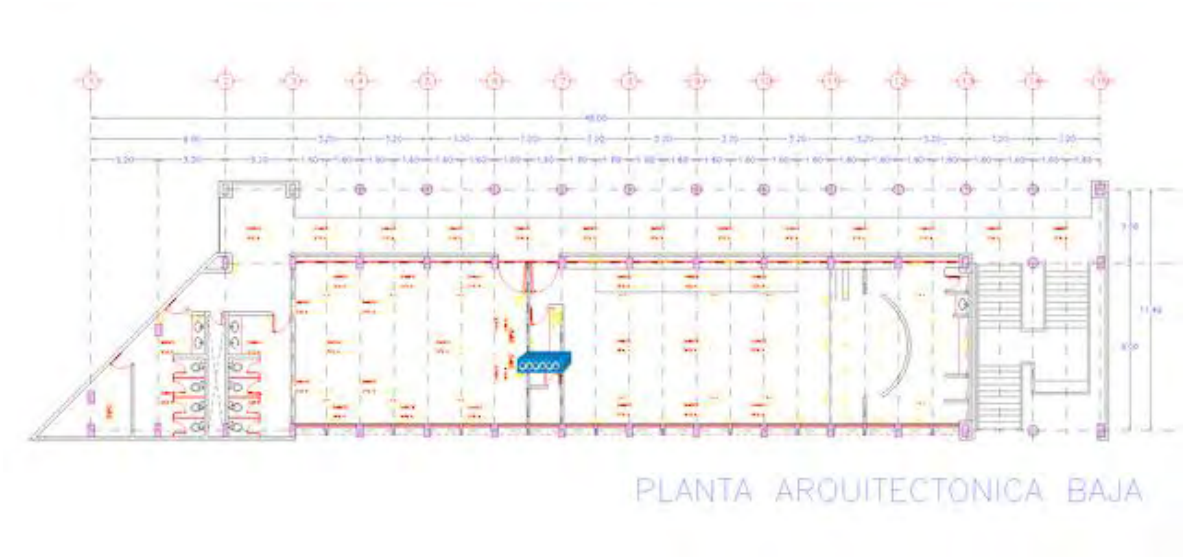

Figura 11. Ubicación física de los dispositivos dentro del edificio E

Ubicación física de los dispositivos dentro del edificio F

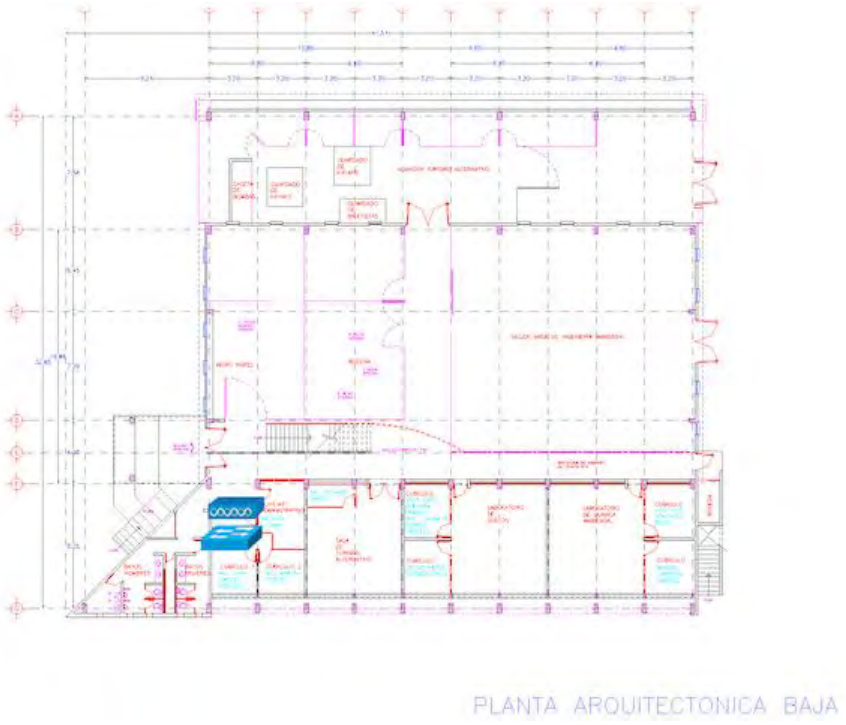

Figura 12. Ubicación física de los dispositivos dentro del edificio F

Ubicación física de los dispositivos dentro del edificio G

Figura 13. Ubicación física de los dispositivos dentro del edificio G

Ubicación de los dispositivos dentro del edificio H (Planta Baja)

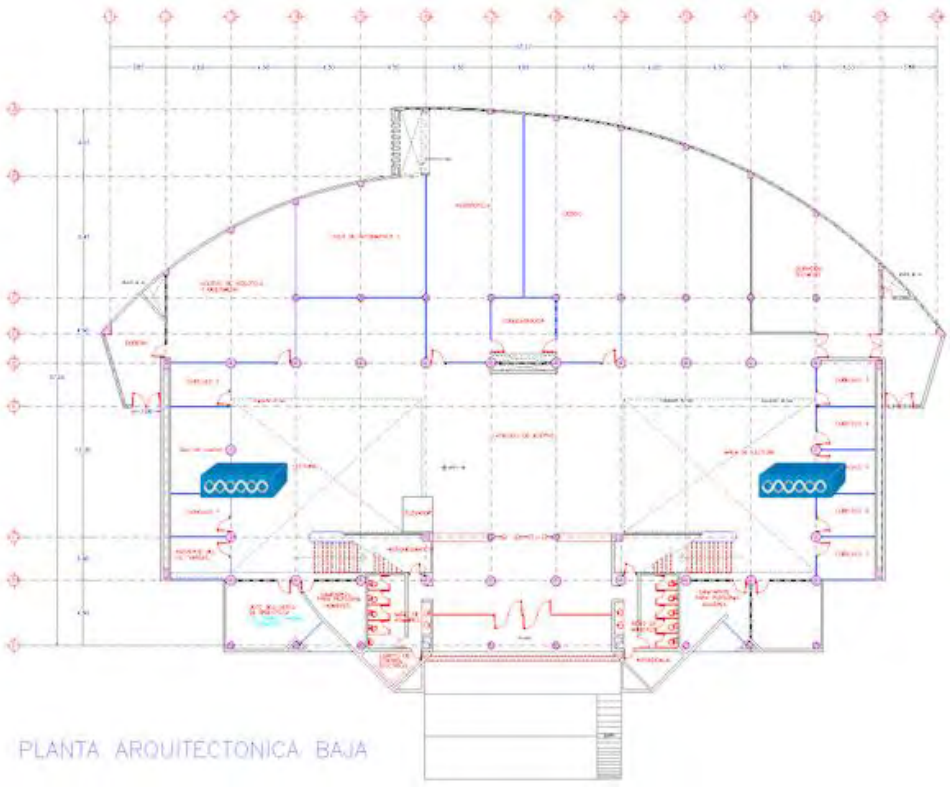

Figura 14. Ubicación física de los dispositivos dentro del edificio H (Planta Baja)

Ubicación de los dispositivos dentro del edificio H (Planta Alta)

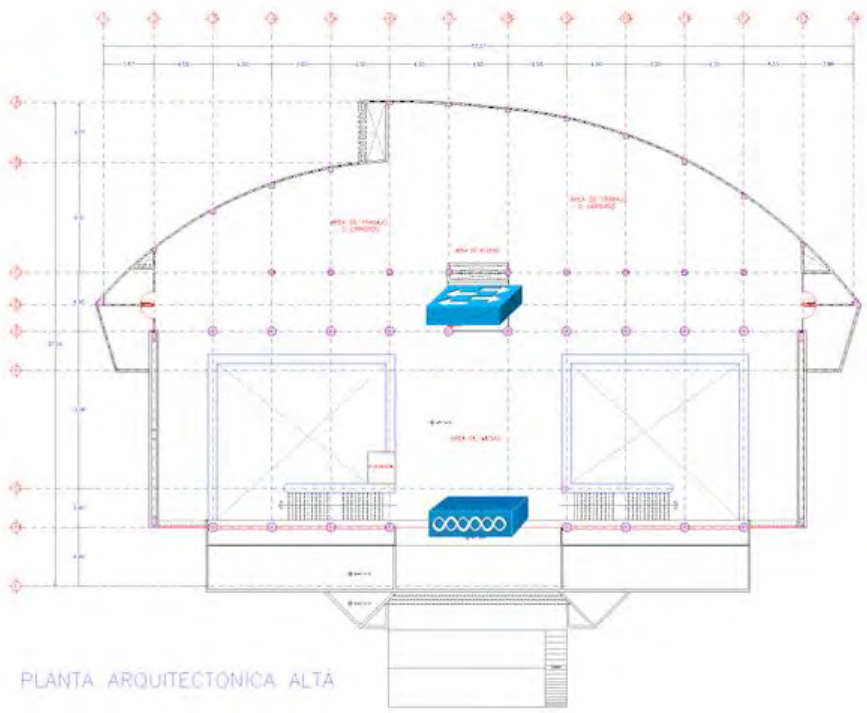

Figura 15. Ubicación física de los dispositivos dentro del edificio H (Planta Alta)

Ubicación de los dispositivos dentro del edificio J

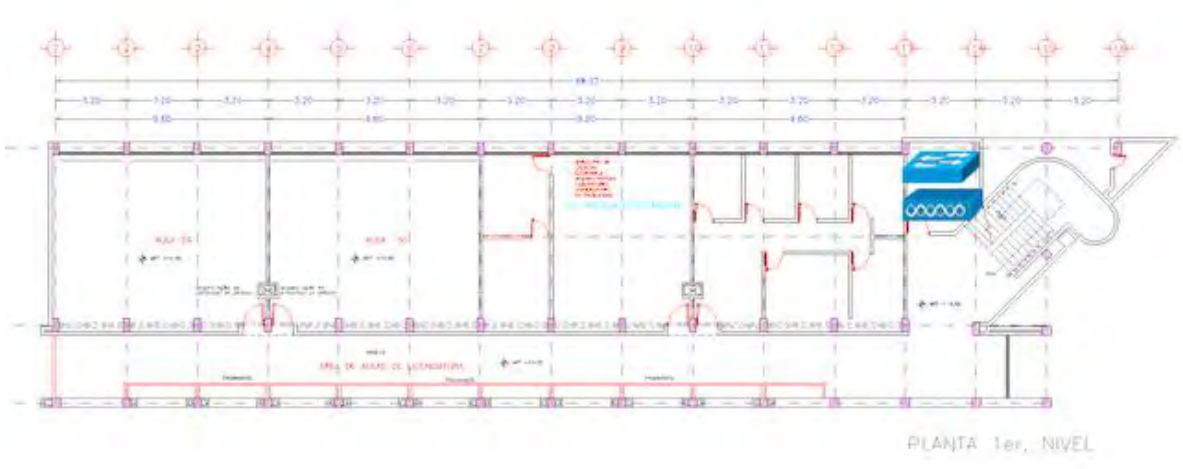

Figura 16. Ubicación física de los dispositivos dentro del edificio J

Ubicación de los dispositivos dentro del edificio K (Planta Baja)

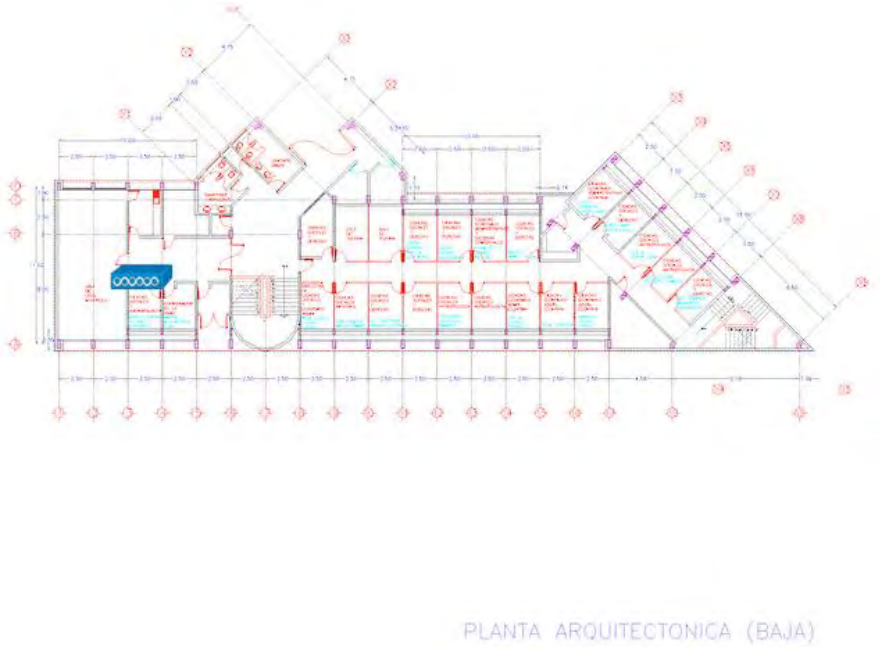

Figura 17. Ubicación física de los dispositivos dentro del edificio K (Planta Baja)

Ubicación de los dispositivos dentro del edificio K (Planta Alta)

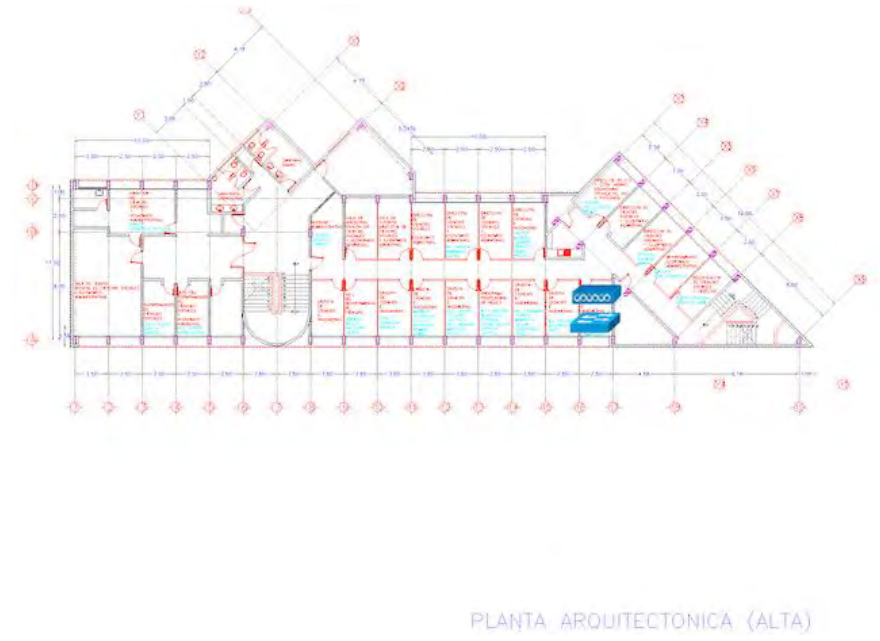

Figura 18. Ubicación física de los dispositivos dentro del edificio K (Planta Alta)

Ubicación de los dispositivos dentro del edificio L (Planta Baja)

Figura 19. Ubicación física de los dispositivos dentro del edificio L (Planta Baja)

Ubicación de los dispositivos dentro del edificio L (Planta Alta)

Figura 20. Ubicación física de los dispositivos dentro del edificio L (Planta Alta)

Ubicación de los dispositivos dentro del edificio M

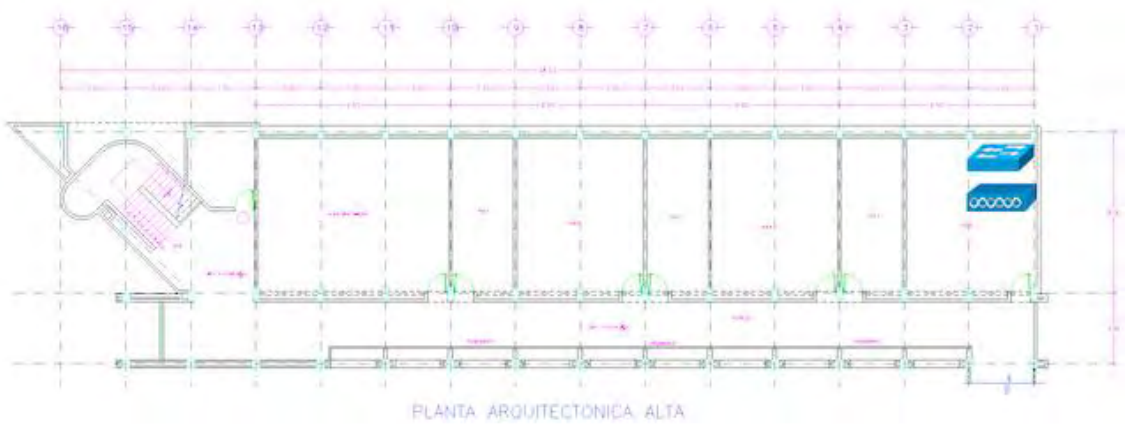

Figura 21. Ubicación física de los dispositivos dentro del edificio M

Ubicación de los dispositivos dentro del edificio V (Planta Baja)

Figura 22. Ubicación física de los dispositivos dentro del edificio V (Planta Baja)

Ubicación de los dispositivos dentro del edificio V (Planta Alta)

Figura 23. Ubicación física de los dispositivos dentro del edificio V (Planta Alta)

Ubicación de los access point alrededor de la UQRoo unidad Chetumal

Figura 24. Ubicación física de los access point en la UQRoo unidad Chetumal

Ubicación física de los switches alrededor de la UQRoo unidad Chetumal

Figura 25. Ubicación física de los switches en la UQRoo unidad Chetumal

Ubicación física de los routers en la UQRoo unidad Chetumal

Figura 26. Ubicación física de routers en la UQRoo unidad Chetumal

Ubicación física de los servidores en la UQRoo unidad Chetumal

Figura 27. Ubicación de los servidores en la UQRoo unidad Chetumal

En la Tabla 4 se presenta el total de dispositivos de red a monitorear ubicados alrededor de la Universidad de Quintana Roo.

Tabla 4. Total de dispositivos a monitorear

Dispositivo	Nombre	Total
	Access Point	21
	Switches	12
	Servidores	1
	Routers	1

Diagramas físicos de red

Diagrama físico general de la UQRoo unidad Chetumal

Conexión entre dispositivos: Cable UTP Cat 5e y UTP Cat 6.
Conexión entre edificios: Cable de fibra óptica multimodo.

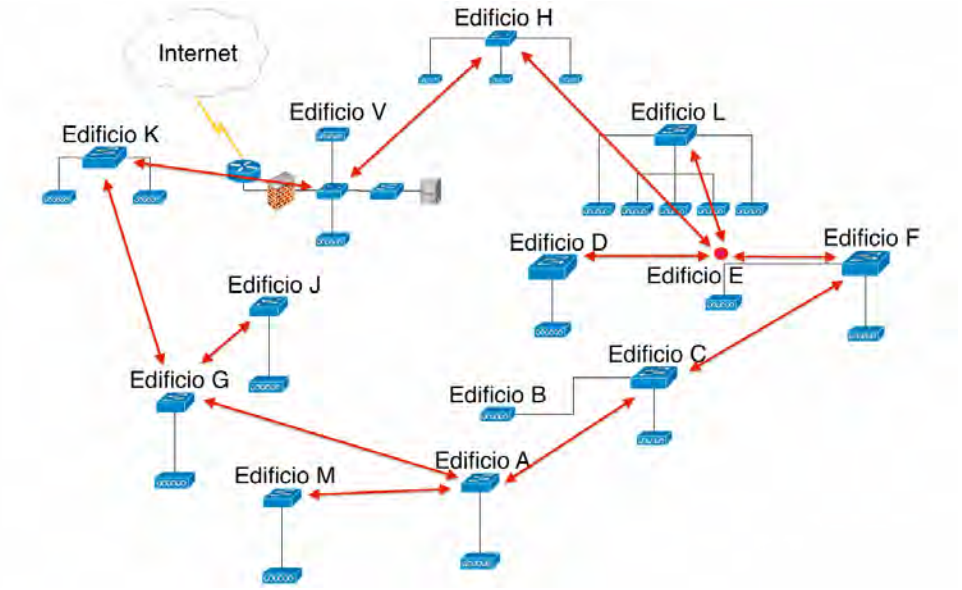

Figura 28. Diagrama físico de la UQRoo unidad Chetumal

Diagrama físico del edificio A

El diagrama físico del edificio A, consta de 1 switch marca Enterasys modelo E7 con 4 tarjetas, una tarjeta de enlaces con 6 puertos Gigabit de fibra óptica, y tres tarjetas con 48 puertos Fast Ethernet. Así también 1 access point marca UBNT modelo NanoStation2. La conexión entre dispositivos es mediante cable UTP Cat 5e y la conexión entre edificios es por cable de fibra óptica multimodo (ver Figura 29).

