UNIVERSIDAD CENTRAL "MARTA ABREU" DE LAS VILLAS
VERITATE SOLA NOBIS IMPONETUR VIRILIS TOGA. 1948

FACULTAD DE INGENIERÍA ELÉCTRICA

Departamento de Telecomunicaciones y Electrónica

TRABAJO DE DIPLOMA

Análisis de un sistema de supervisión para una red inalámbrica 802.11G en La Universidad Central "Marta Abreu" de Las Villas.

Autora: Izaite Franca e Almeida da Vera Cruz.

Tutor: MSc. Miriel Martín Mesa, MSc. Arelys Ramos Fleites.

Co-Tutor: MSc. Hiram de Castillo Sabido.

Santa Clara

Curso 2008-2009

"Año del 50 Aniversario del triunfo de La Revolución"

Universidad Central "Marta Abreu" de Las Villas

FACULTAD DE INGENIERÍA ELÉCTRICA

Departamento de Telecomunicaciones y Electrónica

TRABAJO DE DIPLOMA

Análisis de un sistema de supervisión para una red inalámbrica 802.11G en La Universidad Central "Marta Abreu" de Las Villas.

Autora: Izaite Franca e Almeida da Vera Cruz
Tutor: MSc. Miriel Martín Mesa, MSc. Arelys Ramos Fleites.

MSc. Arelys Ramos Fleites
Especialista en Ciencias Informáticas.
Administradora del nodo central de la red UCLV.
Dirección de Informatización - UCLV.
e-mail: arelys@uclv.edu.cu

MSc. Miriel Martín Mesa
Administrador del nodo central de la red UCLV.
Dirección de Informatización - UCLV.
e-mail: miriel@uclv.edu.cu

Co-Tutor: MSc. Hiram de Castillo Sabido
Prof. Dpto. de Telecomunicaciones y Electrónica
Facultad de Ing. Eléctrica. UCLV.
e-mail: hiramd@uclv.edu.cu

Santa Clara

Curso 2008-2009

"Año del 50 Aniversario del triunfo de La Revolución"

Hago constar que el presente trabajo de diploma fue realizado en la Universidad Central "Marta Abreu" de Las Villas como parte de la culminación de estudios de la especialidad de Ingeniería en Automática, autorizando a que el mismo sea utilizado por la Institución, para los fines que estime conveniente, tanto de forma parcial como total y que además no podrá ser presentado en eventos, ni publicados sin autorización de la Universidad.

Firma del Autor

Los abajo firmantes certificamos que el presente trabajo ha sido realizado según acuerdo de la dirección de nuestro centro y el mismo cumple con los requisitos que debe tener un trabajo de esta envergadura referido a la temática señalada.

Firma del Autor

Firma del Jefe de Departamento
donde se defiende el trabajo

Firma del Responsable de
Información Científico-Técnica

PENSAMIENTO

El genio comienza las grandes obras, pero sólo el trabajo las acaba"

Joseph Jouber

DEDICATORIA

Especialmente a mi madre Laurinda da Franca Almeida que, ha sido madre y padre, sin ella nunca lograría ser lo que soy hoy,

“ **Mimi você é tudo para mim nesta vida** *”.*

Te quiero mamá ❤️

A mi primo del alma Yarub Neto que aunque no esté mas en este mundo estará siempre presente en mi coración.

A mis hermanas Eyse, Milda y mi hermanito querido Ray que les quiero muchísimo.

AGRADECIMIENTOS

Primeramente quisiera agradecer a Deus por estar siempre conmigo y por todo lo que he logrado.

A mi madre Laurinda que siempre me dio la fuerza para seguir adelante.

A mis Tutores Arelys y Miriel por su paciencia y colaboración en la elaboración de esta Tesis.

A mis Profesores que sin ayuda de ellos no llegaríamos hasta aquí especialmente al profesor Hiram de Castillo.

A mi novio Samnio por estar siempre conmigo en todo y por suportarme..

A mi Tío Carlos Vera Cruz por toda la ayuda.

A todas mis amigas en especial (Lany, Indira, Anisa, Lay, Mariza, Nita, Hengue, Neuza) por la fuerza, amistad y paciencia que me han dado todo este tiempo.

A todos mis compañeros del aula especialmente a Kito, Davidson, Kesnila y Candida.

TAREA TÉCNICA

Las tareas a realizar en este trabajo son:

- Revisión de la bibliografía sobre el estado del arte en el campo de los sistemas de supervisión inalámbricos.
- Realizar un análisis de los sistemas de supervisión actuales en el mundo basado en licencia libre.
- Elaboración de la propuesta de solución para la supervisión de la red WIFI de La UCLV.
- Redacción y presentación del informe.

Firma del Autor	Firma del Tutor

RESUMEN

En el presente trabajo se hace un estudio de los diferentes sistemas de supervisión para redes de área local inalámbricas.

Se analiza los aspectos teóricos más importantes relacionados con la gestión y monitorización en redes de computadoras y se explica el protocolo necesario para realizar esta función.

En todos los casos se especifica donde encontrar información adicional con el fin de profundizar más en temas muy específicos.

Después del estudio de los diferentes sistemas se hace una breve comparación entre los mismos y el utilizado en la red Universitaria para determinar si existe la necesidad de implementar un nuevo sistema o se puede utilizar el existente.

Para finalizar se realizan las configuraciones pertinentes y se deja bien explícitos los resultados obtenidos.

TABLA DE CONTENIDOS

INTRODUCCIÓN

La universidad Central “Marta Abreu” de las Villas cuenta hoy con una red de computadoras que cubre el 95 % del área universitaria, con 14 enlaces principales y un total de 7 Km de fibra óptica, esta red fue creada en junio del año 2000 y cuenta hoy con más de 10 000 usuarios. Se brindan fundamentalmente, servicios de correo electrónico y acceso a Internet para todos nuestros profesores y estudiantes, y otras aplicaciones y servicios que son vitales para el trabajo docente e investigativo. Cuenta con una intranet bien consolidada donde están representadas todas las áreas universitarias.

En los últimos años se ha producido un crecimiento espectacular en lo referente al desarrollo y aceptación de las comunicaciones móviles y en concreto de las redes de área local inalámbricas conocidas por las siglas WLAN o por Wi-Fi que definimos como un sistema flexible que utiliza como medio de transmisión el aire, mediante Ondas de Radio o Luz Infrarroja. No obstante, Cuba, como otros tantos países en vías de desarrollo, ha asumido el reto de las redes WLAN; y ya varias empresas e instituciones se han sumado al empleo de las mismas.

En la zona central del país podemos citar como algunos ejemplos La OBE, Cayería Norte de Villa Clara, Radio Cuba, Etecsa, Copextel, Movitel, Cubalse, SEPSA, ECIE y La Universidad Central “Marta Abreu” de Las Villas (UCLV)(Fleites, 2007).

En La Universidad Central “Marta Abreu” de Las Villas (UCLV) ya desde algún tiempo se está haciendo uso de redes inalámbricas, una vez que el campus universitario es muy extenso, y había lugares que por las condiciones geográficas del terreno, era imposible llegar con el enlace por fibra óptica. De ahí hubo la necesidad de buscar otras variantes en la instalación de las redes de comunicaciones, para lograr llevar a todas las áreas

universitarias los servicios con que cuenta la red y que estaban totalmente incomunicadas. Ejemplo de ello es el enlace inalámbrico punto a punto entre La Facultad de Ingeniería Eléctrica y el Jardín Botánico.

El uso de las redes WLAN en La UCLV es una necesidad y más en los momentos actuales en que ha aumentado el numero de usuarios con Laptops y tarjetas para la conexión inalámbrica y con estas redes WI-FI tienen acceso a la información en tiempo real mientras se encuentran en movimiento y en lugares donde no se puede acceder a redes cableadas esto constituye una ayuda, una mejora, un proceso más eficiente y rápido cuando se quiere acceder a la información en la red desde cualquier punto de La Universidad.

Los motivos generales por los cuales se hace necesario el montaje de la misma son:

a) En un aula de reuniones donde las computadoras son instaladas de forma provisoria.
b) En una residencia o en un aula donde puede ser inviable romper paredes para instalar cables.
c) En situaciones donde hay la necesidad de mover computadoras.
d) En zonas donde resulta difícil hacer llegar el cable.
e) En la interconexión de redes de área local o sea interconectar dos o más redes de área local cableadas que se encuentran en lugares físicos distintos o por la congestión de la red cableada (Oliver y Escudero, 1999).