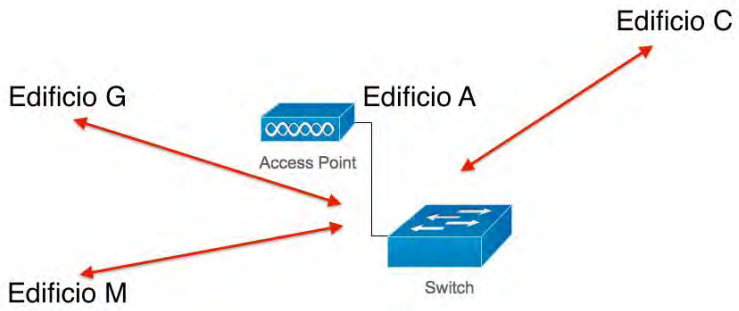

Figura 29. Diagrama físico del edificio A

Diagrama físico de los edificios B y C

El diagrama físico de los edificios B y C se compone de 1 switch marca Cisco modelo 3750 G con 52 puertos Gigabit Ethernet. Así también 2 access point, uno marca UBNT modelo NanoStation2 en el edificio B y otro marca Linksys modelo WAP54G en el edificio C, éste último no soporta el protocolo SNMP. La conexión entre dispositivos es mediante cable UTP Cat 5e y la conexión entre edificios es por cable de fibra óptica multimodo (ver Figura 30).

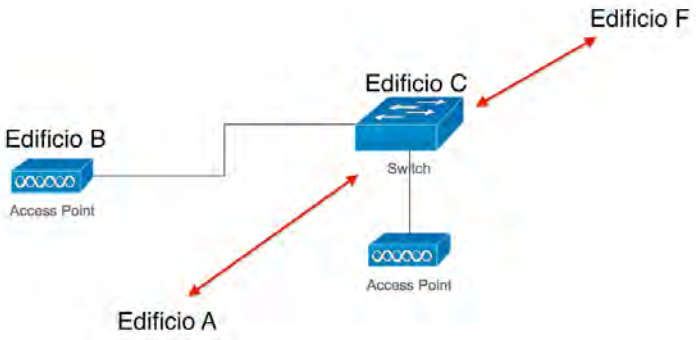

Figura 30. Diagrama físico de los edificios B y C

Diagrama físico del edificio D

El diagrama físico del edificio D está compuesto por 1 switch marca Enterasys modelo Matrix E7 con 4 tarjetas, una tarjeta de enlaces con 2 puertos Gigabit de fibra óptica y 24 puertos Fast Ethernet, dos tarjetas con 48 puertos Fast Ethernet, y una tarjeta más con 48 puertos Ethernet. También cuenta con 1 access point marca UBNT modelo NanoStation2. La conexión entre dispositivos es mediante cable UTP Cat 5e y la conexión entre edificios es por cable de fibra óptica multimodo (ver Figura 31).

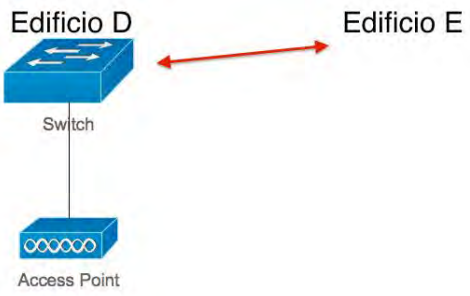

Figura 31. Diagrama físico del edificio D

Diagrama físico de los edificios E y F

El diagrama físico de los edificios E y F se conforma de 1 switch marca Enterasys modelo Matrix E7 con 2 tarjetas, una tarjeta de enlaces con 6 puertos Gigabit de fibra óptica y otra tarjeta con 48 puertos Fast Ethernet. Cuenta también con 2 access point, uno en el edificio E marca TRENDnet modelo TEW-637AP y otro en el edificio F marca Proxim modelo AP-2000, ambos access point no soportan el protocolo SNMP. La conexión entre dispositivos es mediante cable UTP Cat 5e y la conexión entre edificios es por cable de fibra óptica multimodo (ver Figura 32).

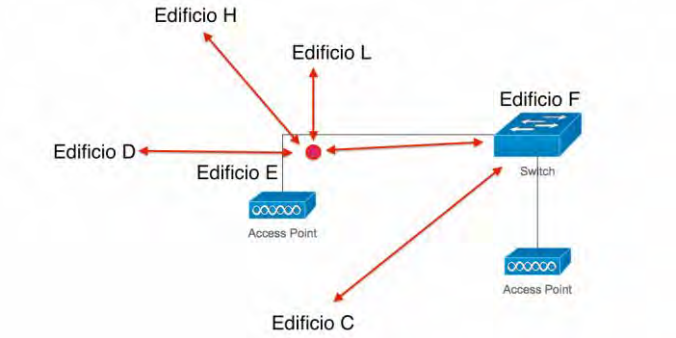

Figura 32. Diagrama físico de los edificios E y F

Diagrama físico del edificio G

El diagrama físico del edificio G, consta de 1 switch marca Enterasys modelo SmartSwitch 6000 con 2 puertos Gigabit de fibra óptica y 24 puertos Fast Ethernet. Además, 1 access point marca Proxim modelo AP-4000N, éste access point no soporta el protocolo SNMP. La conexón entre dispositivos es mediante cable UTP Cat 5e y la conexión entre edificios es por cable de fibra óptica multimodo (ver Figura 33).

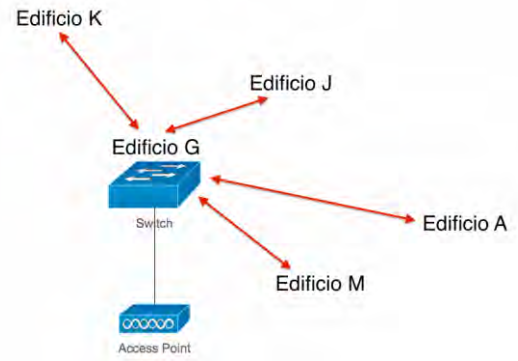

Figura 33. Diagrama físico del edificio G

Diagrama físico del edificio H

El diagrama físico del edificio H se compone de 1 switch marca Enterasys modelo E7 con 4 tarjetas, una tarjeta de enlaces con 2 puertos Gigabit de fibra óptica y 24 puertos Fast Ethernet, dos tarjetas con 48 puertos Fast Ethernet, y otra tarjeta más de enlaces con 6 puertos Gigabit de fibra óptica. Además, tres access point, uno marca Linksys modelo WAP54G y otros dos marca Proxim modelo AP-4000M, éstos access point no soportan el protocolo SNMP. La conexión entre dispositivos es mediante cable UTP Cat 5e y la conexión entre edificios es por cable de fibra óptica multimodo (ver Figura 34).

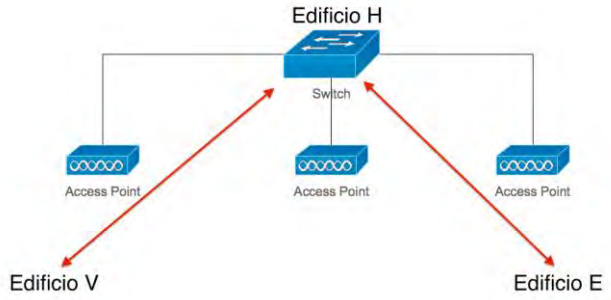

Figura 34. Diagrama físico del edificio H

Diagrama físico del edificio K

El diagrama físico del edificio K está conformado por 1 switch marca Enterasys modelo Matrix E7 con 3 tarjetas, una tarjeta de enlaces con 6 puertos Gigabit de fibra óptica, y dos tarjetas con 48 puertos Fast Ethernet. Además, 2 access point marca Enterasys modelo RBT3K-AG, ambos access point tampoco soportan el protocolo SNMP. La conexión entre dispositivos es mediante cableado UTP Cat 5e y la conexión entre edificios es por cable de fibra óptica multimodo (ver Figura 35).

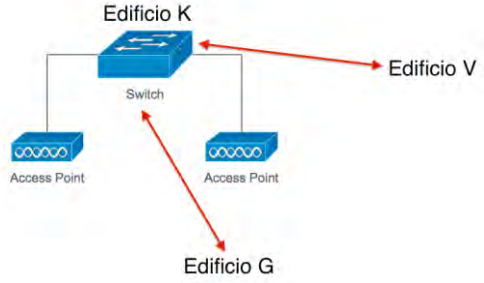

Figura 35. Diagrama físico del edificio K

Diagrama físico del edificio J

El diagrama físico del edificio J se conforma por 1 switch marca Cisco modelo 2960 G con 48 puertos Gigabit Ethernet. Así también 1 access point marca UBNT modelo NanoStation2. La conexión entre dispositivos es mediante cable UTP Cat 5e y la conexión entre edificios es por cable de fibra óptica multimodo (ver Figura 36).

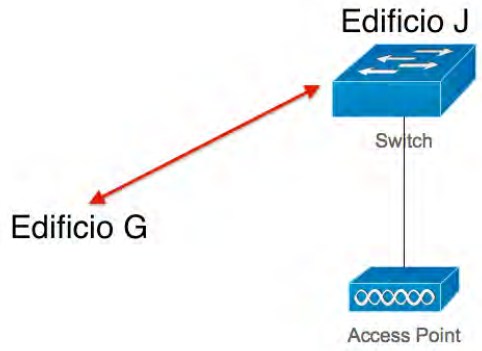

Figura 36. Diagrama físico del edificio J

Diagrama físico del edificio L

El diagrama físico del edificio L está compuesto por 1 switch marca Enterasys modelo Matrix S8 con 2 tarjetas, una tarjeta con 60 puertos Gigabit Ethernet y otra tarjeta más con 48 puertos Gigabit Ethernet. Además, 5 access point marca Enterasys modelo RBT-4102C. La conexión entre dispositivos es mediante cable UTP Cat 6 y la conexón entre edificios es por cable de fibra óptica multimodo (ver Figura 37).

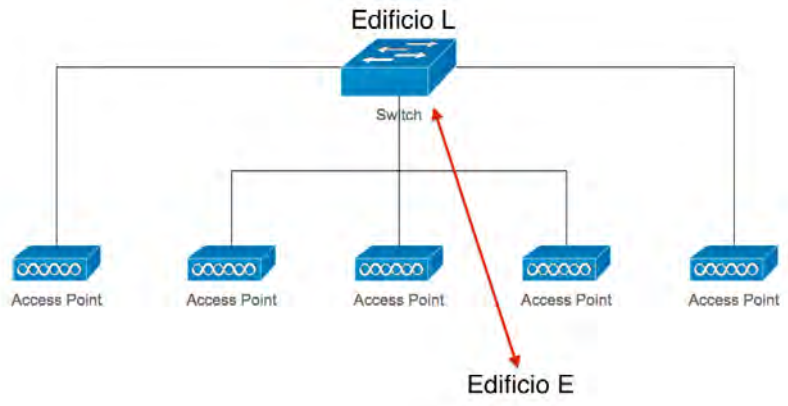

Figura 37. Diagrama físico del edificio L

Diagrama físico del edificio M

El diagrama físico del edificio M se compone de 1 switch Cisco 2960 S con 52 puertos Gigabit Ethernet. También cuenta con 1 access point marca UBNT modelo NanoStation2. La conexión entre dispositivos es mediante cable UTP Cat 5e y la conexión entre edificios es por cable de fibra óptica multimodo (ver Figura 38).

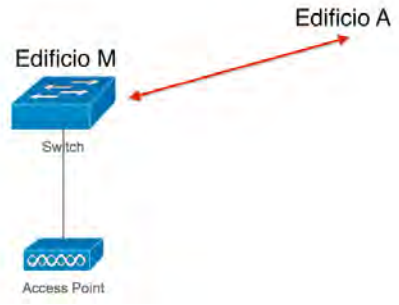

Figura 38. Diagrama físico del edificio M

Diagrama físico del edificio V

El diagrama físico del edificio V está conformado por 1 switch marca Enterasys modelo N7 que incorpora 2 tarjetas, una con 48 puertos Gigabit Ethernet y otra con 12 puertos de fibra óptica, también incorpora 1 switch marca Cisco modelo 2950 con 24 puertos Fast Ethernet. Además, 1 router marca Cisco modelo 2911 con 3 puertos Gigabit Ethernet, 2 access point, uno marca Linksys modelo WAP4400N y otro marca UBNT modelo NanoStation2. La conexión entre dispositivos es mediante cable UTP Cat 6 y la conexión entre edificios es por cable de fibra óptica ı

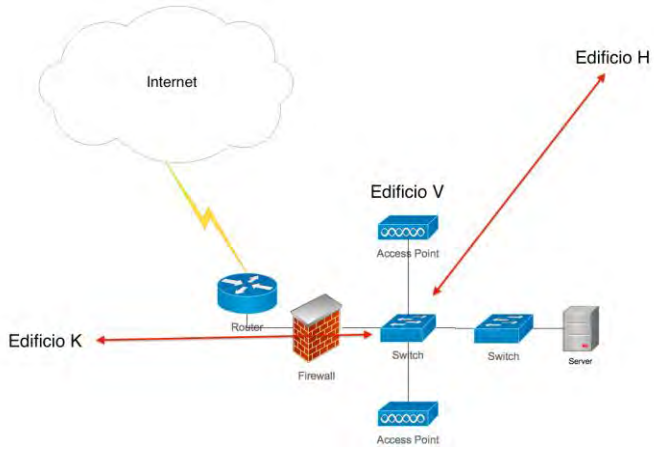

Figura 39. Diagrama físico del edificio V

Dispositivos y servicios a monitorear

El criterio de monitoreo es para saber el por qué sería importante monitorear cada uno de los dispositivos.

Monitoreo de *access point*: Los *access point* son el medio principal de acceso para los usuarios que en su mayoría son estudiantes, mantener su correcto funcionamiento garantiza la movilidad necesaria para realizar actividades académicas desde cualquier parte de la UQRoo, por lo tanto de estos dispositivos únicamente se necesita conocer si están activos.

Monitoreo de *switches*: Los *switches* son pieza fundamental para la conectividad en la red de datos universitaria, cualquier problema con los switches impacta directamente a las actividades administrativas o academicas de los estudiantes, profesores o administrativos de la UQRoo, debido a su importancia es necesario monitorear si están activos, la carga del CPU, memoria RAM, los puertos de red activos y el ancho de banda en cada uno de esos puertos.

Monitoreo de *routers*: El *router* es la última línea, es la frontera entre la red universitaria e Internet, un problema con el router significaría perder el acceso a Internet en toda la red universitaria, por lo tanto, al igual que a los switches es importante monitorear su actividad, la carga del CPU, la memoria RAM, los puertos de red activos y el ancho de banda de cada uno de esos puertos.

Monitoreo de servidores: Muchos de los servicios que utilizan los estudiantes, profesores y administrativos de la red universitaria se ejecutan desde servidores, mantener el correcto funcionamiento de los mismos garantiza la realización de las actividades académicas y administrativas sin contratiempos. Debido a la gran demanda de los usuarios, es necesario monitorear su disponibilidad, el tiempo de actividad, la memoria RAM, la carga del CPU, el espacio en disco duro, los servicios de red, las interfaces de red y el ancho de banda en dichas interfaces.

En la Tabla 5 se encuentra una lista de los dispositivos con los servicios a monitorear en cada uno de ellos.

Tabla 5. Dispositivos y servicios a monitorear

Dispositivo	Servicios a monitorear
Access Point	Disponibilidad en la red (PING) Tiempo activo
Switches	Disponibilidad en la red (PING) Tiempo activo Memoria RAM Carga del CPU Puertos activos Ancho de banda en cada puerto
Routers	Disponibilidad en la red (PING) Tiempo activo Memoria RAM Carga del CPU Puertos activos Ancho de banda en cada puerto
Servidores	Disponibilidad en la red (PING) Tiempo activo Memoria RAM Carga del CPU Espacio en disco duro Servicios de red Interfaces de red Ancho de banda en cada interfaz

Elección de la herramienta de monitoreo

Despues de haber determinado los dispositivos y los servicios a monitorear, se eligió la herramienta de monitoreo a utilizar, para ello se investigó cada una de las tres herramientas sugeridas por el administrador de la red universitaria.

La investigación derivó en una tabla comparativa (ver Tabla 6) que se realizó visitando las páginas Web oficiales de cada herramienta, así como foros, tutoriales en línea y redes sociales, donde los puntos a comparar fueron:

- ✓ Open source
- ✓ Precio
- ✓ Límites
- ✓ Facilidad de instalación
- ✓ Facilidad de uso
- ✓ Soporte

Tabla 6. Comparativa entre las herramientas de monitoreo

Nombre	Versión	Open Source	Precio	Limitado	Facilidad de instalación	Facilidad de uso	Soporte
Nagios	Core	✔	gratis	✘	✘	✘	✘
	XI Free	✔	gratis	✔	✔	✔	✔
	XI Enterprise	✔	De 1500 – 4000 dólares	✘	✔	✔	✔
Pandora FMS	Demo	✔	gratis	✔	✔	✔	✘
	Enterprise	✘	Depende al # de agentes	✘	✔	✔	✔
Zenoss	Core	✔	gratis	✘	✔	✔	✘
	Core Enterprise	✘	Enviar solicitud	✘	✔	✔	✔

Si nos enfocamos en las versiones gratuitas Nagios XI Free parece la mejor opción, es gratuita, facil de instalar y utilizar, además cuenta con soporte técnico por parte de Nagios, pero tiene un detalle, la versión XI Free está limitada para monitorear 10 equipos, por lo que queda descartada.

Quizá Nagios Core no cumpla con la mayoría de los requisitos que se consideraron para evaluar la herramienta, pero durante la etapa de investigación

se encontraron razones suficientes para implementar esta herramienta (ver Tabla 7).

Tabla 7. Razones para elegir Nagios

Razón	Descripción
Es un estándar	Nagios fue la primera herramienta de monitoreo, muchas otras herramientas se han basado en su arquitectura para realizar la misma tarea.
Presencia en el mercado mundial	Muchas compañías importantes utilizan Nagios como herramienta para monitorear sus dispositivos y servicios de red, entre ellas se encuentran at&t, Linksys, AOL, McAfee, Sony, Toshiba y muchas más.
Recomendaciones	En todos los foros visitados siempre hay gente que recomienda esta herramienta y en la mayoría siempre tenía el mayor número de recomendaciones.
Comunidad	Nagios tiene una enorme comunidad de usuarios que ayudan a dar soporte en foros, redes sociales, etc.
Plugins	Debido a la extensa comunidad de usuarios, Nagios Core cuenta con cientos de plugins disponibles para instalar en la versión gratuita, por lo que es una herramienta muy flexible.

Por lo tanto, para la implementación de una estación de gestión, se utilizó como sistema base la distribución GNU/Linux Debian 7.1 en una PC de escritorio y como herramienta de monitoreo Nagios Core en su versión 3.5.1.

Nagios Core

Nagios es un poderoso sistema de monitoreo que permite a las organizaciones identificar y resolver problemas en su infraestructura de red antes de que afecten a los procesos que en ella se encuentran (Nagios).

Características de Nagios Core

- ✓ Gestión de servicios (SMTP, POP3, HTTP, NNTP, PING, etc.).
- ✓ Monitorización de recursos de sistemas.
- ✓ Diseño simple de plugins para que podamos crear los nuestros a nuestras necesidades específicas.
- ✓ Habilidad de definir una jerarquía de hosts usando la opción parent.
- ✓ Notificaciones a contactos cuando un servicio o host tenga problemas y puedan resolverlo (email, pager o definido por el usuario).
- ✓ Gestión de servicios pasivos generados por aplicaciones o comandos externos (servicios pasivos).
- ✓ Monitorización de factores ambientales a través de sondas físicas (temperatura, humedad relativa, luminosidad, líneas de tensión, etc.).
- ✓ Arquitectura simple de integración que permita a los usuarios desarrollar fácilmente sus propios agentes de chequeo de servicios y recursos.
- ✓ Escalado y distribución de servicios, recursos y nodos gestionados por grupos de contacto.
- ✓ Definición de acciones reactivas que permitan solventar un problema de forma inmediata.
- ✓ Soporte de arquitecturas de servidor redundantes y distribuidas.
- ✓ Interfaz de comandos externos (triggers, web o terceras aplicaciones) que permitan mo “ -the- ”
- ✓ Programación de intervalos de tiempo sin notificaciones
- ✓ Visión rápida y sencilla de elementos gestionados.
- ✓ Portal web que permite consultar el estado de los elementos gestionados, las notificaciones realizadas, los problemas acontecidos, el estado de los servidores, etc.
- ✓ Definición de usuarios de lectura y administración del portal web.

Ventajas y desventajas de Nagios Core

Utilizar una herramienta como Nagios Core tiene sus ventajas y desventajas, pero está claro que son muchísimas más ventajas, las cuales se listan en la Tabla 8.

Tabla 8. Ventajas y desventajas de Nagios Core

Ventajas	Desventajas
Gratuita	Configuración manual
Escalable	
Flexible	
Permite identificar problemas	
Permite resolver problemas	
Permite planificar acciones y estrategias	
Ahorra tiempo	
Disminuye costos	

Estrategias de uso de Nagios

Algunas implementaciones que pueden realizarse con el uso de Nagios son:

- ✓ Plan de mejoras de infraestructura antes de que los sistemas fallen
- ✓ Responder a los distintos cuestionamientos a la primera señal de un problema.
- ✓ Reparar automáticamente los problemas cuando se detectan.
- ✓ Supervisar toda la infraestructura y los procesos de negocio.

Instalación y configuración de Nagios Core 3.5.1

La instalación y configuración de la herramienta de monitoreo se encuentra en el Anexo A de este mismo documento, y en el Anexo B, la instalación y configuración del agente SNMP en diversos sistemas operativos.

La configuración de los equipos fue con la ayuda de una herramienta desarrollada para facilitar y agilizar la configuración de Nagios Core. Los detalles de ésta herramienta se encuentran en el Anexo F.

CAPÍTULO 4

CAPÍTULO 4 – Resultados experimentales

Laboratorio

La fase de pruebas consistió en aprender el funcionamiento de Nagios Core en conjunto con el protocolo SNMP para monitorear los dispositivos más comunes que componen una red, *access point*, *switches*, servidores y routers, en un mini-laboratorio como ambiente controlado.

El laboratorio ' marca HP, una funcionando como estación de gestión y la otra como servidor ejecutando el agente SNMP. Además, también se contó con un switch Catalyst 2950, un switch Catalyst 2960 y un router 2800, todos de la marca Cisco Systems (ver Figura 44).

Figura 40. Mini-laboratorio de pruebas

Las características de la PC que funcionaba como estación de gestión Nagios son:

- Procesador Intel Core 2 CPU 6300 a 1.86 GHz x 2
- Memoria RAM 1GB
- Disco duro de 250 GB
- Sistema Operativo GNU/Linux Debian 7.

Las características de la PC que funcionaba como servidor fueron las siguientes:

- Procesador Intel Pentium 4 CPU a 3.00 GHz
- Memoria RAM 1286 MB
- Disco duro de 160 GB
- Sistema Operativo Linux Mint Debian Edition

Resultados

En las pruebas se utilizó SNMP versión 2, todos los dispositivos mencionados anteriormente fueron monitoreados con éxito, algunos en mayor o menor medida. Los resultados de las pruebas son las siguientes:

En los servidores basados en Unix (GNU/Linux y Solaris) se logró monitorear el tiempo de actividad del sistema, la carga del CPU, cantidad de memoria RAM, cantidad de memoria SWAP, espacio en el disco duro, así como el estado de las interfaces de red (UP, DOWN).

En los servidores basados en Microsoft Windows ®, únicamente se pudo monitorear el tiempo de actividad del sistema, ya que el agente SNMP de Windows es muy limitado debido a que Microsoft implementa su propio protocolo de monitoreo, el protocolo WMI.

En los switches, se pudo monitorear objetos como el tiempo de actividad del sistema y el e “ ” “G ”

(UP, DOWN). Los demás parámetros como la carga del CPU o cantidad de RAM, etc, no se encontró la forma de monitorearlos, posiblemente porque Cisco System dispone de una MIB diferente, propia para sus dispositivos.

Aunque los switches son del mismo fabricante, hubo una ligera diferencia a la hora de monitorear las interfaces, En los switches Catalyst 2950 el OID para monitorear el puerto FastEthernet 1 es .1.3.6.1.2.1.2.2.1.8.1 y en los Catalyst 2960 el OID correcto para el puerto FastEthernet 1 es .1.3.6.1.2.1.2.2.1.8.10001.

En el caso de los routers se logró monitorear el tiempo de actividad del sistema, el “ ” “S ” W l caso de los demás objetos, sucedió lo mismo que con los switches.

Algo que no se pudo monitorear en los dispositivos mediante el protocolo SNMP fueron los servicios de red (FTP, SSH, HTTP, DHCP, etc), tampoco el ancho de banda en cada interfaz de red, por lo que Nagios hace uso de otros plugins para complementar el monitoreo.

Estos resultados son independientes de la versión de SNMP utilizada, ya que el tipo de versión es únicamente para cuestiones de autenticación entre la estación de gestión y el agente.

Como en toda fase de pruebas, los errores siempre están presentes, ya sea por la inexperiencia o errores involuntarios al escribir, y son parte del aprendizaje. Cuando estos errores se produzcan, Nagios lo hará saber a través de un novedoso sistema de notificaciones.

Alertas para host

En la Figura 41 “ ” (ACTIVO), esto indica que el host está activo y funcionando con normalidad. El color de la notificación es verde y el status OK.

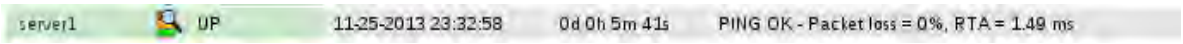

Figura 41. Host activo

Caso contrario en la Figura 42, donde se aprecia que el estado del host es " W " (CAÍDO), esto quiere decir que el host está fue de alcance, muy posiblemente se encuentre apagado. El color de la alerta es rojo y el status CRITICAL.

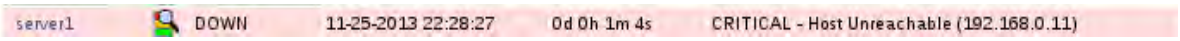

Figura 42. Host inalcanzable

Alertas para servicios

La primera vez que se configura un servicio en Nagios Core, éste aparece en color gris indicando que está "PENDING" significa que el servicio se encuentra en espera de ser verificado (ver Figura 43).

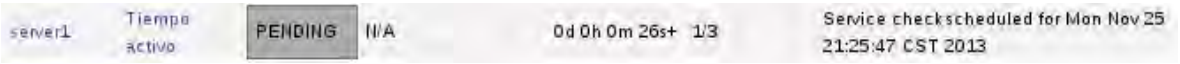

Figura 43. Servicio pendiente

La configuración inicial de Nagios Core 3.5.1 trae un error en el comando que se utiliza para hacer las consultas SNMP, si no se arregla este comando, puede que " o OIDs sp " Figura 44), aunque el OID esté especificado de manera correcta.

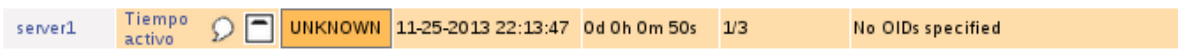

Figura 44. Alerta: Error en comando

Esto se arregla “ ” y agregando el parámetro “- ” argumento 1, de la siguiente manera:

check_line $USER1$/check_snmp –H $HOSTADDRESS$ -o $ARG1$

Cuando de verdad se trata de un OID incorrecto, Nagios manda una alerta color “ : k ” (ver Figura 45).

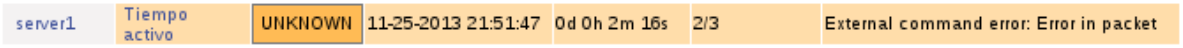

Figura 45. Alerta: OID incorrecto

Un último caso de error podría darse cuando el agente SNMP esté mal configurado, la alerta de este error también es de color naranja y en el status se “ : : …” (ver Figura 46).

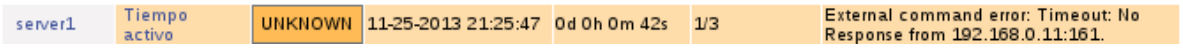

Figura 46. Alerta: Agente mal configurado

Reportes

Si algo no se puede medir, entonces no se puede controlar. Los reportes son parte fundamental en el método de monitoreo, porque reflejan aspectos estadísticos de los dispositivos, aspectos que son importantes para la toma de decisiones y mejorar las fallas.

Nagios Core permite generar diferentes tipos de reportes, que se encuentran en la “ ” W

(ver Figura 47).

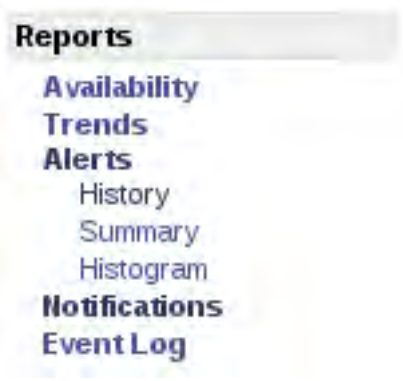

Figura 47. Tipos de Reportes en Nagios Core 3.5.1

Los reportes solicitados por el administrador de red fueron: Reporte de disponibilidad de los dispositivos y Reporte de alertas. Estos reportes se generaron con datos recabados durante un periodo de monitoreo que duró un mes, del 26 de octubre al 26 de noviembre de 2013.

En el reporte de disponibilidad se encuentran los porcentajes de tiempo que han estado funcionando los dispositivos (ver Figura 48).

All Hosts

10-26-2013 14:59:35 to 11-26-2013 13:59:35
Duration: 31d 0h 0m 0s

Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
CIG	23.707% (23.707%)	76.293% (76.293%)	0.000% (0.000%)	0.000%
Computo	14.784% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	85.216%
Edificio-J	4.945% (33.446%)	9.839% (66.554%)	0.000% (0.000%)	85.216%
Edificio-M	14.784% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	85.216%
Enterasys-N7	11.558% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	88.442%
Matrix-S8	14.784% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	85.216%
Ordenamiento	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Posgrado-L	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Redes1-AP	14.784% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	85.216%
Redes2-AP	14.784% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	85.216%
Sistemas	14.784% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	85.216%
T1-Enlaces-D	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
T1-Enlaces01	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
T1-Enlaces01-Biblioteca	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
T1-Enlaces01-Ing	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
T1-Posgrado	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
T2-Biblio	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
T2-EdificioD	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
T2-EdificioK	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
T2-Ingenierias	94.176% (94.176%)	5.824% (5.824%)	0.000% (0.000%)	0.000%
T2-Rectoria	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
T3-Biblio	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
T3-EdificioD	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
T3-EdificioK	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
T3-Rectoria	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
T4-EdificioD	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
T4-Enlaces02-Ing	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
T4-Rectoria	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
T5-Enlaces02	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
UBNT1	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
UBNT2	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
UBNT3	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
UBNT4	90.172% (90.172%)	9.828% (9.828%)	0.000% (0.000%)	0.000%
UBNT5	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
localhost	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Average	77.522% (95.471%)	2.908% (4.529%)	0.000% (0.000%)	19.570%

Figura 48. Reporte de disponibilidad

“ ”

100% han estado funcionando desde que se comenzó con el monitoreo. Cabe destacar que algunos host fueron agregados tiempo después, por lo que no tienen 100% “ ” esto no quiere decir que hayan estado fuera de “ ”

Los host Edificio-J, T2-Ingenierias y UBNT4 presentan un ligero porcentaje en “ w ” ncionamiento por un lapso leve de tiempo, y fue debido a un apagón en toda la UQRoo unidad Chetumal.

G “ w ” ven a encender al día siguiente.

Todos los dispositivos listados en el reporte de disponibilidad generan alertas, ya sean alertas de host o alertas de servicios. En la Figura 49 se muestra el reporte del total de alertas generadas por los dispositivos y servicios.

Alert Totals

10-26-2013 14:58:11 to 11-26-2013 13:58:11
Duration: 31d 0h 0m 0s

Overall Totals

Host Alerts				Service Alerts			
State	Soft Alerts	Hard Alerts	Total Alerts	State	Soft Alerts	Hard Alerts	Total Alerts
UP	107	25	132	OK	535	1278	1813
DOWN	316	22	338	WARNING	597	181	778
UNREACHABLE	0	0	0	UNKNOWN	2053	1019	3072
All States	423	47	**470**	CRITICAL	107	41	148
				All States	3292	2519	**5811**

Figura 49. Reporte total de alertas

Así también, se puede generar un reporte de alertas donde se muestran los 25 host o servicios que producen más alertas (ver Figura 50).

Top Alert Producers

10-26-2013 14:55:49 to 11-26-2013 13:55:49
Duration: 31d 0h 0m 0s

Displaying top 25 of 781 total matching alert producers

Rank	Producer Type	Host	Service	Total Alerts
#1	Host	CIG	N/A	229
#2	Service	UBNT5	PING	211
#3	Service	T3-Biblio	FTM Backplane Port 1 bandwidth	118
#4	Service	T1-Enlaces01	Gigabit Port 5 bandwidth	109
#5	Service	T1-Enlaces01-Biblioteca	FTM Backplane Port 1 bandwidth	107
#6	Service	T5-Enlaces02	SmartTrunk Aggregator 1 bandwidth	90
#7	Service	Enterasys-N7	Tarjeta 2 - Aggregator Port 01 bandwidth	76
#8	Service	T1-Enlaces01-Ing	Gigabit Port 5 bandwidth	67
#9	Host	UBNT5	N/A	66
#10	Service	Enterasys-N7	Tarjeta 1 - Gigabit Ethernet 48 bandwidth	56
#11	Service	CIG	Tiempo activo	49
#12	Service	CIG	PING	49
#13	Service	Enterasys-N7	Tarjeta 1 - Gigabit Ethernet 38 bandwidth	46
#14	Service	T4-Enlaces02-Ing	Gigabit Port 03 bandwidth	40
#15	Service	T4-Enlaces02-Ing	Gigabit Port 04 bandwidth	40
#16	Service	T2-Biblio	FTM Backplane Port 1 bandwidth	35
#17	Service	T4-Rectoria	FTM Backplane Port 1 bandwidth	33
#18	Service	Enterasys-N7	Tarjeta 2 - Aggregator Port 02 bandwidth	31
#19	Service	Sistemas	FastEthernet 18 bandwidth	30
#20	Service	T5-Enlaces02	Gigabit Port 1 bandwidth	29
#21	Service	UBNT5	Tiempo activo	26
#22	Service	Sistemas	FastEthernet 24 bandwidth	25
#23	Service	T5-Enlaces02	FTM Backplane Port 1 bandwidth	24
#24	Service	T4-Rectoria	Fast Ethernet 06 bandwidth	24
#25	Service	T2-Ingenierias	FTM Backplane Port 1 bandwidth	22

Figura 50. Top 25 de los host y servicios con más alertas

Como se puede observar, la mayoría de las alertas se producen en los servicios que monitorean el ancho de banda de las interfaces de red, esto se debe a que durante el transcurso del día se generan picos de tráfico de red en determinados puertos.

CAPÍTULO 5

CAPÍTULO 5 – Conclusiones

El proceso de gestión de una red no es sencillo y se vuelve aún más complejo si se compone de numerosos dispositivos y servicios, siendo el la persona responsable encargada de monitorear, detectar y corregir los fallos que pudieran presentarse en la red día a día.

SNMP es un protocolo que sirve para gestionar los dispositivos y servicios de una red, y su funcionamiento se basa en el concepto gestor-agente, permitiendo que múltiples herramientas lo puedan utilizar con las cuales el administrador de red puede y se recomienda que lo utilice, para llevar a cabo una mejor gestión de la red.

Una de estas herramientas es Nagios Core, un poderoso sistema de monitoreo *open source* que permite a las organizaciones identificar y resolver problemas en su red antes de que afecten a los procesos que en ella se encuentran. Esto lo hace informando al administrador de red mediante un novedoso sistema de notificaciones a través de su interfaz Web o también mediante el envío de correo electrónico.

En la Universidad de Quintana Roo no existía un programa de monitoreo previo, por lo tanto, éste trabajo de tesis es un primer esfuerzo para llevar una mejor gestión de la red, facilitando un método y una herramienta de monitoreo, cuyos resultados irán variando conforme la red universitaria vaya creciendo, esto debido a que las redes modernas son dinámicas.

La implementación de una estación de gestión con Nagios Core en el Centro de Tecnologías de la Información y Comunicación (CTIC) de la Universidad de Quintana Roo benefició enormemente al administrador de red mejorando el monitoreo y la gestión de los dispositivos, al notificarle en tiempo real distintos eventos que se llevan a cabo con los dispositivos de la red universitaria.

Ahora bien, ya se han mencionado los beneficios de utilizar Nagios y SNMP en la gestión de red, pero no todo es miel sobre hojuelas, a ambos se les detectaron puntos débiles que podrían ser un problema o volver insegura la gestión de la red.

Aunque Nagios Core es *open source*, es una herramienta de gestión muy completa en cuanto a monitoreo, pero que en lo que se refiere a facilidad de configuración es muy limitada, por lo que el desarrollo de una aplicación que agilizara la configuración de los dispositivos de red fue de bastante ayuda casi automatizando por completo la configuración.

Aún así, la configuración de los dispositivos se tornó tediosa, debido a que se desconocían por completo las características y funcionamiento de algunos dispositivos que se encuentran funcionando en la red de datos universitaria, que en su mayoría, son de marcas y modelos diferentes. Por otro lado, la herramienta que se desarrollo estaba basada en dispositivos de un solo fabricante y modelos específicos utilizados en el mini-laboratorio de pruebas.

En cuanto a SNMP, uno de estos puntos débiles consiste en que no todos los OIDs funcionan en todos los dispositivos por igual, cada fabricante implementa su propia MIB, y por consiguiente, la mayoría de OIDs varian por cada tipo de dispositivo o inclusive, aunque sean del mismo tipo y del mismo fabrincante.

Por lo tanto, para una mejor gestión de los dispositivos se recomienda (en medida de lo posible) adquirir dispositivos del mismo fabricante, ya que si bien puede llegar a haber diferencias, estas son mínimas, y el principal beneficio es que la red se vuelve homogénea, es decir, que no hay variedad de dispositivos.

Otro punto debil de SNMP es que es un protocolo inseguro a menos que sea configurado con la versión 3. Los dispositivos de la Universidad de Quintana Roo están configurados con el agente SNMP versión 1, por lo que se recomienda enfáticamente al administrador de red configure los dispositivos con la versión 3 del agente SNMP.