Las redes Inalámbricas surgen como una alternativa de las redes cableadas pero el sistema WLAN no pretende sustituir a las tradicionales redes cableadas, sino más bien complementarlas.

A nivel financiero y económico las redes inalámbricas se adecuan mejor que la red cableada porque ofrecen disminución continua del costo del equipamiento, además:

- Proporcionan al usuario movilidad sin perder conectividad.
- Flexibilidad en la localización de la estación, permitiendo a la red llegar a puntos donde el acceso es difícil para una LAN cableada.
- Fácil y rápida instalación y elimina el tendido de cables a través de paredes y techos.
- Escalabilidad, menos costos de mantenimiento que una red convencional, porque se pueden configurar en diversas topologías para cumplir con las necesidades de las instalaciones y aplicaciones específicas.

Los usuarios de una red inalámbrica, pueden transmitir y recibir voz, datos y vídeo dentro de edificios, entre edificios o dentro del campus universitario (Martinez, 2000).

Dentro de las desventajas que presentan estas redes están:

- La calidad de servicio es en algo más mala si la comparamos con las redes cableadas.
- Tienen velocidades de transmisión de datos más lentas.
- Es inestable o sea la intensidad de la señal oscila mucho.
- Tienen menos capacidad de ancho de banda aunque ya en la actualidad las redes WI-MAX han llegado al orden de los 100 Mbps.
- La seguridad como uno de los mayores problemas que tiene este tipo de tecnología (Martinez, 2000).

Actualmente se instalaron un grupo de 40 puntos de acceso inalámbricos (AP's) de la marca Trendnet modelo TEW-430APB con una antena de 5 DBi modelo TEW-A1750B en todas las áreas de la universidad. Estos AP's serán gestionados de forma independiente lo cual dificultará el conocimiento de los parámetros de funcionamiento de los mismos, haciendo que el personal encargado de supervisarlos sean los últimos en enterarse de los problemas que ocurran en estos equipos. El modelo TEW-430APB no cuenta con el protocolo SNMP lo que también dificulta su gestión y aparte a esto el sistema de supervisión con que cuenta la Universidad no está apto para realizar esta función.

El objetivo principal del trabajo es analizar y hacer una propuesta de solución de un sistema que pueda gestionar y supervisar el servicio inalámbrico brindado por cada uno de los AP's instalados en la UCLV, utilizando preferiblemente soluciones de Software libre existentes.

Como objetivos específicos se encuentran:

- Indagar sobre las diferentes soluciones existentes para el monitoreo de redes WIFI.
- Caracterizar las tecnologías WIFI instaladas en La Red UCLV.
- Determinar los parámetros que serán tenidos en cuenta para el monitoreo de los puntos de acceso.

- Proponer una solución de supervisión para la red WIFI.

Organización del informe

Este trabajo se ha estructurado en: Introducción, dos Capítulos que abordan las tareas anteriormente citadas, Conclusiones, Recomendaciones, Referencias Bibliográficas, Glosario de términos y Anexos. A continuación se describen brevemente los contenidos de cada uno de los capítulos de este informe.

En el capítulo I se realiza una revisión bibliográfica sobre los aspectos teóricos de los Sistemas de Supervisión actuales en el mundo basados en el software Libre. También se explican aspectos importantes sobre Gestión y Monitoreo de redes de computadoras y los protocolos que se utilizan para realizar esta tarea.

En el capítulo II se deja planteada la propuesta del sistema de supervisión que se pretende utilizar, se realizan las pruebas y la configuración del software y se dejan explícitos los resultados obtenidos. Se hace una breve descripción del punto de acceso especificando sus características técnicas y el mapa de distribución por todo el campus universitario también se realiza un análisis económico referente al equipo supervisado. Se dan conclusiones y recomendaciones.

CAPÍTULO 1. Estado del arte sobre los sistemas de supervisión Inalámbricas

Una red puede ser supervisada o monitoreada utilizando un software instalado en una computadora personal o algún servidor destinado a realizar esta función. Generalmente el administrador de red es el encargado de supervisar los dispositivos de la red que pueden ser puntos de acceso, Routers, Switch, etc. En este trabajo se supervisar el sistema inalámbrico instalado en La UCLV.

Se pretende en este capítulo abordar los aspectos teóricos relacionados con la supervisión de redes de computadoras y hacer una búsqueda sobre los sistemas de supervisión utilizados actualmente.

1.1 Gestión de Redes

No podemos hablar de sistemas de supervisión sin hablar de Gestión de redes; porque la monitorización o supervisión es una forma básica de actuación que posee la gestión de red. Gestión de Redes es la supervisión, la obtención de información y el control de dispositivos inteligentes distribuidos a lo largo de una red de computadoras. Para lograr esto se crea un canal de gestión, que está compuesto por un agente (agent) y una estación de monitoreo que se comunican mediante un protocolo preestablecido conocido como SNMP (Simple Network Management Protocol) (Dominguez, 2004).

Más detalladamente se muestra a continuación la arquitectura típica de la gestión red (Figura 1. 1), donde el administrador de la red interactúa con el sistema de gestión mediante una interfaz llamada aplicación de gestión que se comunica con los dispositivos

gestionados mediante los agentes que estos tienen incluidos establecida mediante un protocolo de gestión (Albalate, 2007).

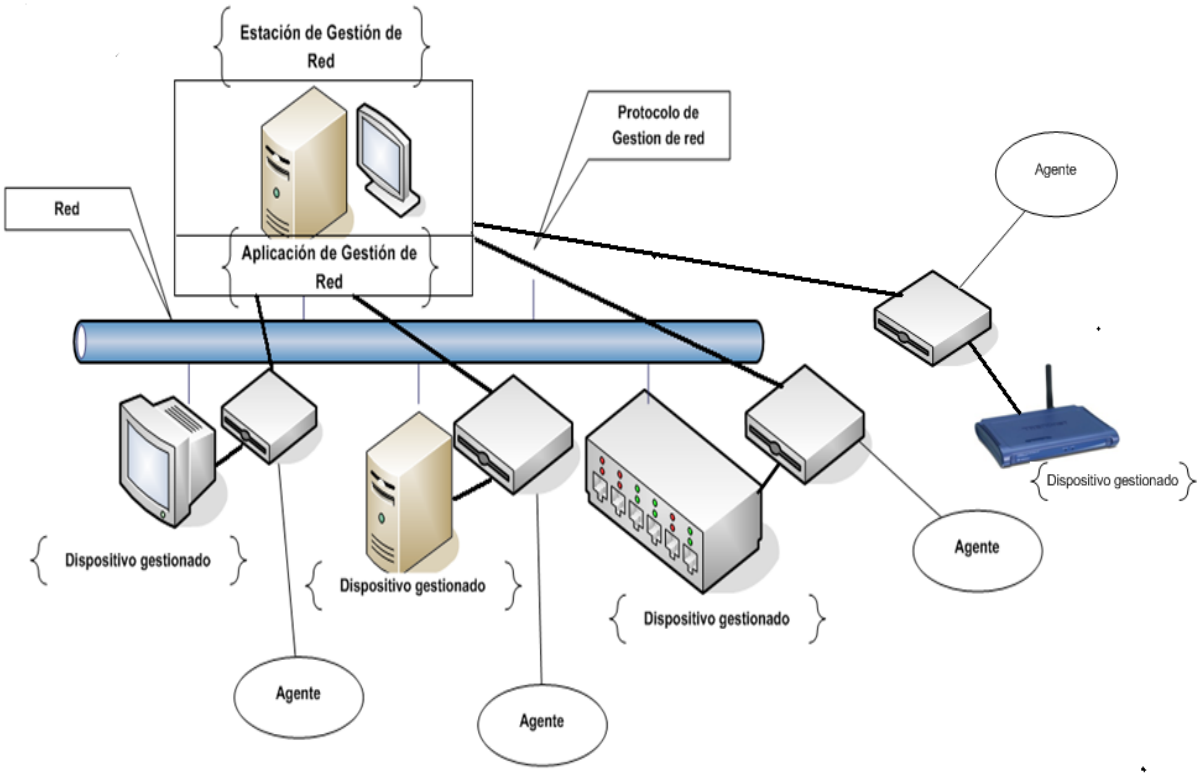


Figura 1. 1. Figura Arquitectura típica de la gestión de Red

Gestión de Red surge para dar solución al problema del crecimiento de las redes porque en una red pequeña el administrador de red puede darse cuenta rápidamente cuando ocurre algún problema.

1.2 Monitorización o supervisión de redes

El monitoreo de redes permite recolectar información necesaria para administrar una red(Inchauspe, 2001), ayuda a prevenir problemas y a obtener tiempos de respuesta menores ante incidencias debido a que en una red monitorizada el administrador esta siempre pendiente de todos los detalles facilitando una respuesta inmediata frente a las anomalía que presenta la misma .

Este sistema se considera como una función de lectura y se encarga de observar y analizar el estado de la red y el comportamiento de la configuración de sus componentes, engloba todas las operaciones de obtención de datos acerca del estado de los recursos cuyo

procesamiento posterior va al sistema de gestión y utilizar los procesamientos de control para actuar sobre el comportamiento de la red gestionada (Albalate, 2007).

Supervisando una red se obtiene la determinación y representación gráfica de las condiciones de funcionamiento de un sistema real en tiempo real.

El monitoreo de redes es necesario en ambientes distribuidos, como la arquitectura cliente servidor, ya que hay que tener en cuenta situaciones críticas para el funcionamiento de la red; para advertir las necesidades de crecimiento; poder administrar redes complejas y poder deducir los recursos necesarios para el funcionamiento de la misma. Para la realización de la misma se deben cumplir con tres áreas fundamentales del monitoreo de redes: el monitoreo de prestaciones, el monitoreo de fallas y el monitoreo de contabilidad (Inchauspe, 2001) pero Albalate (2007) complementa que las áreas de configuración y seguridad también son importantes.

La gestión de configuración: Trata el control de inventario de los componentes individuales y los subsistemas de la red, así como su localización y las licencia de software. Para realización de la misma se debe tener en cuenta los siguientes pasos:

- Realización de la información de la configuración.
- Establecer y modificar los valores de configuración.
- Definir y cambiar las relaciones entre los componentes.
- Iniciar y finalizar operaciones de red.
- Distribución de software.
- Mapas de red.
- Descubrimiento de recurso.
- Bases de datos.

La gestión de prestaciones: Evalúa el comportamiento de la red y para ello utiliza indicadores como la disponibilidad (porcentaje de tiempo que un componente está disponible para los usuarios); factor de bloqueo (la cantidad de usuarios que en teoría no pueden acceder a la red por encontrar ocupada la señal; el tiempo de respuesta (el tiempo transcurrido hasta que se recibe la respuesta de un dispositivo de la red); exactitud (la cantidad de paquetes defectuosos en la red en un determinado período de tiempo); el

throughput (el número de paquetes atómicos que transitan la red en un determinado período de tiempo).

La gestión de fallas: Testea la conectividad entre distintas direcciones de la red, la integridad de los datos, las congestiones que se producen, etc. La Administración de fallas implica los siguientes pasos:

- Primero se determinan los síntomas y se aísla el problema.
- Entonces el problema es fijo, y la solución se prueba en todos los subsistemas. importantes.
- Finalmente la detección y la resolución del problema son registradas.

La gestión de contabilidad: Determina si se están utilizando los recursos de forma eficiente y permite planificar la asignación de carga de trabajo a determinados sectores de la red así como también permite planificar futuros crecimientos de la red.

La gestión de seguridad: Su objetivo es asegurar la seguridad de red de forma tal que la misma no sea saboteada. Por tanto ella encarga de que se cumplan los siguientes requisitos:

- Privacidad; a la información solo debe acceder aquel que esté autorizado.
- Integridad; las características de sistema solo deben poder modificarse por personas autorizadas.
- Disponibilidad; los recursos deben estar disponibles para los usuarios a los que están destinados.

En alguna ocasión realizan informes que posibilitan el uso de la información recabada en la toma de decisiones para mejorar el rendimiento de la red.

La información sobre supervisión de la red de transmisión servirá de orientación para la aplicación de los controles de tráfico y también puede ser de utilidad para el Punto de Control del Restablecimiento al establecer las prioridades correspondientes.

Una información oportuna permitirá al gestor de la red conocer el estado de esta y proceder al control/reconfiguración de los flujos de forma inmediata, en vez de actuar reactivamente una vez que se haya producido una congestión de tráfico o se haya detectado una calidad de funcionamiento inadecuada.

La motorización según Albalate (2001) consta de las siguientes fases:

Definición de la información de gestión que se monitoriza se divide en: Información estática (caracteriza la configuración de los recursos y no cambia con la actividad de la red y generalmente está almacenada en los elementos monitorizados), información dinámica (cambia con la actividad de la red y suele estar almacenada en los propios elementos monitorizados o en equipos especializados), información estadística (se genera a partir del pos-procesado de la información dinámica y proporciona mayor significado a la gestión, puede residir en cualquier sitio que tenga acceso a la información dinámica y que tenga capacidad de procesar dicha información).

Acceso a la información de monitorización: Tiene como objetivo la monitorización remota de los recursos, para lo cual necesita una cooperación entre los gestores y los equipos gestionados. Esta cooperación se realiza a través de un método común de acceso a la información de gestión independientemente de la tecnología o del fabricante del equipo monitorizado.

Diseño de mecanismo de monitorización: Sondeo o polling (acceso periódico del gestor a la información de monitorización o gestión). Este posee la ventaja de que los agentes solo deben estar preparados para responder, lo cual posibilita su simplicidad, de esta manera se descarga la complejidad hacia los gestores**),** informe de Eventos (Event Reporting) o notificaciones a los propios recursos (a través de los agentes y por propia iniciativa, envían notificaciones a los gestores bajo ciertas condiciones esto minimiza el trafico de gestión por la red y balancea la complejidad entre gestores y equipos gestionados).

Procesado de la información de monitorización: Depende de la aplicación de gestión asociada (configuración, fallo, prestaciones, contabilidad y seguridad) ya mencionadas.

Esta información puede ser presentada de varias formas fundamentales, en pantallas de video, mediante representaciones graficas en un tablero de visualización o consola de gestión.

1.2.1 Evolución del monitoreo de redes

Las primeras herramientas utilizadas para el monitoreo de redes fueron herramientas muy simples como *ping*, para detectar la conectividad entre direcciones; *arp* para detectar interfaces de red; *traceroute*, para detectar posibles rutas para que un paquete alcance su

destino; *telnet* y *finger* para chequear el funcionamiento de las operaciones con el protocolo TCP; *netstat*, para ver las tablas de ruteo en sistemas UNIX (Inchauspe, 2001).

SNMP (Simple Network Management protocolo) o protocolo simple de administración de redes es el protocolo más utilizado para esta tarea. Comúnmente se usa sobre un protocolo de transporte no orientado a la conexión, que generalmente es UDP. Este protocolo se explica más adelante.

1.3 Plataforma de gestión de red

Las plataformas de gestión de redes proporcionan el soporte común para las aplicaciones de gestión y herramienta asociadas. Para ello se pueden apoyar en protocolos de gestión e interfaces normalizadas (Albalate, 2007).

Se deben tener en cuenta diferentes aspectos a la hora de elegir la plataforma de red como:

Aplicaciones genéricas o propias: Son aquellas que forman parte del software de gestión y proporcionan la supervisión coherente y eficaz de los elementos a gestionar en la red realizando el inventario de dichos elementos y la gestión de los mapas físicos además de recoger y presentar en tiempo real todos los acontecimientos, deben proporcionar todos los servicios reactivos al manejo de alarmas (registros de incidencias históricas de las alarmas) de un sistema de gestión registrando todas las alarmas que ocurren y manejando las activas.

Interfaz para el programador de aplicaciones (API) para la integración de otras aplicaciones de gestión: El software de gestión debe proporcionar facilidad para la integración de aplicaciones de gestión ya sean del proveedor de dicho software de gestión o de terceros.

Las APIs garantizan la apertura de software y se recomienda que estén basadas en estándares internacionales como por ejemplo La X/Open, la interfaz de gestión Java para el Programador de aplicaciones (JMAPI, del ingles Java Management APIs), etc. También el software puede poseer herramientas para los desarrollos de agentes y aplicaciones de gestión.

Seguridad que posee: La interfaz de usuario, o consola de gestión del software de gestión se debe proteger. Para esto se emplean nombres de usuarios, contraseñas y perfiles de

usuario. Además, el intercambio de la información de gestión entre agentes y gestor debe estar protegido a través de la autenticación.