Aún así, trabajando en conjunto, son una excelente herramienta para el monitoreo y gestión de dispositivos de red.

Finalmente, como resultado del monitoreo realizado a los principales dispositivos de red de la Universidad de Quintana Roo, se puede concluir lo siguiente:

1. La red de la Universidad de Quintana Roo no es homogénea en cuanto a marcas y modelos de dispositivos.
2. Algunos dispositivos importantes para proporcionar acceso a la red de datos universitaria no soportan el protocolo SNMP.
3. La gestión de los dispositivos de red de la Universidad de Quintana Roo no es segura, debido al uso del protocolo SNMP v1.
4. La red de la Universidad de Quintana Roo no presenta inconsistencias a nivel de dispositivos.
5. El problema de la red de datos de la Universidad de Quintana Roo muy posiblemente sea por causas de una incorrecta configuración de protocolos de red.

REFERENCIAS BIBLIOGRÁFICAS

Comer, D. E. (1997). *Redes de Computadoras, Internet e Interredes* (1ª edición ed.). México: Prentice-Hall.

empresas, S. d. (n.d.). *Proton.* From Universidad de Guadalajara: http://proton.ucting.udg.mx/somi/memorias/sistemas/sis-0-4.PDF

FIEC, I. d. (n.d.). *Repositorio de la Escuela Superior Politécnica del Litoral.* From DSpace en ESPOL: http://www.dspace.espol.edu.ec/bitstream/123456789/16202/1/Implementación%20de%20un%20Sistema%20de%20Gestión%20y%20Administración%20de%20Redes%20Basados%20en.pdf

Forouzan, B. A. (2002). *Transmisión de datos y redes de comunicaciones* (2ª edición ed.). España: McGraw-Hill.

Fundamentos de redes de datos. (n.d.). From http://dc352.4shared.com/doc/CQZ-X4Pk/preview.html

Gestión de redes. (n.d.). From http://www.angelfire.com/wy/licut/tareas/redes/gestion_osi.html

Gestión de redes. (n.d.). From http://www.ac.usc.es/docencia/ASRII/Tema_1html/node13.html

Hablemos del modelo OSI Open System Interconexion. (n.d.). From http://clasico83.wordpress.com/2013/10/07/hablemos-del-modelo-osi-open-system-interconexion/

Hill, B. (2002). *Cisco - Manual de referencia* (1ª edición ed.). España: McGraw-Hill.

Hucaby, D. (2002). *Cisco Field Manual: Catalyst Switch Configuration.* Estados Unidos: Cisco Press.

Nagios. (n.d.). *Overview*. From Nagios: http://www.nagios.org/about/overview

Raya, J. (1997). *Redes locales y TCP/IP* (1ª edición ed.). México: Alfaomega Grupo Editor.

Sánchez, J. (2000). *Redes* (1ª edición ed.). España: McGraw-Hill.

TCP/IP. (n.d.). From http://adminredesfpo.wikispaces.com/TCP+-+IP

TCP/IP, P. (n.d.). *Guide.* From McGraw-Hill: http://www.mcgraw-hill.es/bcv/guide/capitulo/8448199766.pdf

UQRoo. (n.d.). *Historia*. From Universidad de Quintana Roo: http://www.uqroo.mx/nuestra-universidad/identidad-universitaria/historia/

UQRoo. (n.d.). *Infraestructura y servicios*. From Universidad de Quintana Roo: http://www.uqroo.mx/nuestra-universidad/identidad-universitaria/infraestructura-y-servicios/

ANEXO A – Nagios Core 3.5.1

Requisitos de hardware

El hardware utilizado dependerá del entorno del sistema operativo que se desee utilizar. Existen dos escenarios de configuración posibles:

Sin entorno gráfico

- 256 MB de RAM
- 20 GB en disco duro
- Procesador Celeron o superior

Con entorno gráfico

- 1 GB de RAM
- 20 GB en disco duro
- Procesador Celeron o superior

Preparación del sistema

Es importante preparar el sistema para que no se tenga ningún problema durante la compilación de Nagios y sus plugins. Por lo tanto, es necesaria la instalación de paquetes y librerías mediante la línea de comandos utilizando el comando “apt-get install” en modo superusuario:

- apt-get install –y build-essential
- apt-get install –y php5
- apt-get install –y snmp

- apt-get install –y libssl-dev
- apt-get install –y libgd2-xpm
- apt-get install –y libgd2-xpm-dev
- apt-get install –y libgd-tools

Directorio de instalación

La ruta donde se instalará Nagios Core es "/usr/local/nagios", pero la carpeta " " no existe, por lo tanto, hay que crearla utilizando el " k "

```
mkdir /usr/local/nagios
```

Después de haber creado la carpeta " " debe cambiar el propietario de la misma. Cambiar el propietario, significa que esa carpeta pertenece a determinado usuario y grupo, en este caso se cambiara al usuario y grupo nagios.

" w "

desde la línea de comandos.

```
chown –R nagios:nagios /usr/local/nagios
```

Paquetes a compilar

Nagios Core

http: //prdownloads.sourceforge.net/sourceforge/nagios/nagios-3.5.1. tar.gz

Nagios plugins

http://prdownloads.sourceforge.net/sourceforge/nagiosplug/nagios-plugins-1.5. tar.gz

GD Utils

http://www.boutell.com/gd/http/gd-2.0.33. tar.gz

Compilación e instalación de la librería GDUtils

- **Descomprimir utilizando el comando "tar"**

  tar zxvf gd-2.0.33.tar.gz

- **Compilar**

  ./configure

- **Instalar**

  make && make install

Compilación e instalación de Nagios Core

- **Descomprimir utilizando el comando "tar"**

  tar zxvf nagios-3.5.1.tar.gz

- **Compilar**

  ./configure

- **Instalar**

  make all

  make install

  make install-init

  make install-commandmode

  make install-config

Donde:

make all →Genera todos los archivos de instalación.
make install→ Instala Nagios Core.
make install-init→ Instala el script para iniciar Nagios Core
make install-config → Instala los archivos de configuración de ejemplo en /usr/local/nagios/etc
make install-commandmode →Instala y configura permisos en el directorio en espera del archivo de comandos externos.

Compilación e instalación de Nagios-plugins

- **Descomprimir utilizando el comando "tar"**

  tar zxvf nagios-plugins-1.5.tar.gz

- **Compilar**

  ./configure

- **Instalar**

  make && make install

Configuración de la interfaz Web

Una vez instalados Nagios Core y los plugins, es momento de crear el front end para la interfaz Web. Para ello, se crea el archivo " " que contendrá las W G '
Web de Nagios Core.

" " "/etc/apache2/sites-available"
" "

nano /etc/apache2/sites-available/nagios

Las instrucciones dentro del archivo “ ” son las siguientes:

```
ScriptAlias /nagios/cgi-bin /usr/local/nagios/sbin

<Directory "/usr/local/nagios/sbin">
        Options ExecCGI
        AllowOverride None
        Order allow,deny
        Allow from all
        AuthName "Nagios Access"
        AuthType Basic
        AuthUserFile /usr/local/nagios/etc/htpasswd.users
        Require valid-user
</Directory>

Alias /nagios /usr/local/nagios/share

<Directory "/usr/local/nagios/share">
        Options None
        AllowOverride None
        Order allow,deny
        Allow from all
        AuthName "Nagios Access"
        AuthType Basic
        AuthUserFile /usr/local/nagios/etc/htpasswd.users
        Require valid-user
</Directory>
```

“ ” el sitio Web de Nagios Core, para ello se “ 2 ”

```
a2ensite nagios
```

Ahora se debe recargar el servidor Web

```
service apache2 reload
```

Configuración de la autenticación

Para poder acceder a la interfaz Web de Nagios Core se debe crear un usuario con su respectiva contraseña “ ”. Esto se hace “ w ”

```
htpasswd –c /usr/local/nagios/etc/htpasswd.users nagiosadmin
```

Reiniciar el servidor Web e iniciar Nagios Core

```
service apache2 restart
service nagios start
```

Crear el enlace simbólico para iniciar Nagios Core automáticamente en cada reinicio.

```
ln -s /etc/init.d/nagios /etc/rcS.d/S99nagios
```

Primeros pasos en Nagios Core

Lo primero que se debe hacer después de instalar Nagios Core es corregir algunos detalles de la configuración inicial. El primer archivo a corregir es “ ”, este archivo se encuentra en la ruta “ ” Se modifica “ ” superusuario.

```
nano /usr/local/nagios/etc/objects/commands.cfg
```

Una vez abierto el archivo hay que ubicar las líneas donde está definido el comando “check_snmp” “- ” siguiente manera:

```
check_line    $USER1$/check_snmp –H $HOSTADDRESS$ -o $ARG1$
```

“ ”

“ ” “ ”

superusuario.

nano /usr/local/nagios/etc/objects/localhost.cfg

Con el archivo abierto, ubicar las líneas donde se encuentra definido el hostgroup y borrarlas (o poner el símbolo # al principio de la línea).

Luego “ ”

“ ” s el que define la ruta de donde están ubicados los diferentes objetos que intervienen en la configuración de Nagio Core.

Después, agregar la siguiente línea debajo de los demás archivos de configuración individual:

cfg_file=/usr/local/nagios/etc/objects/hostgroups.cfg

Ubicar y quitar el símbolo # de las siguientes instrucciones:

cfg_dir=/usr/local/nagios/etc/servers
cfg_dir=/usr/local/nagios/etc/switches
cfg_dir=/usr/local/nagios/etc/routers

Y si se requiere configurar Access point, agregar la instrucción:

cfg_dir=/usr/local/nagios/etc/aps

Por último, crear las carpetas donde se alojarán los objetos

mkdir /usr/local/nagios/etc/servers

mkdir /usr/local/nagios/etc/switches

mkdir /usr/local/nagios/etc/routers

mkdir /usr/local/nagios/etc/aps

Ahora ya se puede comenzar a configurar dispositivos en Nagios Core.

NOTA: Las configuraciones con las defiiciones de dispositivos y servicios mostradas a continuación son sólo demostrativas, ya que por cuestiones de confidencialidad no se mostrarán las configuraciones con los nombres de host y direcciones IP reales.

Sólo se definirán unos cuantos servicios a manera de ejemplo, debido a que todos los servicios SNMP se configurán igual, lo único que cambia es el OID. De igual

"*check_mrtgtraf*"

banda de las interfaces de red.

Definición de un servidor Microsft Windows

Crear el archivo "W w " " "

nano /usr/local/nagios/etc/servers/Windows.cfg

El contenido del archivo "W w " es el siguiente:

```
# Ejemplo de definición de un servidor Windows

define host{
        use             windows-server
        host_name       windows
        alias           Servidor Windows
        address         10.10.10.4
        }
```

```
# Ejemplo de definición de un servicio
define service{
        use                     generic-service
        host_name               windows
        service_description     Tiempo activo
        check_command           check_snmp!.1.3.6.1.2.1.1.3.0
        }
```

Definición de un servidor GNU/Linux

“ ” “ ”

nano /usr/local/nagios/etc/servers/Linux.cfg

“ ” :

```
# Ejemplo de definición de un host GNU/Linux

define host{
        use             linux-server
        host_name       linux
        alias           Servidor Linux
        address         10.10.10.5
        }

# Ejemplo de definición de un servicio
define service{
        use                     generic-service
        host_name               linux
        service_description     Tiempo activo
        check_command           check_snmp!.1.3.6.1.2.1.1.3.0
        }

# Ejemplo de servicio para monitorear la interfaz eth0
define service{
        use                     generic-service
        host_name               linux
        service_description     eth0
        check_command           check_snmp!.1.3.6.1.2.1.2.2.1.8.1
        }
```

```
# Ejemplo de servicio para monitorear el ancho de banda en eth0
define service{
        use                     generic-service
        host_name               linux
        service_description     Ancho de banda en eth0
        check_command           check_local_mrtgtraf!/var/www/mrtg/10.10.10.5_
                                1.log!AVG!1000000,2000000!5000000,5000000
                                ¡10
        }
```

Definición de un servidor Solaris

"S " " "

nano /usr/local/nagios/etc/servers/Solaris.cfg

"S " :

```
# Ejemplo de definición de un host Solaris

define host{
        use             linux-server
        host_name       solaris
        alias           Servidor Solaris
        address         10.10.10.6
        }

# Ejemplo de definición de un servicio
define service{
        use                     generic-service
        host_name               solaris
        service_description     Tiempo activo
        check_command           check_snmp!.1.3.6.1.2.1.1.3.0
        }

# Ejemplo de servicio para monitorear la interfaz net0
define service{
        use                     generic-service
        host_name               solaris
        service_description     net0
        check_command           check_snmp!.1.3.6.1.2.1.2.2.1.8.1
        }
```

```
# Ejemplo de servicio para monitorear el ancho de banda en net0
define service{
        use                     generic-service
        host_name               net0
        service_description     Ancho de banda en eth0
        check_command           check_local_mrtgtraf!/var/www/mrtg/10.10.10.6_
                                1.log!AVG!1000000,2000000!5000000,5000000
                                ¡10
        }
```

Definición de un switch Catalyst 2950 series

Crear el archivo " w " " "

```
nano /usr/local/nagios/etc/switches/switch.cfg
```

El " w " :

```
# Ejemplo de definición de un switch

define host{
        use             generic-switch
        host_name       catalyst-2960
        alias           Cisco Catalyst 2960
        address         10.10.10.2
        }

define service{
        use                     generic-service
        host_name               catalyst-2960
        service_description     Tiempo activo
        check_command           check_snmp!.1.3.6.1.2.1.1.3.0
        }

define service{
        use                     generic-service
        host_name               catalyst-2960
        service_description     Fast Ethernet 1
        check_command           check_snmp!.1.3.6.1.2.1.2.2.1.8.1
        }

define service{
        use                     generic-service
        host_name               catalyst-2960
```

```
        service_description Gigabit Ethernet 1
        check_command    check_snmp!.1.3.6.1.2.1.2.2.1.8.25
        }
```

Definición de un router Cisco 2800 series

“ ” “ ”

nano /usr/local/nagios/etc/routers/router.cfg

El co “ ” :

```
# Ejemplo de definición de un router

define host{
        use             generic-switch
        host_name       cisco-2800
        alias           Cisco 2800 series
        address         10.10.10.254
        }

define service{
        use                     generic-service
        host_name               cisco-2800
        service_description     Tiempo activo
        check_command    check_snmp!.1.3.6.1.2.1.1.3.0
        }

define service{
        use                     generic-service
        host_name               cisco-2800
        service_description     Fast Ethernet 0/1
        check_command    check_snmp!.1.3.6.1.2.1.2.2.1.8.1
        }

define service{
        use                     generic-service
        host_name               cisco-2800
        service_description     Serial 0/0/1
        check_command    check_snmp!.1.3.6.1.2.1.2.2.1.8.4
        }
```

ANEXO B – Agente SNMP

Windows server 2008

Instalación

A “ ”

“ ”

“A ” (ver Figura 51).

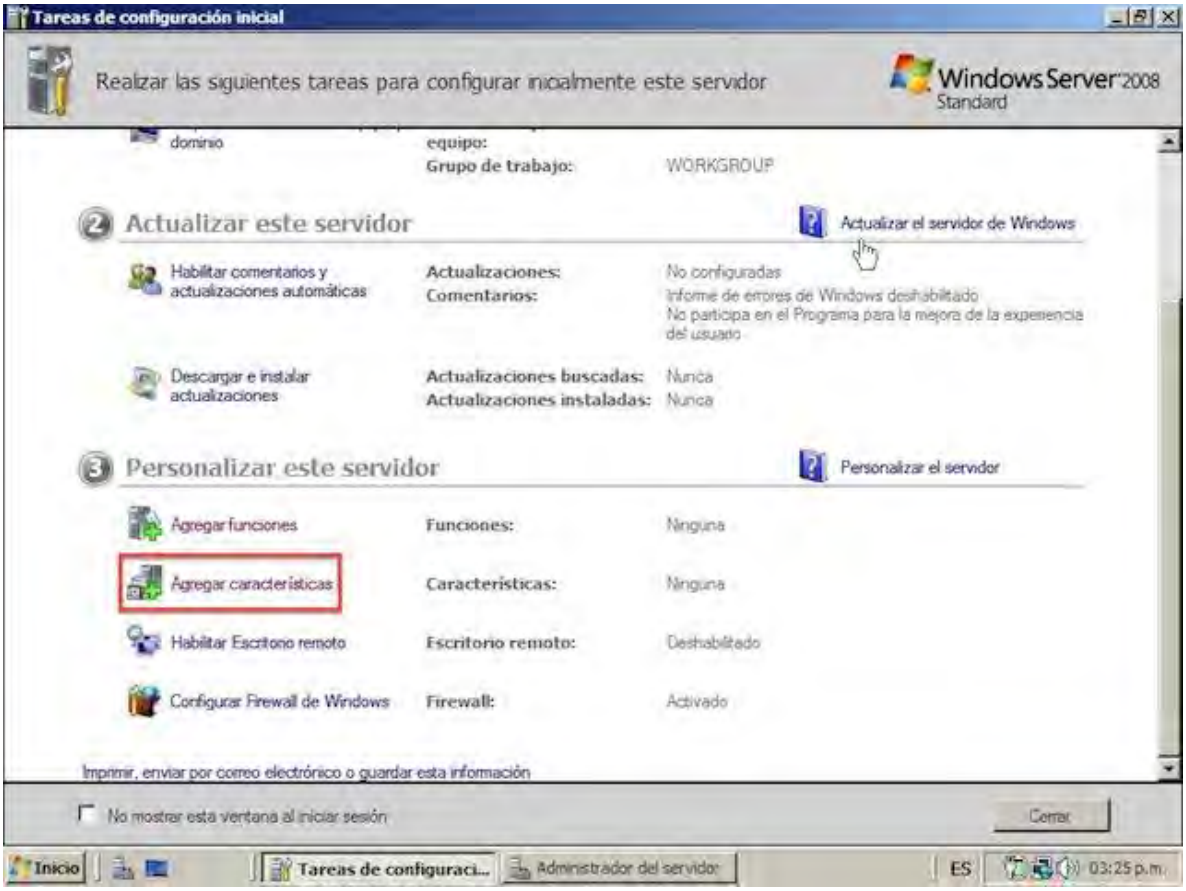

Figura 51. Pantalla Tareas de configuración inicial

“A

” “ ” “A

” (ver Figura 52).