Sistemas Operativos sobre los que se soporta: El software de gestión debe estar soportado por los sistemas operativos más comunes, o sea Windows de Microsoft, Linux, Unix, etc. Cada sistema operativo tiene sus ventajas, pero el Windows es uno de los más usados en el mundo y es muy amigable.

Interfaz de usuario: La interfaz de usuario es el punto de contacto de los usuarios de la gestión con el software, por lo que este debe proveer una Interfaz gráfica de usuario (GUI) por las ventajas que ofrece la misma, la cual debe integrar a todos las aplicaciones de gestión y que tenga una arquitectura modular donde cada módulo puede funcionar por si solo con su consola independiente.

Protocolo de gestión que soporta: Para gestionar las redes TCP/IP el protocolo empleado tradicionalmente es el SNMP aunque es conveniente que el software de gestión soporte el mayor número posible de estos protocolos.

Base Web: Se debe analizar si el software de gestión brinda soporte para la gestión basada en web.

Requerimiento del Sistema: El hardware necesario para el buen funcionamiento del software de gestión debe estar en correspondencia con las posibilidades reales de que exista o se pueda adquirir por la institución y con la arquitectura de gestión a emplear, distribuida o centralizada, con agentes inteligentes.

Precio: Es otro aspecto a tener en cuenta a la hora de seleccionar en tener varias opciones.

1.4 Protocolo de gestión

Para realizar la supervisión de los AP’s se depende enteramente de un protocolo que ayude en la realización del mismo, el más conocido para esta aplicación es SNMP aunque existan otros protocolos.

El SNMP (protocolo simple de administración de red) es un protocolo de capa de aplicación que facilita el intercambio de información entre los dispositivos de la red, además permite a los administradores supervisar el desempeño de la misma (Rios, 2009)

para posteriormente resolver sus problemas y para ello planear o generar nuevas políticas para el crecimiento de la red (Orozco, 2009).

Tuvo su primera versión en el año 1988, cuando se presentó como un protocolo básico para la administración de redes (SNMPv1). La segunda versión del protocolo se llama SNMPv2 apareció en el año 1993 que tuvo el objetivo de mejorar la transferencia de información entre agentes y gestores, y aunque la propuesta del protocolo incluía cuestiones de seguridad, las mismas no pudieron ser implementadas, su conclusión fue en 1994(Domínguez, 2004) con la introducción de la tercera versión.

SNMP Versión 1 (SNMPv1): Es la versión estándar del protocolo SNMP. Está definida en la RFC[1] 1157 y es un estándar completo de la IETF[2](Domínguez, 2004).

La seguridad de SNMPv1 se basa en comunidades, que no son más que palabras claves, cadenas de caracteres en texto plano que permiten a las aplicaciones basadas en SNMP ganar acceso a la información del dispositivo gestionado.

Los agentes que implementan dicha versión del protocolo disponen generalmente de dos comunidades, una de dichas comunidades recibe el nombre de comunidad pública, y sus variables pueden ser accedidas sólo para lectura. Por el contrario los valores asociados a las variables que componen la otra comunidad, denominada comunidad privada, pueden ser modificados (Fernández et al., 2008).

Versión 2 (SNMPv2): Esta es técnicamente referenciada como SNMPv2c, está declarada en La RFC 1905, RFC 1906 y RFC 1907 y también se basa en comunidades y utiliza los dos tipos de comunidad que utiliza la versión anterior, la misma se usa para acceder a una computadora.

En una red gestionada por SNMP el se encarga de monitorizar los elementos especificados y en caso de detectar cualquier anomalía en su funcionamiento avisa a la persona responsable de solucionarlo mientras que para una red no gestionada si ocurre alguna falla

---

[1] Son documentos que deben ser primeramente una propuesta para estándar, luego un *drafts* y solo cuando se aprueben adquieren el nivel de estándar.

[2] Es la responsable de la definición de los estándares que gobiernan el tráfico en Internet.

en el sistema la persona responsable puede tardar en percatarse del problema y las pérdidas podrían ser enormes. Una de las ventajas de este protocolo es que permite a los especialistas contar con información que facilita la previsión de fallas en los sistemas (Domínguez, 2004).

1.5 Protocolo RMON (*Remote Monitoring*)

Muchas implementaciones de SNMPv1 *y* SNMPv2 debieron ser limitadas a aplicaciones de solo lectura por la falta de encriptación y la falta de autenticación. Además el protocolo se implementaba solamente con un gestor y varios agentes; un modelo que se vuelve ineficiente cuando el tamaño de las redes crece. Luego apareció RMON (monitoreo remoto) un estándar basado en el protocolo SNMP que agregó a las redes dispositivos compiladores de RMON que se llaman "monitors" o "proves". RMON provee estadísticas de alto nivel, para las cuales debieron agregarse grupos en el MIB (Inchauspe, 2001).

Este protocolo se utiliza para desarrollar el proceso de monitorización, es un estándar que define objetos actuales e históricos de control, permitiendo que se capture la información en tiempo real a través de la red entera y proporciona una información más detallada y a la vez fácil de recopilar. El estándar de RMON es una definición para Ethernet (Domínguez, 2004). Eso provocó que se fuera diversificando la estructura necesaria para el monitoreo de redes.

Existen dos versiones de RMON:

Versión-1: RMONv1: Brinda a los NMS estadísticas a nivel de paquetes sobre la LAN o la WAN.

La Version-2: RMONv2: Brinda no solo información al nivel de red sino que dispone de datos a nivel de aplicaciones. Estas estadísticas pueden ser reunidas de varias formas, una de ellas es situando “sondas RMON” en cada uno de los segmentos de la red que se desee monitorear.

Se creó MIB de RMON para permitir a las sondas de RMON trabajar sin necesidad de contactar al NMS durante un periodo de tiempo el cual aprovechan para recolectar información. Luego NMS puede solicitar esa información a la sonda RMON. Otra de las ventajas de RMON es que se pueden ejecutar hilos que chequeen por ciertas condiciones y

en caso de la ocurrencia de un error o de una alerta se avisa al NMS a través de una trap[3] (Puentes, 2004).

1.6 Evolución de la seguridad proporcionada por el protocolo SNMP

SNMPv3, es la última versión del protocolo SNMP incluye la funcionalidad de las versiones anteriores.

Versión 3 (SNMPv3*):* Está definido en las RFC 1905, 1906, 1907, 2571, 2572, 2573, 2574 y RFC 2575. Adiciona soporte al uso de métodos mucho más seguros para la autentificación y la comunicación entre las entidades involucradas tiene como principales objetivos (Inchauspe, 2001; Domínguez, 2004):

- ✓ proporcionar seguridad a través de la verificación de la integridad del mensaje (asegurar que el paquete no haya sido violado durante la transmisión), encriptación (como forma de prevención) y la autentificación (permite determinar si el mensaje proviene de una fuente válida).
- ✓ utilizar al máximo posible el hardware existente.
- ✓ proveer compatibilidad con el software existente.
- ✓ facilitar la implementación de actualizaciones del protocolo.
- ✓ posibilitar el soporte necesario para el monitoreo de grandes redes.
- ✓ llevar a cabo estos objetivos de una forma sencilla y relativamente barata.

En dicha versión una entidad SNMP se considera compuesta por un motor y una aplicaciones (Fernández et al., 2008).

El motor se divide en cuatro módulos:

Dispatcher (Distribuidor): Es un manejador de tránsito que permite soporte a mensajes de múltiples versiones del protocolo SNMP. Como ejemplo: Intercambiar mensajes con la red (enviar y recibir mensajes), colecciona estadísticas a cerca de las versiones de mensajes SNMP recibidos y enviados, proveer una interfaz abstracta a las aplicaciones SNMP para entregar PDU's a las otras aplicaciones y a entidades remotas.

[3] Es la dirección IP a donde son enviados los avisos por parte del agente.

Subsistema de proceso de mensajes: Prepara los mensajes para que sean enviados agregándoles el header (encabezado) correspondiente a la versión necesaria y extrae los datos de los mensajes recibidos.

Subsistema de seguridad: Es responsable de proveer los servicios de seguridad que pueden ser autenticación y privacidad en el mensaje. Este subsistema verifica se los mensajes SNMP que se reciben no hayan sido modificados durante la transmisión, cuida la privacidad de la información enviada y recibida, etc.

Subsistema de control de acceso: Posibilita restringir el acceso al MIB y limitar las operaciones que los gestores pueden realizar sobre los agentes.

Las aplicaciones están formadas por:

Aplicación Respondedor de Comandos: Recibe las solicitudes destinadas al sistema local y luego deberá desarrollar la operación de protocolos necesaria para generar una respuesta adecuada y reenviarla a la entidad solicitante. Deberá utilizar control de acceso para verificar si el solicitante está autorizado a obtener esa información u ordenar la modificación de datos. Una vez recibida la solicitud y determinado que el mensaje debe responderse, esta aplicación deberá determinar el tipo de mensaje entrante, comunicarse con la base de datos, preparar la respuesta y luego entregar esa respuesta al Dispatcher para que éste la envíe. Si por el contrario se determina que esa solicitud no debe responderse se envía al solicitante un mensaje comunicando una falla en el acceso.

Aplicación Creador de notificaciones: Es el encargado de monitorear al sistema ante condiciones o eventos particulares y, de producirse una anormalidad, genera un mensaje Trap o Inform relativo a esas condiciones monitoreadas. El Creador de notificaciones actúa de la siguiente manera: Primero, empleando mecanismos de filtro apropiados se determina cuál es la información que debe enviarse. Si el filtro determina que una notificación no debe enviarse se continúa el proceso, sino se recuperan variables de la Base de datos de Información local que permitan determinar la entidad a la que se le debe enviar el mensaje, el modelo de seguridad a utilizar y el nivel de seguridad requerido. Luego se hace una verificación para determinar si debe enviarse o no la notificación. Una vez concluidos estos pasos se construye una PDU que si no necesita respuesta se envía al Despachador, en caso contrario antes de que la PDU sea enviada al Despachador se indica la necesidad de una

respuesta, se cachean los datos del gestor al que se le envió la información ante la posible necesidad de retransmitir los datos [RFC 2573].

Aplicación Receptor de Notificaciones: Espera en modo pasivo la llegada de mensajes de notificación. Los mensajes de notificaciones son Inform (de gestor a gestor) y Trap (de agente a gestor). Si el mensaje que se recibe es de tipo Inform deberá responderse. Lo primero que hace el Receptor de Notificaciones es registrar la llegada de la notificación y determinar de qué tipo de notificación se trata. Si se necesita una respuesta la prepara y se la envía al Despachador.

Aplicación Proxy Forwarder: Es una aplicación de implementación opcional, se implementa si:

- Hay partes de la red que no soportan el protocolo SNMP.
- Cuando es necesario tener información en cache para minimizar la carga de trabajo de los dispositivos.
- Para autentificar y autorizar peticiones.

A continuación se presenta un resumen sobre lo explicado en la Figura 1. 2.

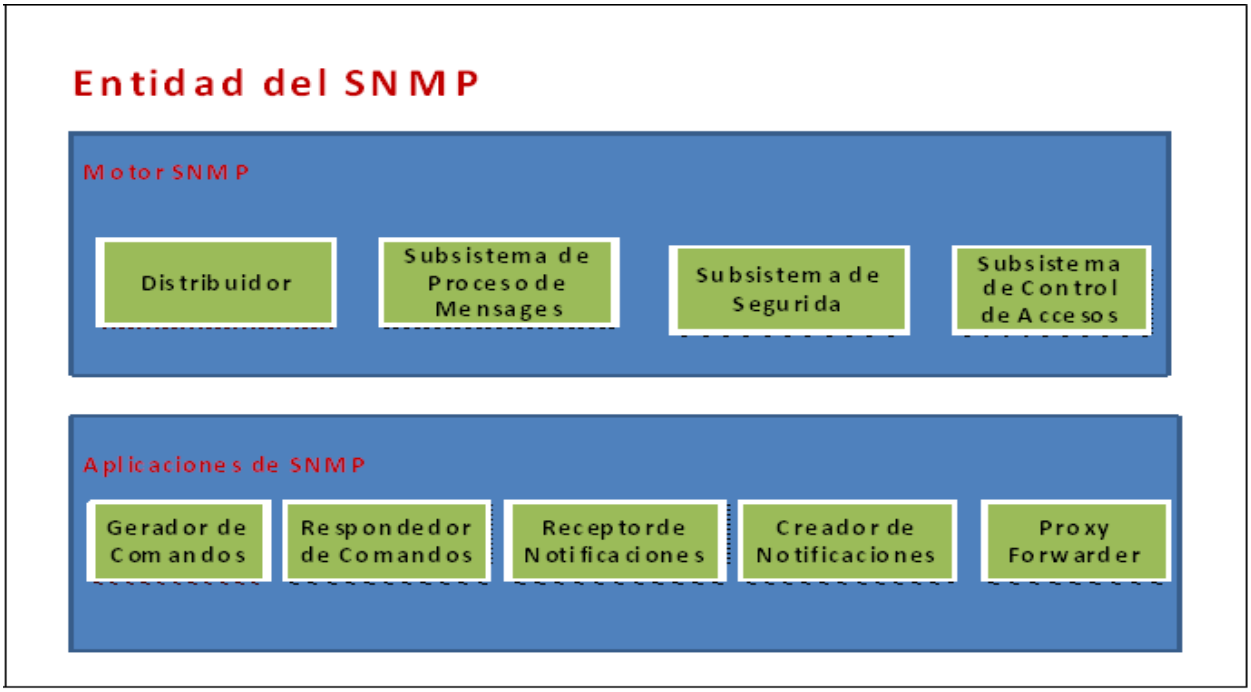


Figura 1. 2. Arquitectura de SNMP version3

1.7 Componentes básicos de SNMP

Una red administrada a través de SNMP consiste de tres componentes claves: dispositivos administrados, agentes y sistemas administradores de red (NMS's) (Member**,** 2006).

Un dispositivo administrado es un nodo de red que contiene un agente SNMP y reside en una red administrada. Estos recogen y almacenan información de administración, la cual es puesta a disposición de los NMS's usando SNMP. Este dispositivo de la red muchas veces se le llama como elemento de la red que puede ser: routers, servidores de acceso, switches, bridges, hubs, computadores o impresoras.

Un agente es un módulo de software de administración de red que reside en un dispositivo administrado. Este posee un conocimiento local de información de administración, la cual es traducida a un formato compatible con SNMP. Es responsable de responder a los comandos ejecutados por el gestor para modificar los parámetros de operación o configuración local, proporcionar información al gestor; ya sea solicitada o avisando anormalidades; y para poder llevar a cabo esas tareas deberá recolectar y mantener información sobre la configuración y funcionamiento del ambiente local en una base de datos (Inchauspe, 2001).

Un NMS ejecuta aplicaciones que supervisan y controlan a los dispositivos administrados, ellos proporcionan el volumen de recursos de procesamiento y memoria requeridos para la administración de la red. Estos elementos pueden comunicarse entre sí a través de cuatro funciones básicas que se encapsulan en la PDU, aunque no es obligatorio que las aplicaciones la soporten a todas: *Get*, *Set*, etc.

A través de la función *Get* el gestor solicita información al agente y a través de Set el gestor envía órdenes al agente de resetear o modificar el contenido de las variables de su base de datos.

Los agentes escuchan o envían y reciben peticiones por el puerto 161 y las estación estaciones gestoras (NMS) escuchan los trap por el puerto 162(Stallings, 1999).

1.8 Característica de SNMP

El SNMP brinda a los usuarios un conjunto muy simple de instrucciones que permiten que los dispositivos que lo soporten sean gestionados de forma remota. Puede ser usado para

gestionar sistemas basados en UNIX o en Windows, impresoras, *rack* de MODEMs o fuentes de respaldo, y supervisar servidores de Web, de archivos o de bases de datos.

El protocolo SNMP está definido sobre un modelo cliente/servidor donde el gestor actúa como un cliente enviando solicitudes al agente y espera la respuesta. En resumen el programa cliente, conocido como *network manager* (administrador de red) o NMS (*Network Management Stations*) crea conexiones virtuales hacia un programa servidor llamando SNMP agent (*agente de SNMP*) el cual se ejecuta en un dispositivo de red remoto y brinda información al *manager* sobre su estado (Domínguez, 2004).

La Figura 1. 3 nos puede demostrar el vínculo existente entre el NMS y el Agent.