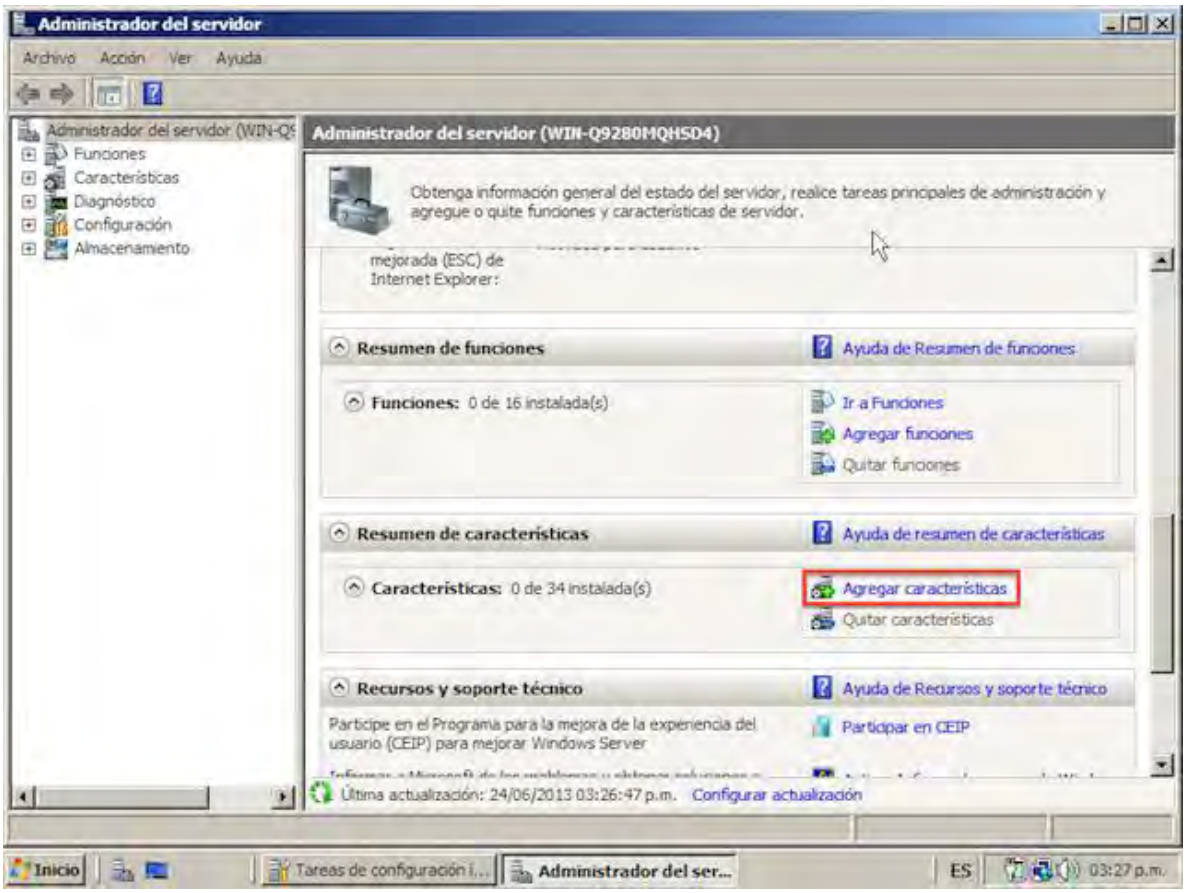

Figura 52. Pantalla Administrador del servidor

A “A ”
“S S ” +
“S S ” “S ” (ver Figura 53).

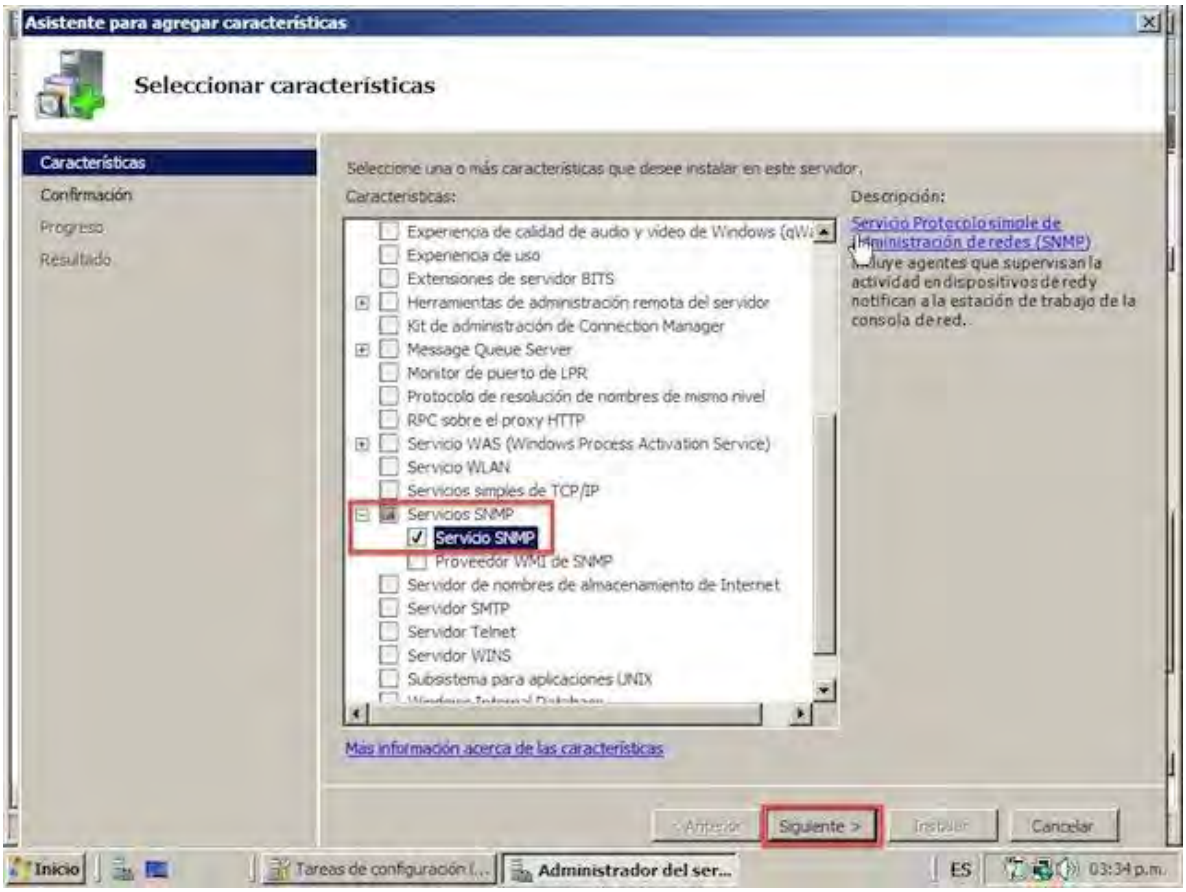

Figura 53. Pantalla Asistente para agregar características

A “ ” (ver Figura 54).

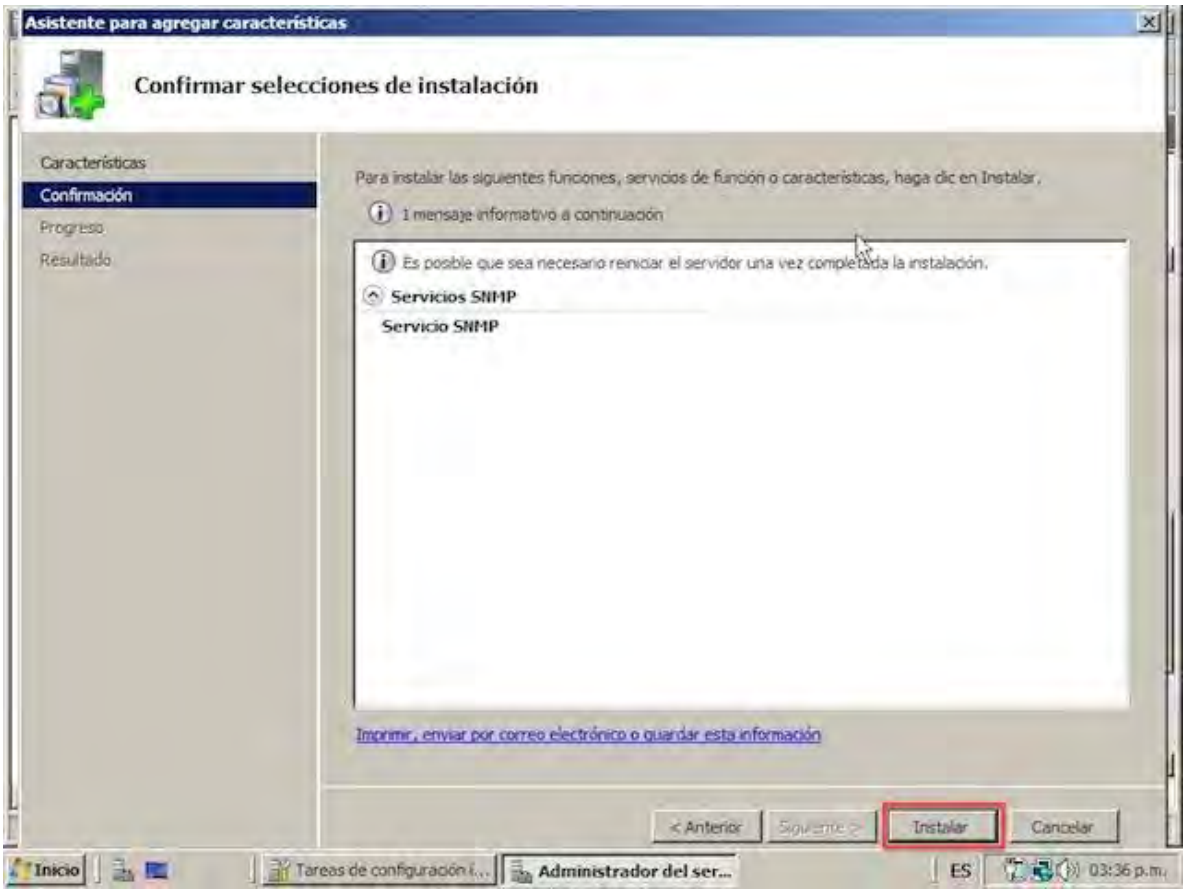

Figura 54. Pantalla Confirmación de instalación

La instalación tarda alrededor de 1 minuto.

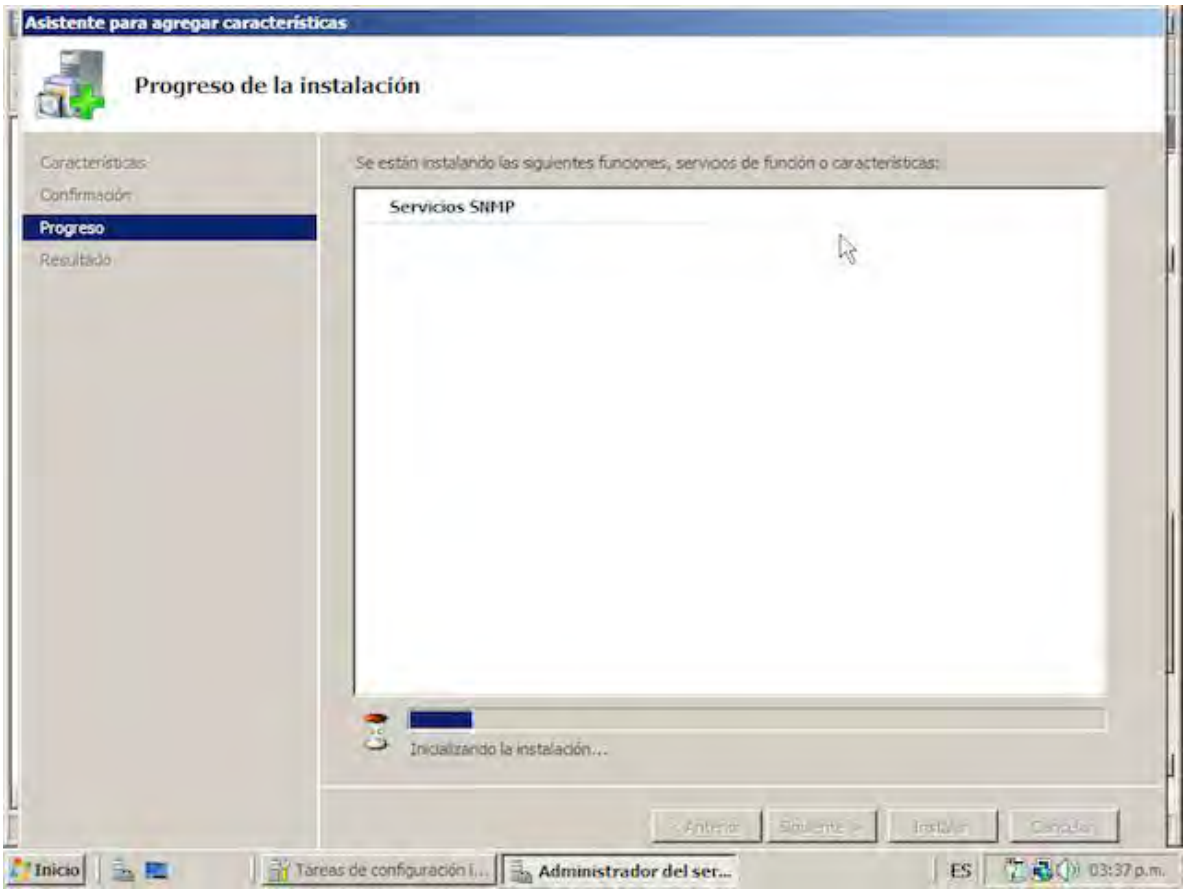

Figura 55. Pantalla Progreso de instalación

A “ ”

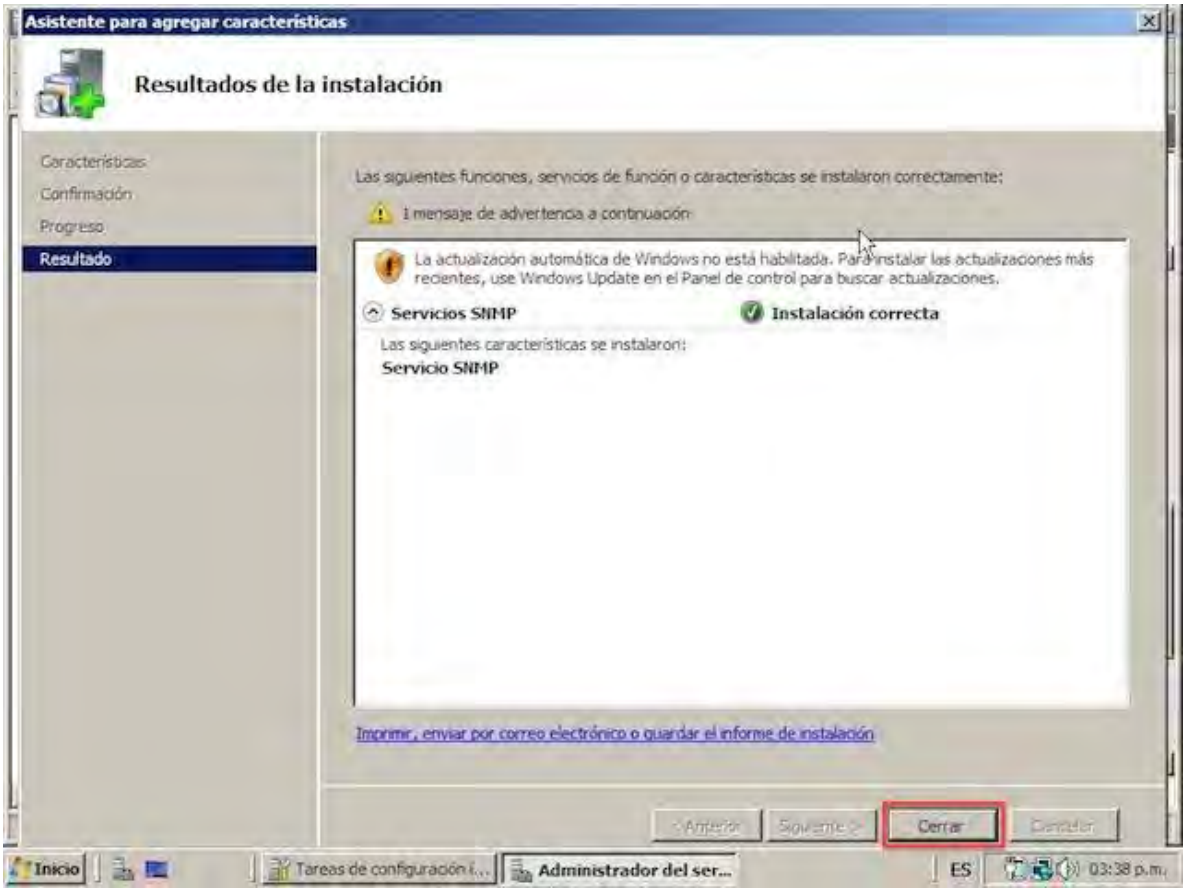

Figura 56. Pantalla Resultados de la instalación

Configuración

A “A ” “ ”
“S ” , tal como se muestra en la Figura 57.

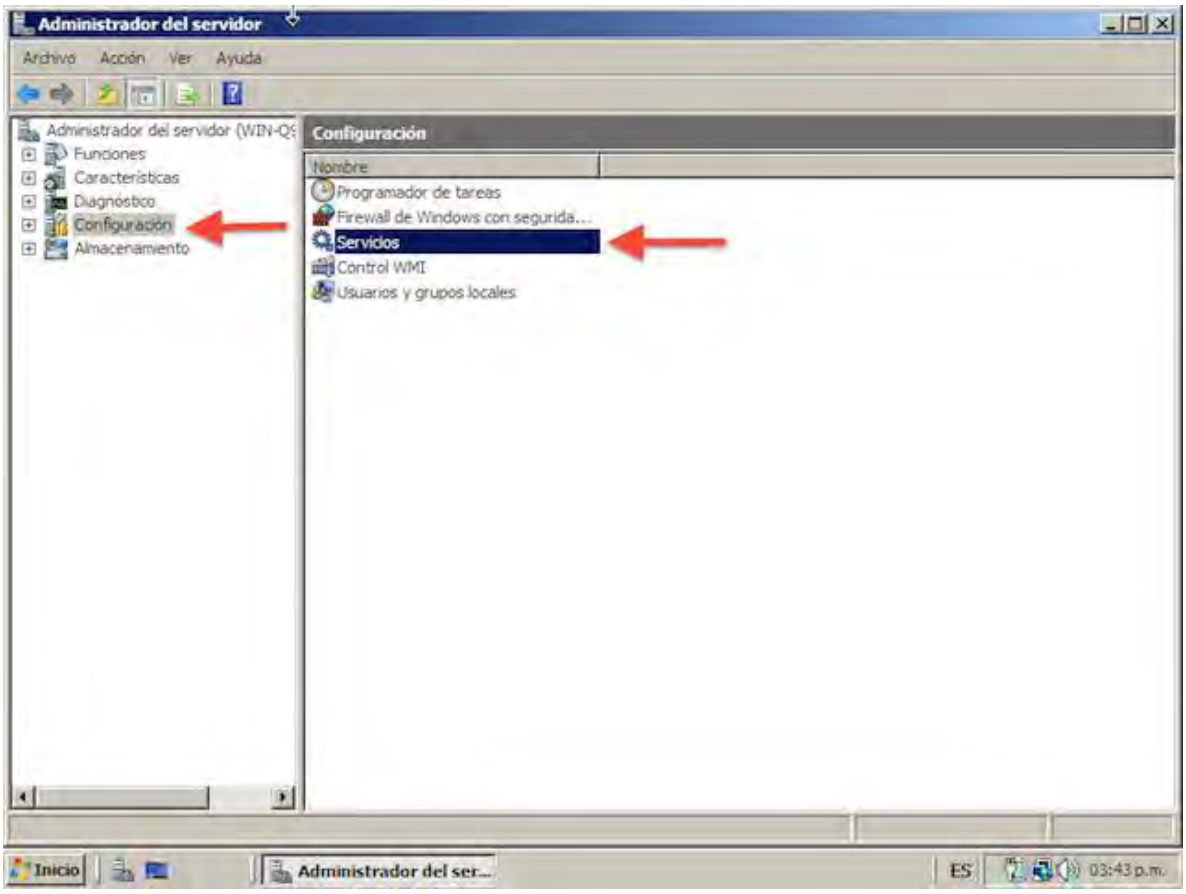

Figura 57. Pantalla Administrador del servidor – configuración

“S S ”

Luego clic derecho y entrar a sus propiedades (ver Figura 58).

Figura 58. Pantalla Administrador del servidor - servicios

A “S S ” (ver Figura 59).

“A ” “ ”

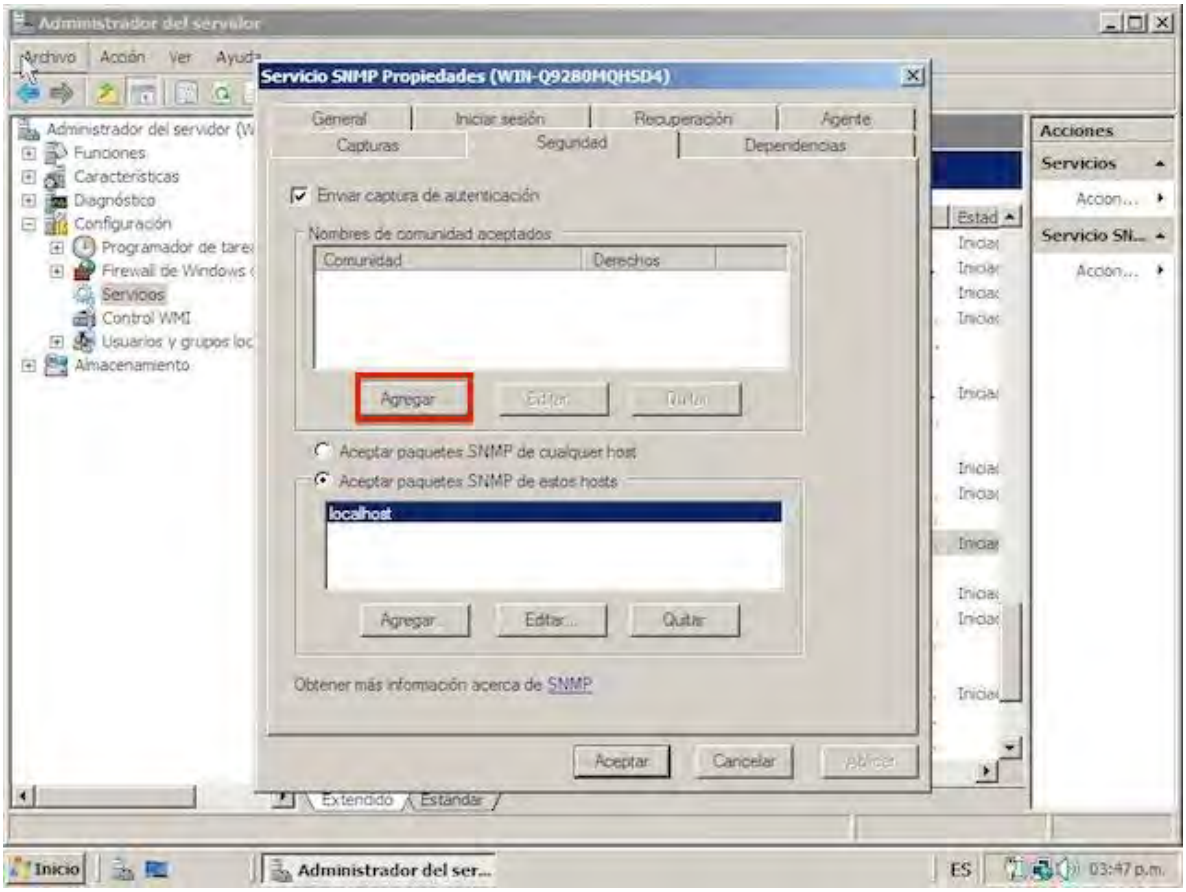

Figura 59. Pantalla Agregar comunidad

“ ” SÓ A “ ” tal y como se indica en la Figura 60. Posteriormente, clic en “A ”

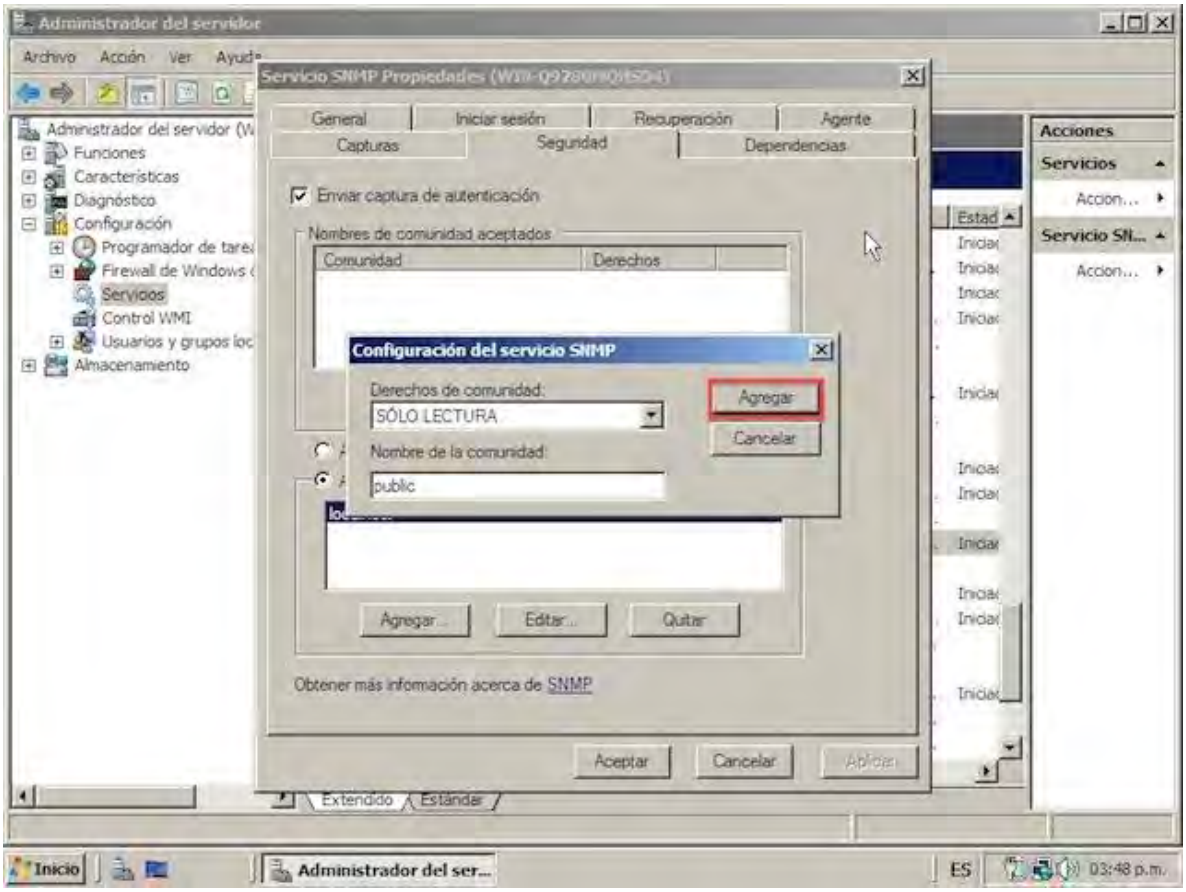

Figura 60. Pantalla Configuración de la comunidad

“S S ” de la Figura 61, “A S ” luego clic en “A ”

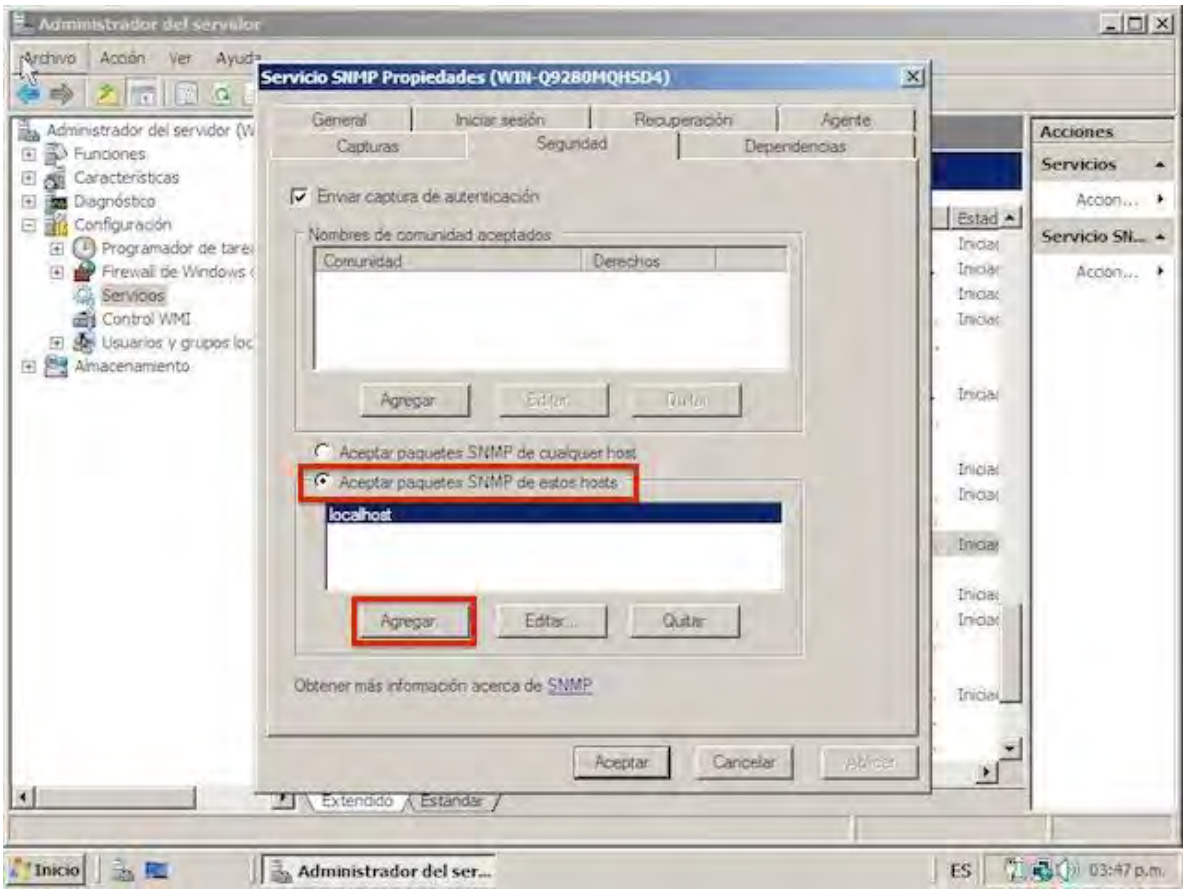

Figura 61. Pantalla Agregar estación de gestión

Escribir la IP del servidor donde se encuentra el cliente Nagios de la misma manera como se indica en la Figura 62. Luego c “A ”

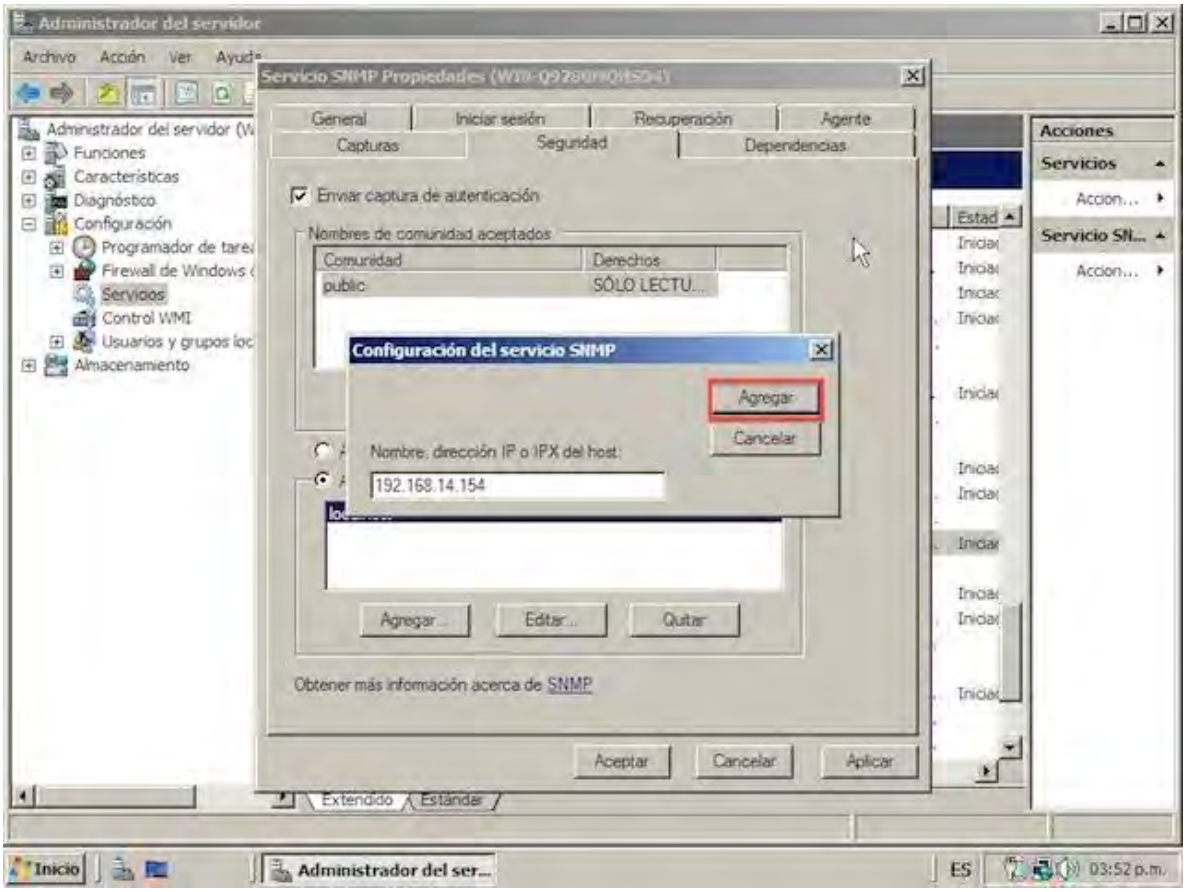

Figura 62. Configuración de la estación de gestión

Para finalizar, sólo queda dar “A ” (ver Figura 63).

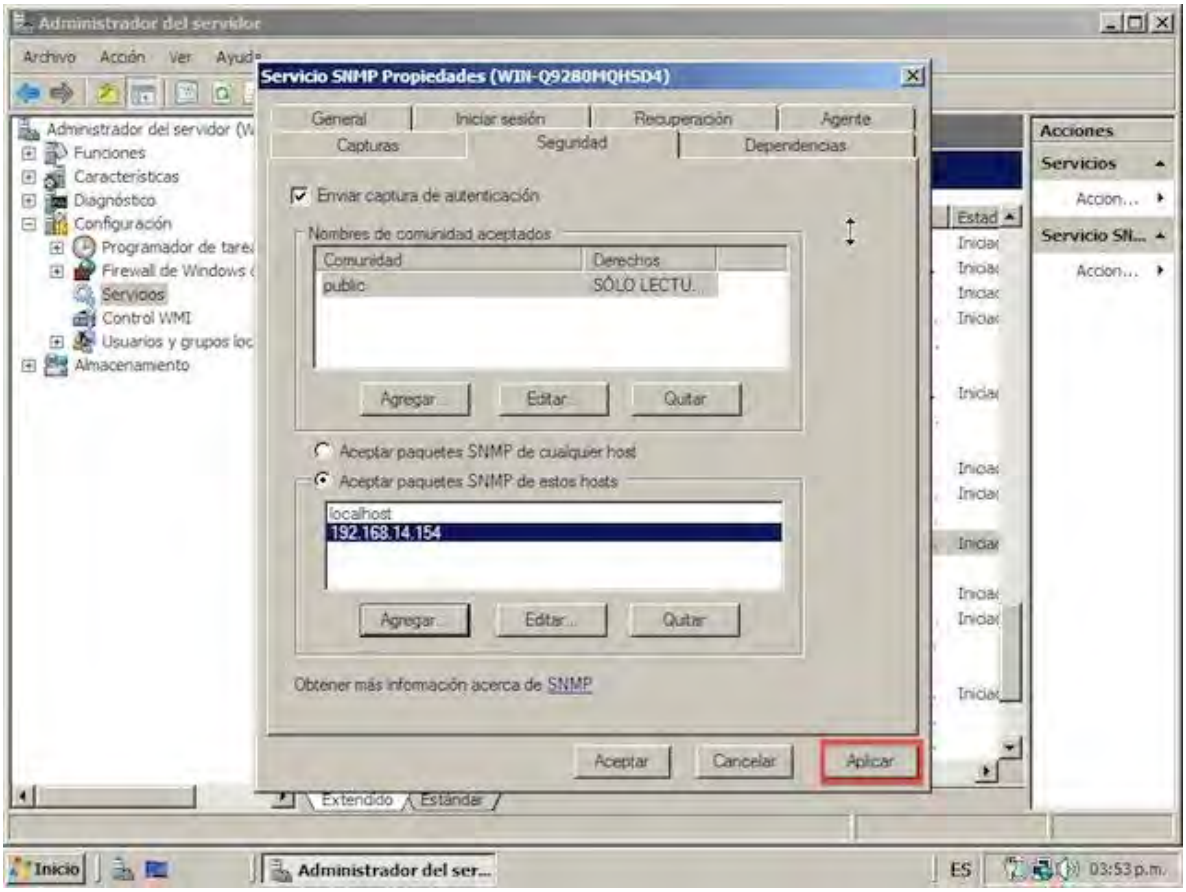

Figura 63. Pantalla Aplicar configuración al agente SNMP

GNU/Linux Debian 7.1

Instalación

La instalación se hace mediante la línea de comandos utilizando el “ -
”

apt-get install – y snmp
apt-get install – y snmpd

Configuración del agente SNMP

El archivo de configuración del demonio SNMP se encuentra en la ruta
“ ”

Nota: Por seguridad, se recomienda guardar el archivo original y crear uno nuevo para comenzar a configurar desde cero. Para ello, sólo es cuestión de renombrar el archivo “ ”

mv /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.backup

Después de respaldar, “ ”

nano /etc/snmp/snmpd.conf

El contenido del archivo “snmpd.conf” es el siguiente:

rocommunity public 127.0.0.1
rocommunity public 192.168.14.154

includeAllDisks

Posteriormente se debe configurar el PID (Identificador del proceso). Éste archivo es el que le indica al proceso de dónde tomar la configuración del agente SNMP. S “ ” “ ”
en modo superusuario.

nano /etc/default/snmpd

Dentro del archivo, ubicar y comentar (#) la siguiente instrucción:

S S=’ -Lsd –Lf /dev/null –u snmp –l –smux – ’

Después de comentar la instrucción anterior, se agrega la nueva:

S S=’ -Lsd –Lf /dev/null –u snmp –l –smux –p /var/run/snmpd.pid –c
’

Por último, sólo reiniciar el servicio

service snmpd restart

Solaris 11.1

Instalación

En Solaris 11.1, el agente NET-SNMP ya viene instalado, sólo es cuestión de configurarlo y habilitarlo.