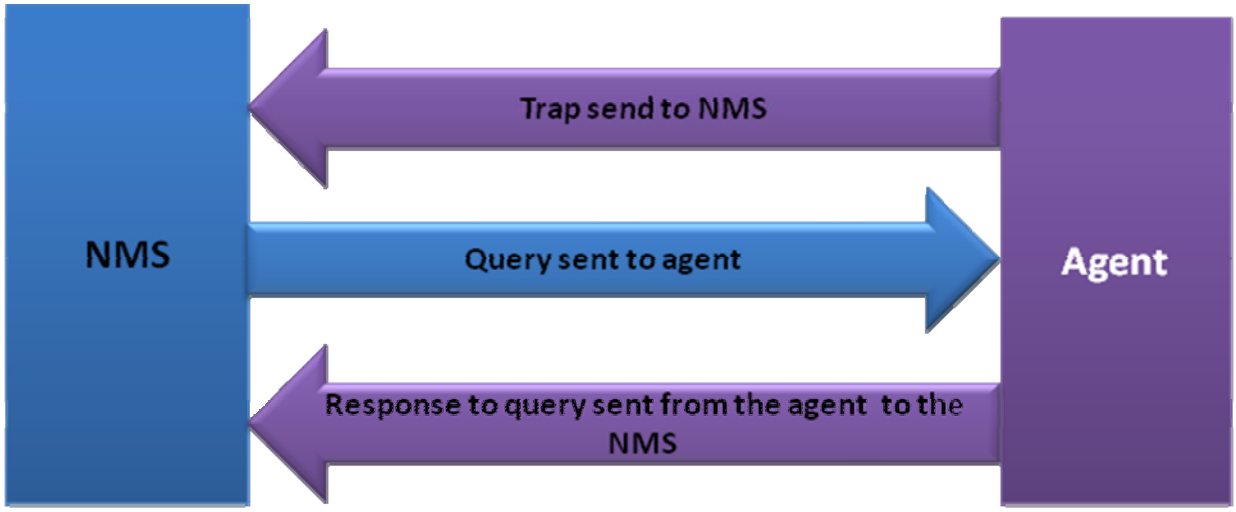


Figura 1. 3. Relación entre un NMS y un Agent

SNMP usa UDP (*User Datagram Protocol*) como protocolo de transporte para intercambiar datos entre el NMS y el agente. UDP representa una carga más ligera para el tráfico de la red que una conexión por TCP.

El protocolo UDP está definido en la [RFC 768] y fue elegido sobre TCP (*Transmisión Control Protocol*) porque no es orientado a conexión lo que significa que no existe una conexión de extremo a extremo o *end-to-end* por donde los datos puedan ser enviados y recibidos (Domínguez, 2004).

Esta característica de UDP lo hace más confiable porque no hay nunca un reconocimiento de que se pierden paquetes. Corresponde solo a las aplicaciones determinar si se están perdiendo paquetes o no, y si se puede tolerar esto o no sin dar una alarma. El método más

usado generalmente es el de esperar un intervalo de tiempo por los datos (*timeout*). [RFC-1067]

SNMP está diseñado para ser usado en redes con problemas, redes en las cuales la comunicación entre dos dispositivos es algo que puede fallar en cualquier momento, es en ese ambiente donde UDP ha demostrado su superioridad sobre TCP.

La Figura 1. 4 muestra la relación que existe entre SNMP, UDP e IP.

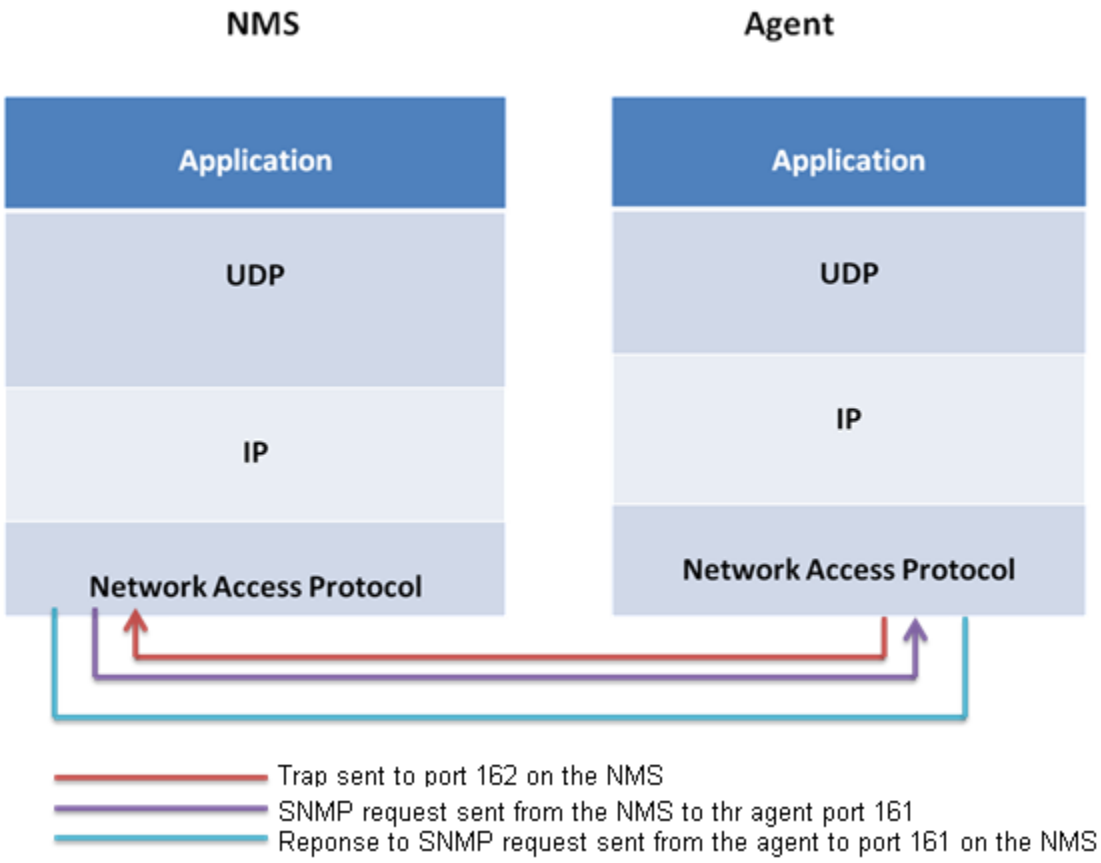


Figura 1. 4 Protocolos TCP/IP y SNMP

En la figura:

Aplicación (Aplication): La aplicación de SNMP (agente o NMS) decide qué es lo que quiere hacer, por ejemplo solicitar el valor que representa la cantidad de bytes enviados por una de las interfaces de un switch.

UDP: Esta capa le permite a la estación que se está usando para gestionar la red comunicarse con el dispositivo que se va a encuestar. Por lo que un paquete tipo UDP es enviado al puerto 161 del Switch.

IP: La capa IP solo debe tratar de entregar ese paquete a la dirección IP que tiene el dispositivo que se desea encuestar, o sea el switch del ejemplo.

1.9 Comandos básicos de SNMP

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

El comando de lectura es usado por un NMS para supervisar elementos de red. El NMS examina diferentes variables que son mantenidas por los dispositivos administrados.

El comando de escritura es usado por un NMS para controlar elementos de red. El NMS cambia los valores de las variables almacenadas dentro de los dispositivos administrados.

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

Las operaciones transversales son usadas por el NMS para determinar qué variables soporta un dispositivo administrado y para recoger secuencialmente información en tablas de variables, como por ejemplo, una tabla de rutas (Member, 2006).

1.10 Base de Dato del SNMP (MIB)

La MIB o base de información de gestión (*Management Information Base*) es una colección de objetos que representa de forma abstracta los dispositivos de red y sus componentes internos (Inchauspe, 2001). Cada empresa puede personalizar la base de datos según sus necesidades pero siguiendo las reglas especificadas en el SMI (estructura de gestión de información).

SMI presenta un marco general donde se especifica el MIB. Define los objetos gestionados y como acceder a ellos. No soporta la creación ni recuperación de datos complejos para mantener la simplicidad y facilitar la implementación de las estructuras.

Las directivas enviadas por el cliente a un agente de SNMP consisten en los identificadores de las variables de SNMP, también conocidas como variables MIB o MIB object identifiers (identificadores de objetos de una MIB) y en una instrucción de pedir el valor (*get*) o de establecer el valor (*set*) (Domínguez, 2004).