Configuración del agente SNMP

Nota: Por seguridad, se recomienda guardar el archivo original y crear uno nuevo para comenzar a configurar desde cero. Esto se hace renombrando el archivo el “ ”

```
mv /etc/net-snmp/snmp/snmpd.conf /etc/net-snmp/snmp/snmpd.conf.backup
```

“ ”

```
nano /etc/net-snmp/snmp/snmpd.conf
```

El contenido del archivo “snmpd.conf” es el siguiente:

```
rocommunity public 127.0.0.1
rocommunity public 192.168.14.154

includeAllDisks
```

Después de configurar el agente SNMP, se debe habilitar el servicio en Solaris 11.1. Esto se puede hacer de dos maneras, la primera con el administrador de servicios SMF en modo gráfico (ver Figura 64) ó desde la línea de comandos “ ”.

```
svcadm enable svc:/application/management/net-snmp:default
```

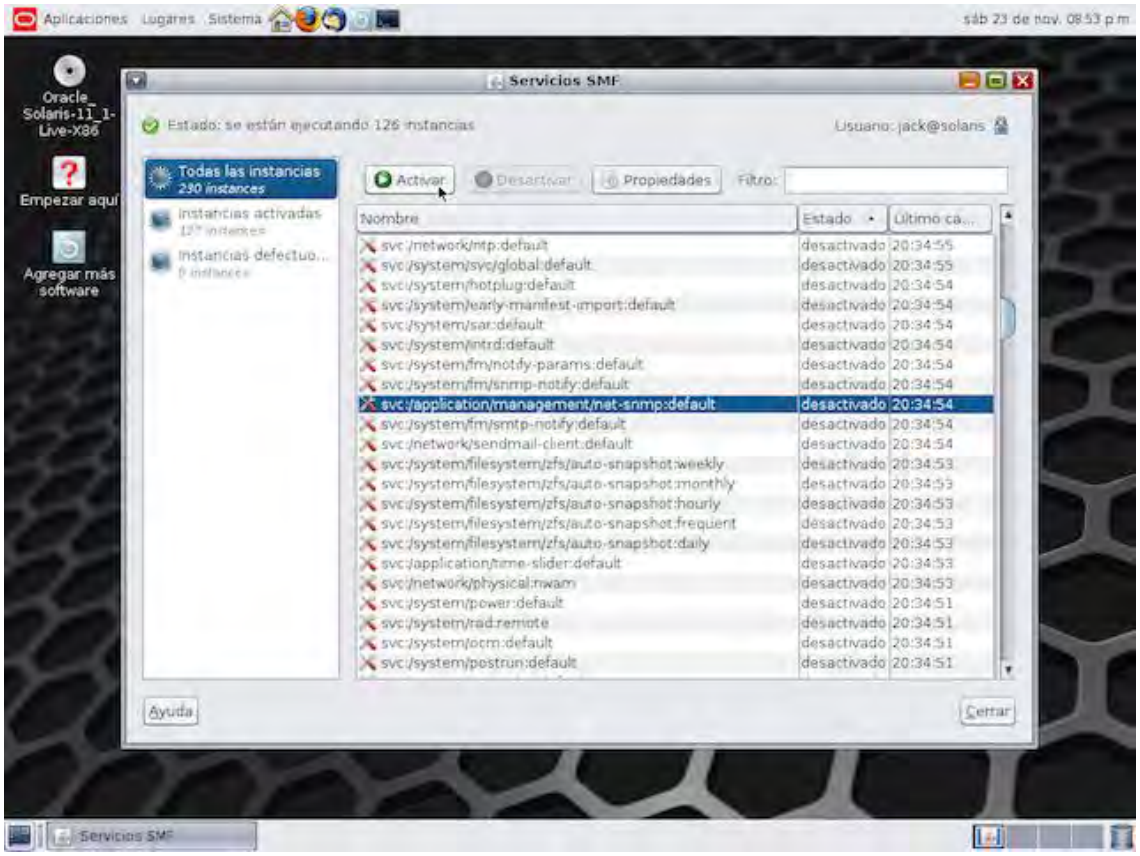

Figura 64. Servicios SMF

Finalmente, reiniciar el servicio

svcadm restart net-snmp

Switches y routers Cisco

La configuración de los switches y routers Cisco es muy sencilla, sólo se tienen que introducir las siguientes instrucciones:

Switch>enable
Switch#configure terminal
Switch(config)#snmp-server community public ro
Switch(config)#snmp-server enable traps
Switch(config)#snmp-server host 192.168.14.154 public

ANEXO C – Postfix

Instalación

Para enviar las alertas se debe instalar un servidor de correo, en este caso Postfix. Para ello se utiliza el " - " modo superusuario.

- apt-get install –y postfix
- apt-get install –y mailutils

Configuración

Después de instalados los paquetes se debe modificar el archivo de configuración principal del servidor de " " " " " " comandos.

nano /etc/postfix/main.cf

" " :

relayhost = [smtp.gmail.com]:587
smtp_use_tls = yes
smtp_tls_CAfile = /etc/postfix/cacert.pem
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl/passwd
smtp_sasl_security_options = noanonymous

Crear el archivo de certificación que usará Postfix para identificarse ante los servidores de Gmail. Para ello se escribe la siguiente instrucción en la línea de comandos.

cat /etc/ssl/certs/Equifax_Secure_CA.pem >> /etc/postfix/cacert.pem

“ w ”

“ ” “ ”

nano /etc/postfix/sasl/passwd

“ w ” :

[smtp.gmail.com]:587 ejemplo@gmail.com:contraseña

Después “ w ”

“ ”

comandos

postmap /etc/postfix/sasl/passwd

Posteriormente, protegerlo para que sólo el propietario pueda leer y escribir en él. Para ello, “ ”

chmod 600 /etc/postfix/sasl/passwd
chmod 600 /etc/postfix/sasl/passwd.db

Por último, iniciar, recargar y reiniciar el servidor de correo Postfix

service postfix start
service postfix reload
service postfix restart

ANEXO D – MRTG

Instalación

MRTG es una utilidad que sirve para graficar el ancho de banda de las interfaces de dispositivos de red. Los valores que genera MRTG son utilizados por el plugin “ k_ ” agios pueda desplegar el ancho de banda en la interfaz Web.

apt-get install –y mrtg

Configuración

El archivo de configuración principal d G “ ” configuración se puede dar de dos maneras:

- **Verificar una única dirección IP**

- -output=/etc/mrtg.cfg comunidad_snmp@dirección_ip

- **Verificar una lista de direcciones IP**

cfgmaker \
- -output=/etc/mrtg.cfg \
- -community=nombre_de_la_comunidad_snmp \
10.10.10.1 \
10.10.10.2 \
10.10.10.3

Esto generará archivos .log en la ruta "/var/www/mrtg" que posteriormente se " k_ " " "
existe por defecto, crearla desde la línea de comandos en modo superusuario.

mkdir /var/www/mrtg

Adicionalmente, se puede crear una página Web donde MRTG muestra las gráficas con las variaciones en el ancho de banda de cada interfaz de red en las direcciones IP listadas.

" k " " k "
instalan al mismo tiempo que MRTG.

El comando es el siguiente:

- -output=/var/www/mrtg/index.html /etc/mrtg.cfg

Nota: Antes de configurar MRTG es necesario que los agentes SNMP estén configurados en los dispositivos de red.

ANEXO E – Nagios-autoinstall Script

```
#!/bin/bash
######################## Nagios Auto-install Script ########################
# File: nagios-autoinstall                                                 #
# Autor: Iván Giovanni Olivera Montalvo                                    #
# e-mail: ig.om.1984@gmail.com                                             #
#                                                                          #
# This program is free software: you can redistribute it and/or modify it under  #
# the terms of the GNU General Public License as published by the Free     #
# Software Fundation, either version 3 of the License, or (at your option) any   #
# later version.                                                           #
#                                                                          #
# This program is distributed in the hope that it will be usefull, but WITHOUT   #
# ANY WARRANTY. See the GNU General Public License for more details.       #
#                                                                          #
# http://www.gnu.org/licenses/                                             #
############################################################################

clear

echo "############################################################"
echo "#                  Welcome to Nagios auto-install script                  #"
echo "#                    by Iván Giovanni Olivera Montalvo                    #"
echo "#                          ig.om.1984@gmail.com                           #"
echo "############################################################"

######################## Declaración de funciones ########################
function createScriptAlias(){
cat > /etc/apache2/sites-available/nagios << EOF
ScriptAlias /nagios/cgi-bin /usr/local/nagios/sbin
<Directory "/usr/local/nagios/sbin">
        Options ExecCGI
        AllowOverride None
        Order allow,deny
        Allow from all
        AuthName "Nagios Access"
        AuthType Basic
```

```
        AuthUserFile /usr/local/nagios/etc/htpasswd.users
        Require valid-user
</Directory>

Alias /nagios /usr/local/nagios/share
<Directory "/usr/local/nagios/share">
        Options None
        AllowOverride None
        Order allow,deny
        Allow from all
        AuthName "Nagios Access"
        AuthType Basic
        AuthUserFile /usr/local/nagios/etc/htpasswd.users
        Require valid-user
</Directory>
EOF
}

function createMaincf(){
echo "" > /etc/postfix/main.cf
cat > /etc/postfix/main.cf << EOF
relayhost = [smtp.gmail.com]:587
smtp_use_tls = yes
smtp_tls_CAfile = /etc/postfix/cacert.pem
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl/passwd
smtp_sasl_security_options = noanonymous
EOF
}

function createSmtpLogin(){
cat > /etc/postfix/sasl/passwd << EOF
[smtp.gmail.com]:587 ejemplo@gmail.com:contraseña
EOF
}

echo "¿Desea continuar con la instalación? (y / n):"
read line
if [ "$line" = "y" ] || [ "$line" = "Y" ]; then
        echo "############################################################"
        echo "#                  Preparando el sistema para Nagios Core                  #"
        echo "############################################################"
        apt-get install -y build-essential
        apt-get install -y php5
        apt-get install -y snmp
        apt-get install -y libssl-dev
```

```
apt-get install -y libgd2-xpm
apt-get install -y libgd2-xpm-dev
apt-get install -y libgd-tools

echo "############################################################"
echo "#              Creando y preparando el directorio de instalación           #"
echo "############################################################"
mkdir /usr/local/nagios
chown -R nagios:nagios /usr/local/nagios

echo "############################################################"
echo "#                        Descargando paquetes a instalar                    #"
echo "############################################################"
echo "Nagios Core 3.5.1"
wget -P Descargas
http://prdownloads.sourceforge.net/sourceforge/nagios/nagios-3.5.1.tar.gz
echo "Nagios plugins 1.5"
wget -P Descargas https://www.nagios-plugins.org/download/nagios-plugins-
1.5.tar.gz
echo "Librería GD Utils 2.0.35"
wget -P Descargas http://google-desktop-for-linux-
mirror.googlecode.com/files/gd-2.0.35.tar.gz

echo "############################################################"
echo "#              Desempaquetando código fuente a compilar           #"
echo "############################################################"
cd /home/nagios/Descargas
echo ""
echo "Nagios Core..."
echo ""
tar zxvf nagios-3.5.1.tar.gz
echo ""
echo "Nagios plugins..."
echo ""
tar zxvf nagios-plugins-1.5.tar.gz
echo ""
echo "Librería GD Utils..."
echo ""
tar zxvf gd-2.0.35.tar.gz

echo "############################################################"
echo "#                        Compilando el código fuente                    #"
echo "############################################################"
echo ""
echo "Librería GD Utils..."
echo ""
```

```
cd /home/nagios/Descargas/gd/2.0.35
./configure
make && make install

echo ""
echo "Nagios Core..."
echo ""
cd /home/nagios/Descargas/nagios
./configure
make all
make install
make install-init
make install-config
make install-commandmode

echo ""
echo "Nagios Plugins..."
echo ""
cd /home/nagios/Descargas/nagios-plugins-1.5
./configure
make && make install

echo "############################################################"
echo "#       Creando el script Alias y activando el sitio Web de Nagios       #"
echo "############################################################"
createScriptAlias
a2ensite nagios
service apache2 reload
htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin

echo "############################################################"
echo "#            Reiniciando Servidor Web e iniciando Nagios Core            #"
echo "############################################################"
service apache2 restart
service nagios start
ln -s /etc/init.d/nagios /etc/rcS.d/S99nagios

echo "############################################################"
echo "#           Preparando el sistema de notificaciones por e-mail           #"
echo "############################################################"
echo ""
echo "Instalando postfix"
echo ""
apt-get install -y postfix
echo ""
echo "Instalando mailsutils"
```

```
        echo ""
        apt-get install -y mailutils

        echo ""
        echo "Respaldando el archivo main.cf original"
        cp /etc/postfix/main.cf /etc/postfix/main.cf.backup

        echo ""
        echo "Creando el nuevo archivo main.cf"
        createMaincf

        echo ""
        echo "Creando el archivo de certificación cacert.pem"
        cat /etc/ssl/certs/Equifax_Secure_CA.pem >> /etc/postfix/cacert.pem

        echo ""
        echo "Creando el archivo de login al correo SMTP"
        createSmtpLogin

        postmap /etc/postfix/sasl/passwd

        chmod 600 /etc/postfix/sasl/passwd
        chmod 600 /etc/postfix/sasl/passwd.db

        echo ""
        echo "Iniciando Postfix"
        echo ""
        service postfix start
        service postfix reload
        service postfix restart

        echo "############################################################"
        echo "#                      Instalación exitosa :D              #"
        echo "#                                                          #"
        echo "# Para comprobar que todo salió bien, ingresa a la interfaz Web de  #"
        echo "# Nagios Core de la siguiente manera: localhost/nagios     #"
        echo "#                                                          #"
        echo "############################################################"

else
        echo "Instalación cancelada"
        exit
fi
```

ANEXO F – CFGMaker

Esta aplicación fue desarrollada pensando en brindar agilidad a la hora de configurar los dispositivos de red con Nagios Core. Se desarrolló con Gambas versión 3, un lenguaje de programación *open source* orientado a objetos derivado de *Visual Basic*, perfecto para el desarrollo fácil y rápido de aplicaciones.

CFGMaker es una aplicación simple y sencilla, su función es generar los archivos de configuración de los dispositivos, agilizando la configuración y minimizando al máximo los errores que se pudieran cometer a la hora de escribir todos los comandos.

Su interfaz también es simple e intuitiva (ver Figura 65), bastarán pocos minutos para que el usuario logre entender el funcionamiento.

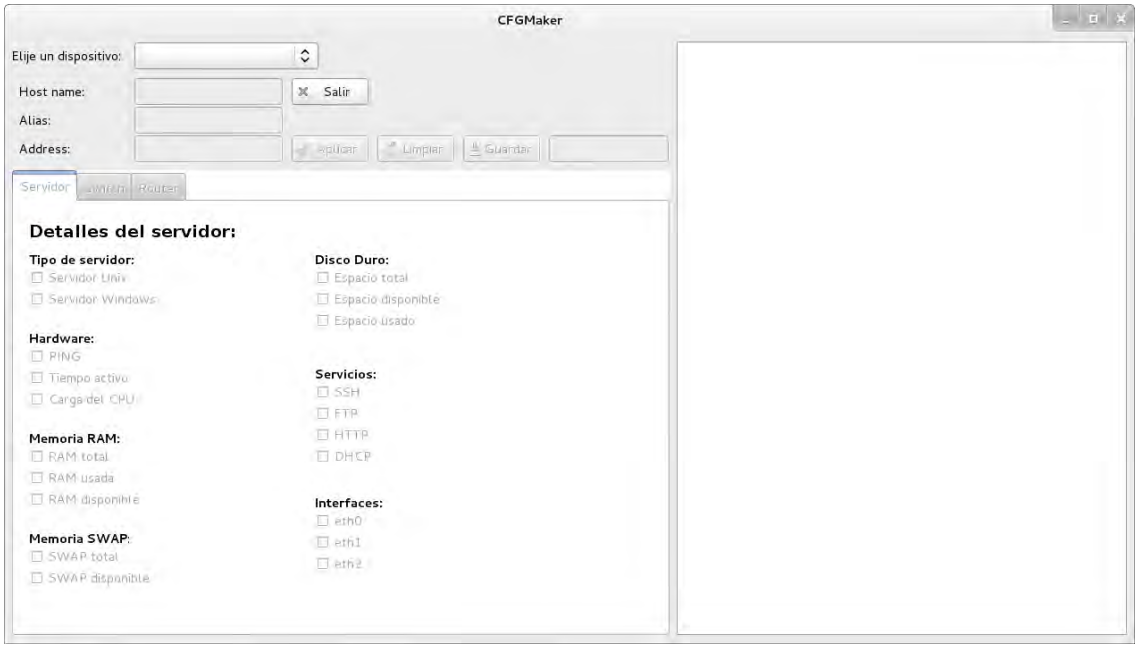

Figura 65. Interfaz gráfica de *CFGMaker*

Crear los archivos de configuración de los dispositivos es fácil y rápido, sólo hay que elegir alguna de las plantillas en la lista desplegable (ver Figura 66).

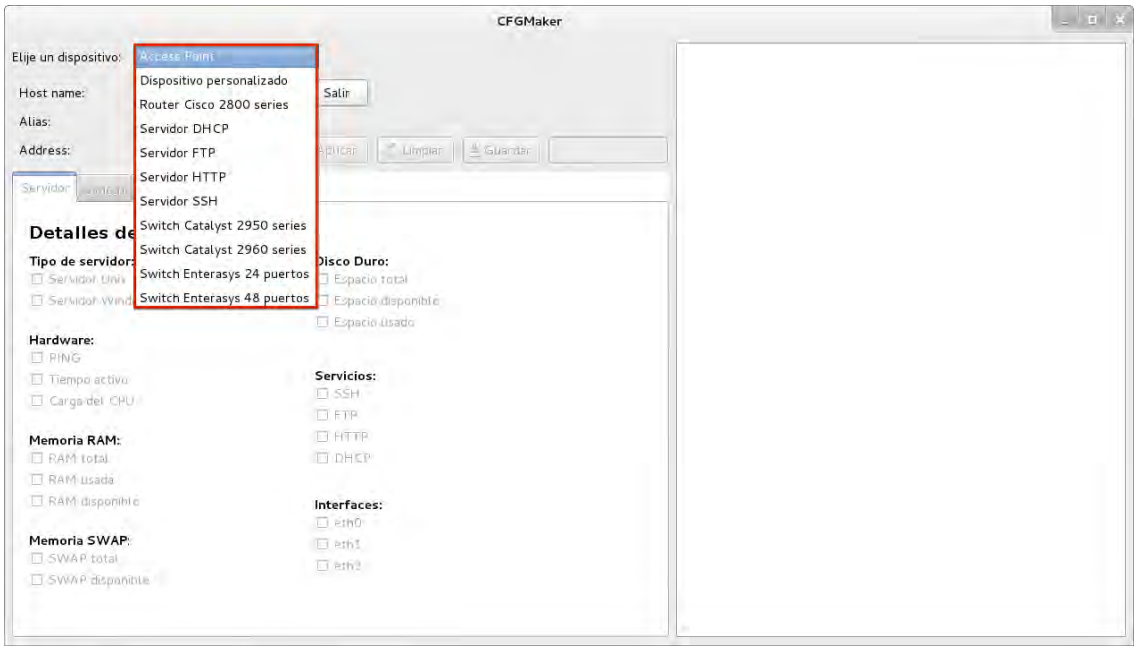

Figura 66. Lista de plantillas

Posteriormente ingresar el *hostname*, el *alias* y la dirección IP (*address*) en los "A " (ver Figura 67).

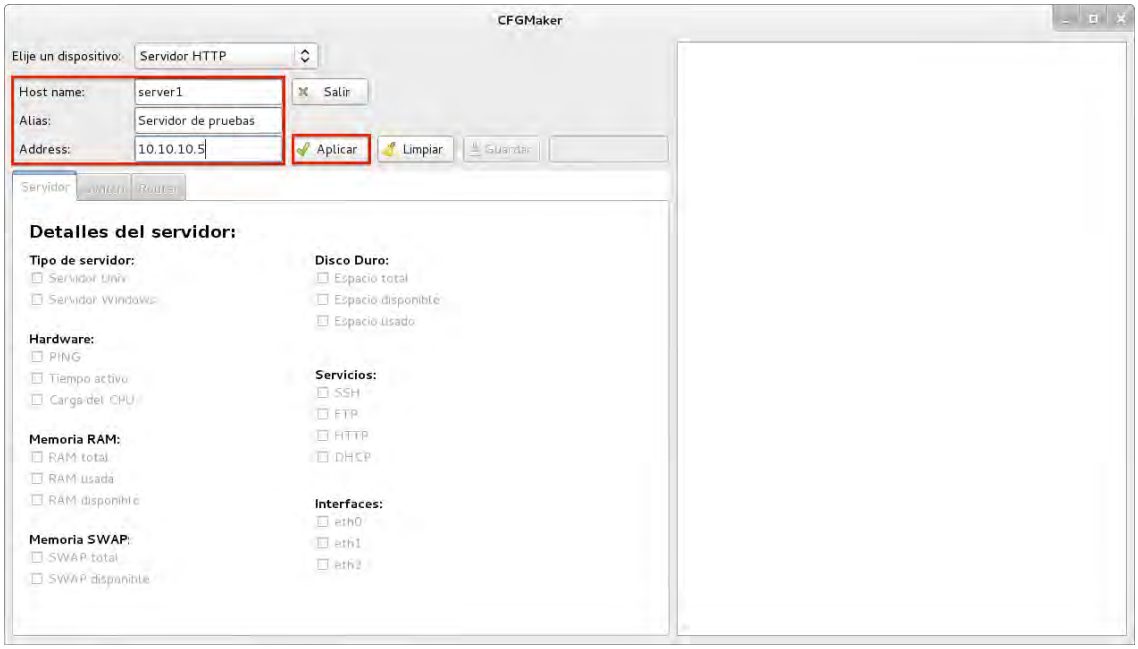

Figura 67. Ingreso de datos en el formulario

A “A ” G k
“ ” (ver Figura 68).