Los nombres de las variables MIB se definen de acuerdo con la norma ASN.1 (*Notación de Sintaxis Abstracta.1*); todas las variables MIB tienen nombres jerárquicos ASN.1 grandes que se traducen en una representación numérica más compacta para su transmisión. Aunque La ASN.1 no incluye una operación de indización de los tipos de datos agregados como tablas o arreglos, una variable MIB puede ser una tabla; la información de indización se agrega al nombre (Albalate, 2007).

Una base de información de administración (MIB) es una colección de información que está organizada jerárquicamente. La jerarquía MIB puede ser representada como un árbol (Member, 2006).

Es importante saber cómo son los datos en el contexto de SNMP. En [RFC-1155] se explica y se especifica cómo son nombrados y de qué tipo son los objetos gestionados (*managed objects*) más comunes.

La definición de los objetos gestionados puede ser separada en tres partes:

Name: El nombre o el *object identifier* (OID) que representa a un objeto especifico. Se puede mostrar en dos formas: numérico o en una cadena de caracteres entendible por humanos. En cualquiera de los casos es algo muy largo y difícil de memorizar. En las aplicaciones SNMP se dedica gran parte del trabajo a ayudar a los administradores a navegar a través de estos OID.

Tipo y sintaxis: El tipo de datos de un OID es definido usando ASN.1, esta es la forma de especificar cómo los datos serán representados y transmitidos entre el *manager* y el agente. Lo bueno acerca de ASN.1 es que no depende de la arquitectura de la máquina, facilitando así la comunicación entre por ejemplo una estación Windows y un SPARC con UNIX de Sun.

Codificación: Una instancia de un OID esta codificada en una cadena de octetos usando BER (*Basic Encoding Rules*). BER define cómo los objetos son codificados y decodificados para que puedan ser transmitidos sobre el medio de transporte.

Los OID están organizados en una jerarquía en forma de árbol de tres ramas iníciales (Domínguez, 2004). Esta estructura es la base del esquema de nombres de SNMP.

El identificador de un objeto está compuesto por una serie de enteros separados por puntos que se obtienen de la ruta desde el inicio del árbol hasta el objeto en cuestión. En la Figura 1. 5 se detallan algunos niveles de este árbol.

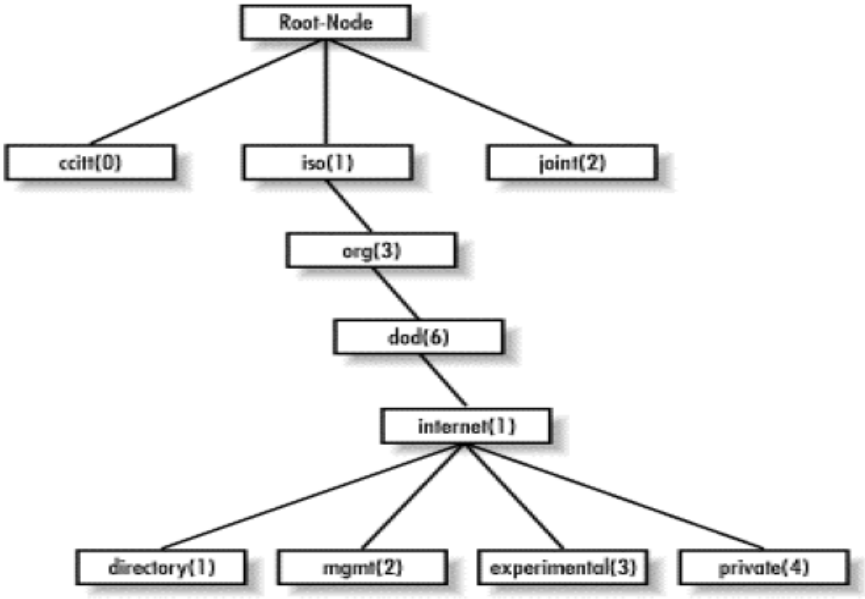


Figura 1. 5. Árbol de objetos SMI o SMIv1.

La parte superior del árbol de objetos es llamada *root* o raíz, cualquier nodo con hijos se conoce como *subtree* y cualquier nodo sin hijos es llamado hoja o *leaf*.

Cuando se habla por ejemplo del nodo *mgmt* se puede referenciar de dos formas: la primera es la que se usa en el protocolo y es la secuencia de los números separados por puntos, esto es 1.3.6.1.2.

La segunda forma es más usada por las personas y consiste en unir los nombres de los nodos, por ejemplo: *iso.org.dod.internet.mgmt*.

La rama *directory* no está en uso actualmente.

La rama *mgmt* define un grupo de objetos estándares para la gestión en redes IP

La rama *experimental* por su parte se reserva para objetos de pruebas y de investigaciones.

La rama *private* está repartida entre los fabricantes de equipos que soportan SNMP de forma que todos dispongan de un área donde poner objetos específicos de sus equipos.

Hubo también una segunda versión SMIv2 donde se extiende el árbol de objetos agregando una rama llamada *snmpv2* a la rama de Internet, y nuevos tipos de datos. Además aparecen los campos siguientes: UNITSPARTS, MAX-ACCESS, STATUS, AUGMENTS. Los cuales se usan para controlar cómo son accedidos los objetos, para obtener mejores descripciones y para aumentar una tabla adicionando columnas (Albalate, 2007).

Con el pasar del tiempo la MIB se hizo ineficiente para resolución de algunos casos y se define una extensión, la MIB-II (Domínguez, 2004), adicionando algunas ramas en el árbol de la MIB original.

La MIB-II (Management Information Base Second Part) es un grupo muy importante de objetos gestionables porque cada dispositivo que soporte SNMP debe también soportarlos. Dada la importancia de este aspecto es bueno aclarar que un agente puede soportar varias MIBs, como por ejemplo una para ATM (RFC 2515), o la especificada en La RFC 1611 relacionada con servidores de DNS pero es de carácter obligatorio que soporte la MIB II(Domínguez, 2004).

A continuación se explica cómo está distribuida la MIB-II:

System (1.3.6.1.2.1.1) define un listado de objetos que están relacionados en la operación del sistema, por ejemplo el tiempo que el dispositivo lleva operando, el nombre de la persona encargada y el nombre del dispositivo.

Interfaces (1.3.6.1.2.1.2) mantiene el estado de cada una de las interfaces de las que dispone el agente.

Addr.transt (1.3.6.1.2.1.3) este grupo solo se brinda para mantener la compatibilidad con versiones anteriores.

Ip (1.3.6.1.2.1.4) mantiene la información de los aspectos relacionados con IP, incluidos el ruteo.

Icmp (1.3.6.1.2.1.5) contiene datos relativos al protocolo ICMP (Internet Control Message Protocol).

Tcp (1.3.6.1.2.1.6) rastrea entre otras cosas el estado de las conexiones TCP, o sea CLOSED, LISTEN, SYN_SENT, etc.

Udp (1.3.6.1.2.1.7) mantiene datos pero de conexiones UDP.

Egp (1.3.6.1.2.1.8) mantiene información relacionada con el protocolo EGP (Exterior Gateway Protocol) incluidas las tablas de vecinos.

Transmission (1.3.6.1.2.1.10) no hay objetos definidos en este grupo pero otras MIBs usan esta rama.

Snmp (1.3.6.1.2.1.11) mediciones relacionadas con el rendimiento de este protocolo. Figura 1. 6 se puede ver la estructura jerárquica de la MIB- II.