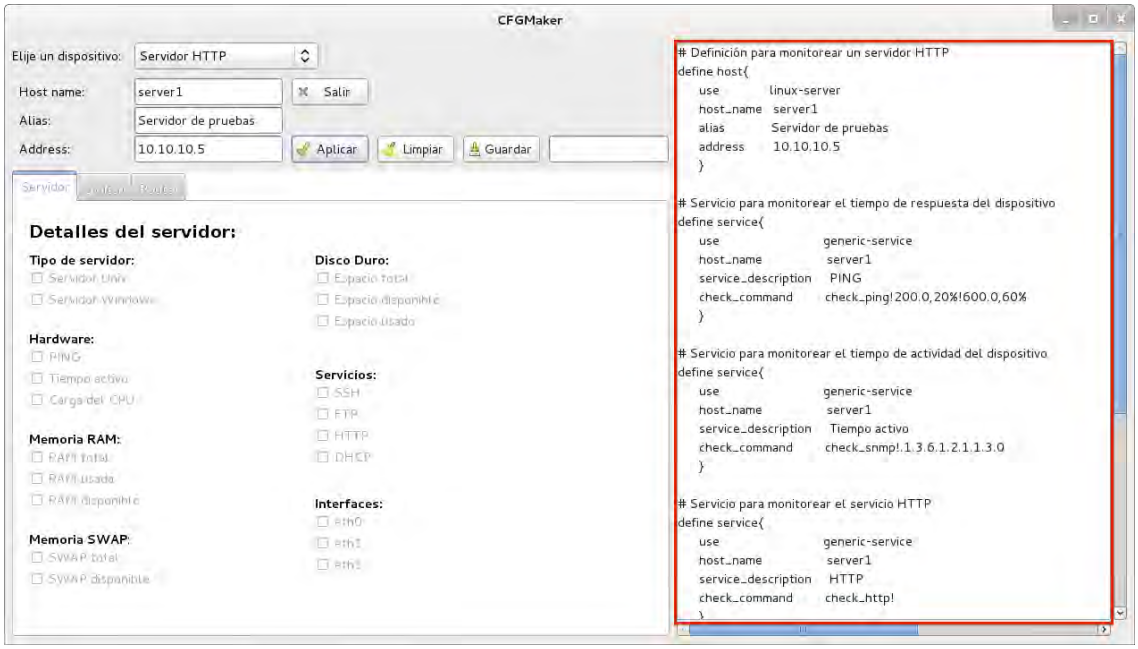

Figura 68. Editor de plantillas de CFGMaker

También se pueden crear archivos de configuración personalizados, donde se podrán elegir las características especificas a monitorear (ver Figuras 69, 70 y 71).

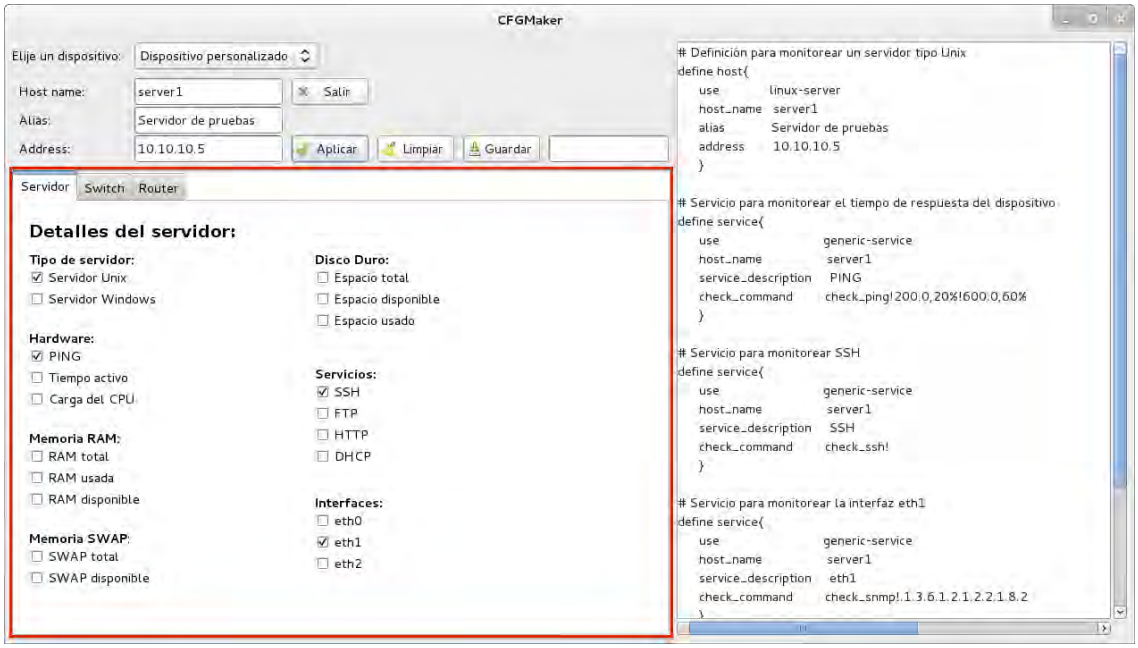

Figura 69. Sección de personalización para servidores

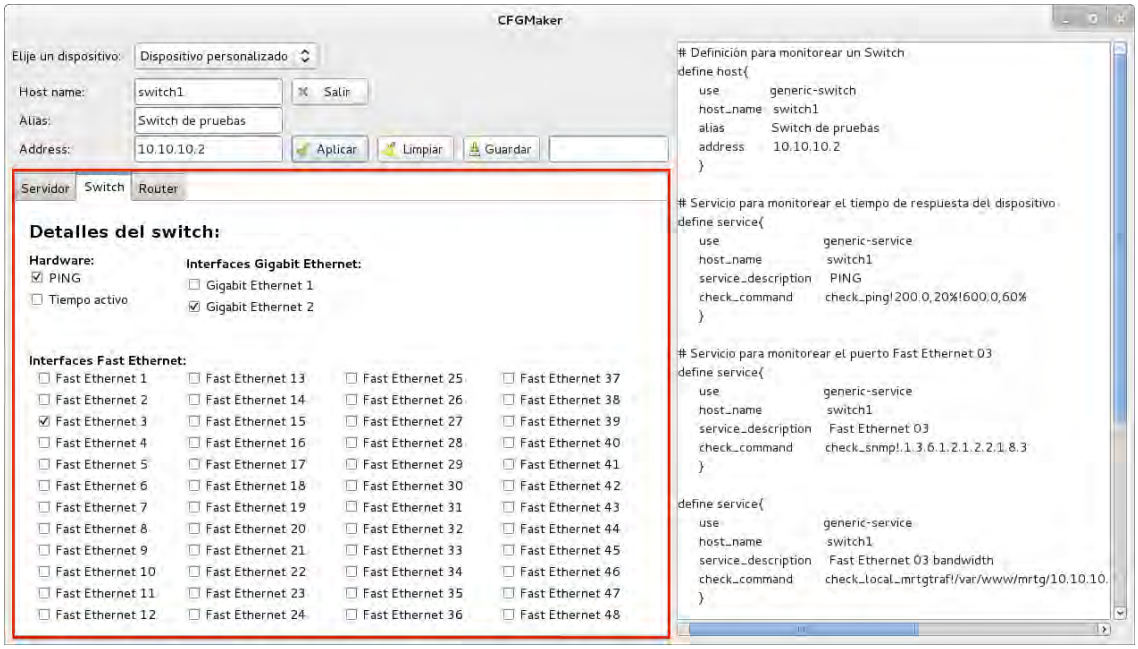

Figura 70. Sección de personalización para switches

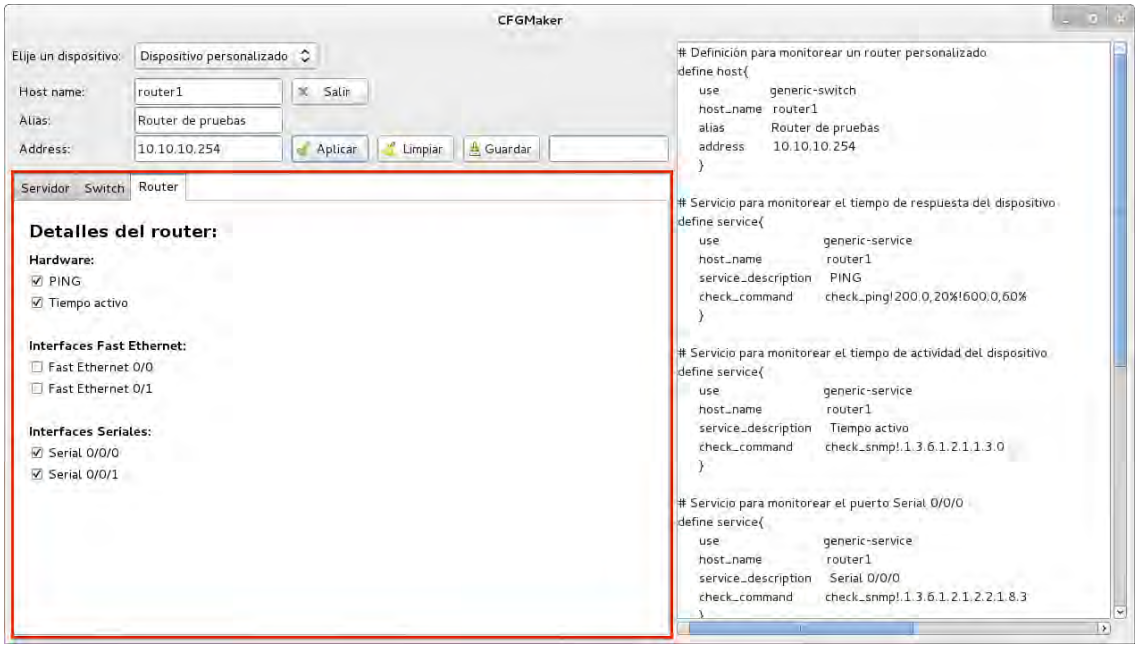

Figura 71. Sección de personalización para routers

Al terminar de configurar o personalizar el archivo de configuración hay que nombrar el archivo y dar clic en e “G ” 7 2).

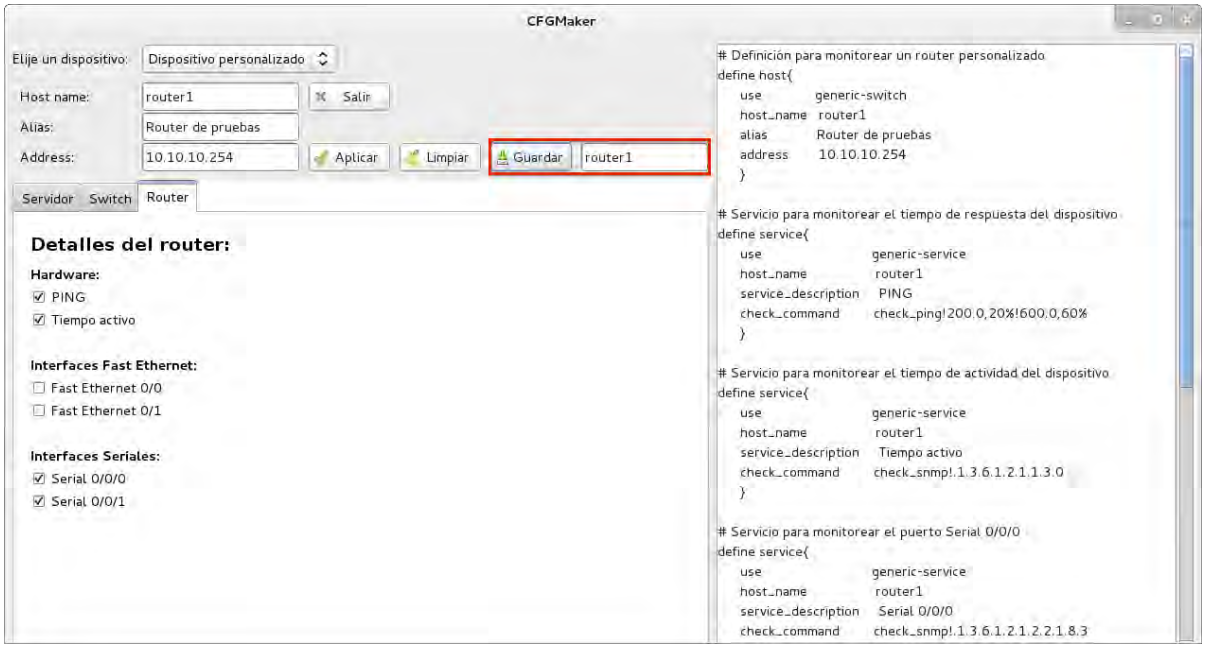

Figura 72. Guardar archivo

El archivo se guardará en la carpeta personal del usuario (ver Figura 73).

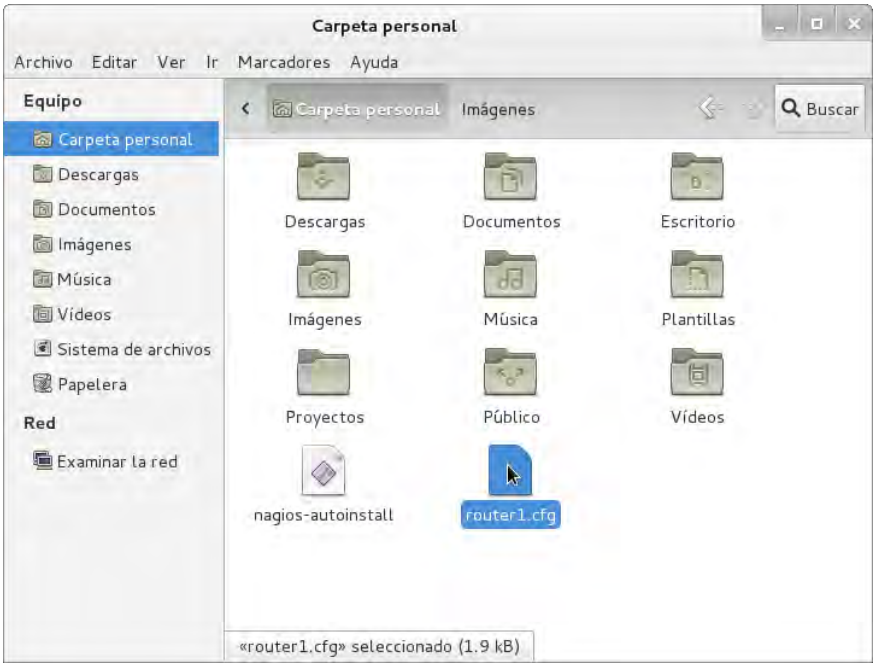

Figura 73. Carpeta de destino

Al abrir archivo se puede observar que la configuración ha sido guardada con las especificaciones seleccionadas (ver Figura 74).

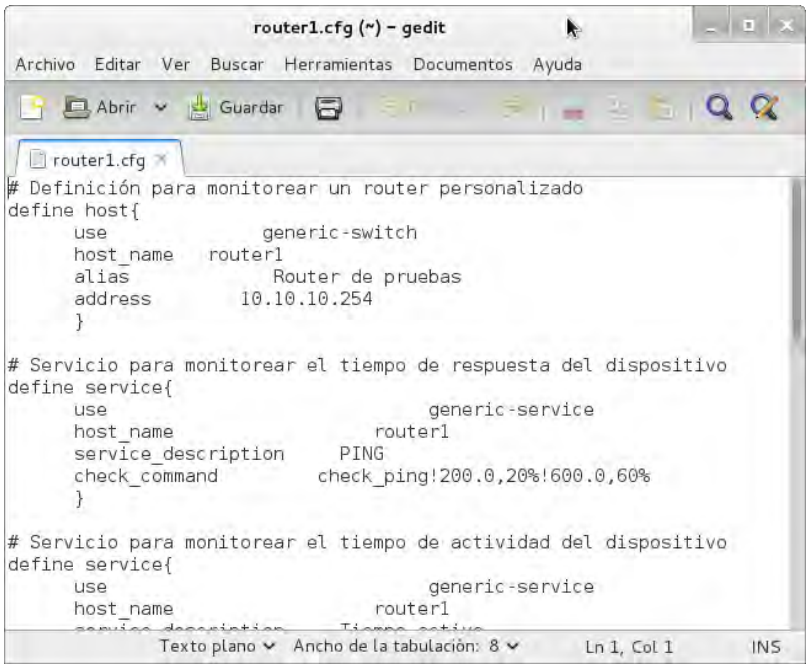

Figura 74. Archivo de configuración final

Por último, sólo queda copiarlo a la carpeta correspondiente y reiniciar el servicio de Nagios Core para que se tomen los cambios.

ANEXO G – Tablas de OIDs

La Tabla 9 muestra los OIDs más comunes para servidores basados en Unix

Tabla 9. OIDs para servidores basados en Unix

Tiempo activo	.1.3.6.1.2.1.1.3.0
Nombre de las tarjetas de red	.1.3.6.1.2.1.2.2.1.2
Estado de las tarjetas de red	.1.3.6.1.2.1.2.2.1.8
Total de memoria Swap	.1.3.6.1.4.1.2021.4.3.0
Total de memoria Swap disponible	.1.3.6.1.4.1.2021.4.4.0
Total de memoria RAM	.1.3.6.1.4.1.2021.4.5.0
Total de memoria RAM usada	.1.3.6.1.4.1.2021.4.6.0
Total de memoria RAM libre	.1.3.6.1.4.1.2021.4.11.0
Total de memoria RAM compartida	.1.3.6.1.4.1.2021.4.13.0
Total de memoria RAM usada por el buffer	.1.3.6.1.4.1.2021.4.14.0
Total de memoria cache	.1.3.6.1.4.1.2021.4.15.0
Ruta donde está montado el disco	.1.3.6.1.4.1.2021.9.1.2.1
Espacio total del disco duro	.1.3.6.1.4.1.2021.9.1.6.1
Espacio libre en el disco duro	.1.3.6.1.4.1.2021.9.1.7.1
Espacio usado en el disco duro	.1.3.6.1.4.1.2021.9.1.8.1
Porcentaje de espacio usado en el disco duro	.1.3.6.1.4.1.2021.9.1.9.1
Carga del CPU en 1 minuto	.1.3.6.1.4.1.2021.10.1.3.1
Carga del CPU en 5 minutos	.1.3.6.1.4.1.2021.10.1.3.2
Carga del CPU	.1.3.6.1.4.1.2021.10.1.3.3

En la Tabla 10 se listan los OIDs más comunes para switches y routers

Tabla 10. OIDs para switches y routers

Tiempo activo	.1.3.6.1.2.1.1.3.0
Nombre de las interfaces	.1.3.6.1.2.1.2.2.1.2
Estado de las interfaces	.1.3.6.1.2.1.2.2.1.8