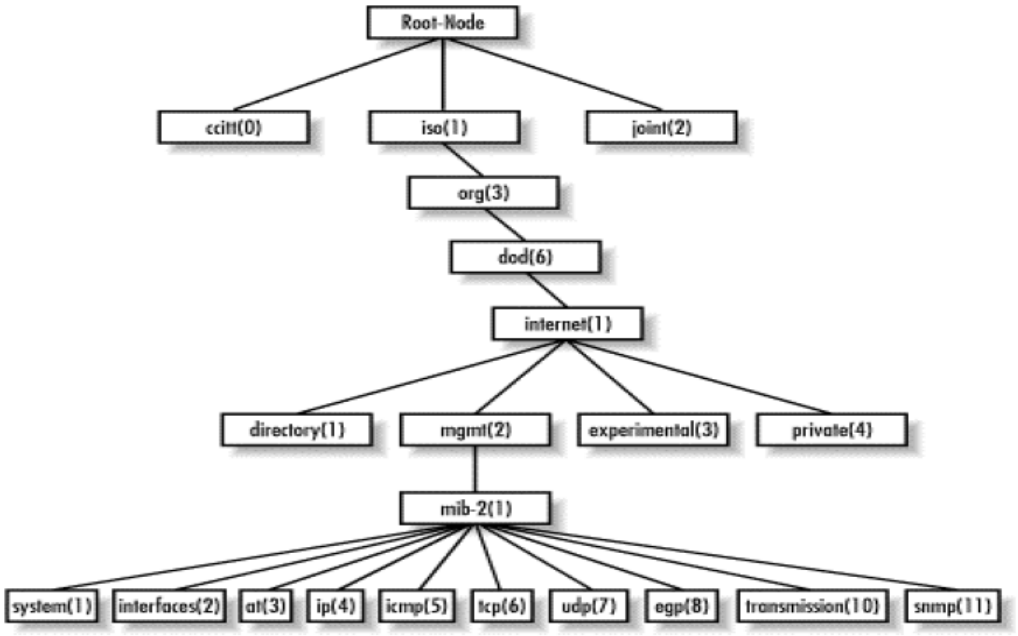


Figura 1. 6 Rama MIB-II

1.11 Mensajes SNMP

Para realizar las operaciones básicas de administración, el protocolo SNMP utiliza un servicio no orientado a la conexión (UDP) para enviar un pequeño grupo de mensajes (PDU's) entre los administradores y agentes. La utilización de un mecanismo de este tipo asegura que las tareas de administración de red no afectarán al rendimiento global de la misma, ya que se evita la utilización de mecanismos de control y recuperación como los de un servicio orientado a la conexión (TCP) (Member, 2006).

Los mensajes SNMP están formadas por:

GetRequest: El gestor solicita al agente información contenida en su base de datos, NMS solicita al agente retornar el valor de un objeto de interés mediante su nombre. En respuesta el agente envía una respuesta indicando el éxito o fracaso del requerimiento. Si el requerimiento fue adecuado, el mensaje resultante también contendrá el valor del objeto solicitado. Este mensaje puede ser usado para recoger un valor de un objeto, o varios valores de varios objetos, a través del uso de listas.

GetNextRequest: El gestor solicita al agente información contenida en su base de datos, con la particularidad de que permite leer el contenido de tablas paso a paso.

Una vez que se ha usado un mensaje *GetRequest* para recoger el valor de un objeto, puede ser utilizado el mensaje *GetNextRequest* para repetir la operación con el siguiente objeto de la tabla. Siempre el resultado de la operación anterior será utilizado para la nueva consulta. De esta forma un NMS puede recorrer una tabla de muchas variables hasta que haya extraído toda la información para cada fila existente.

GetBulkRequest: El gestor le solicita al agente el envío de grandes cantidades de información en forma eficiente cuando es requerida una larga transmisión de datos, tal como la recuperación de largas tablas. Comenzó a existir a partir de la versión 2 del protocolo SNMP. En este sentido es similar al mensaje *GetNextRequest* usado en la versión 1 del protocolo, sin embargo, *GetBulkRequest* es un mensaje que implica un método mucho más rápido y eficiente, ya que a través de un solo mensaje es posible solicitar valores de múltiples objetos administrados.

SetRequest: El gestor solicita al agente el cambio de uno o varios valores de la base de datos. Para realizar esta operación el gestor envía al agente una lista de nombres de objetos con sus correspondientes valores.

GetResponse: Este mensaje es usado por el agente para responder un mensaje *GetRequest*, *GetNextRequest*, o *SetRequest*

Trap: Es utilizado por el agente para enviar información no solicitada al gestor, típicamente avisando a cerca de cambios inesperados en la red.

InformRequest: Los gestores intercambian información entre sí.

En la Figura 1. 7 que sigue se puede ver un resume de lo que explicamos sobre el funcionamiento del protocolo SNMP.

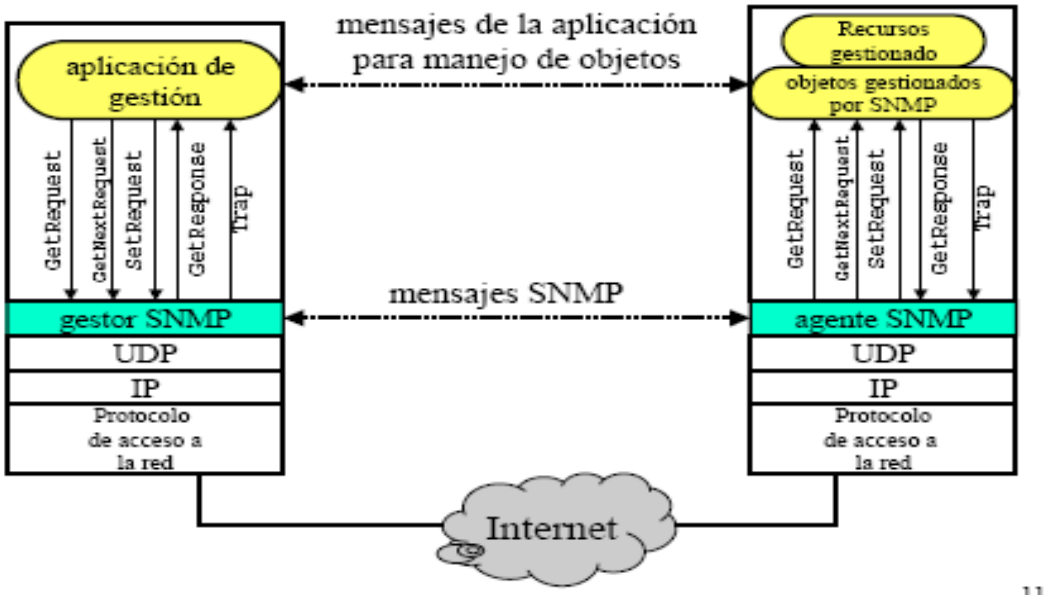


Figura 1. 7. Funcionamiento del SNMP

1.12 Software de gestión

Además de los protocolos que proporcionan servicios a nivel de red y los programas de aplicación que los utilizan, una red necesita software que permita a los administradores depurar problemas, controlar rutas y localizar computadoras que violen los protocolos(Comer, 2005).

El software de gestión de red fue creado para supervisar y controlar los componentes de una red, permitiendo al administrador detectar y corregir los problemas que hacen ineficiente o imposible la comunicación, investigando dispositivos como host, enrutadores, conmutadores, puntos de acceso y puentes para determinar su estado y obtener estadísticas sobre las red a las que se conectan. El administrador de red debe supervisar tanto las fallas de hardware como de software porque las dos pueden generar problemas.

1.13 Puntos de Accesos (AP's)

Los Puntos de Acceso (Access Point), permite conectar a la red cableada con los clientes de la red inalámbrica; su función es convertir los datos que llegan por la interfaz UTP a señales de radio y viceversa en las instalaciones *indoor* o *outdoor* de corto alcance (en las

indoor la distancia máxima es de 40 m a la redonda), suelen disponer de dos antenas, una interfaz LAN RJ-45 10/100 Mbps para conectividad WAN y, en la mayoría de los casos, un puerto de consola para su configuración inicial.

Generalmente también disponen de varias entradas de red LAN 10/100 al tener integrado un hub o un Switch.

Los AP's, pueden enlazarse de tres formas: punto a punto, punto a multipunto y redes malladas. El enlace punto a punto, une dos redes LAN a través del modo puente entre dos redes finales, el enlace punto a multipunto, conecta múltiples redes alambradas con el empleo del modo puente multipunto, y las redes malladas están formadas por AP's conectados punto a punto, para que pueden enlazar en forma de malla (Fleites, 2007).

La infraestructura de un punto de acceso es simple: "Guardar y Repetir", son dispositivos que validan y retransmiten los mensajes recibidos. Estos dispositivos pueden colocarse en un punto en el cual puedan abarcar toda el área donde se encuentren las estaciones.

1.14 Sistemas de supervisión actuales con licencia libre dedicados a supervisar redes inalámbricas

La supervisión es una herramienta muy importante y precisa cuando se quiere mantener informado y tener control de los dispositivos que componen la red, como es caso del Punto de Acceso.

Para el desarrollo de este trabajo se hace un estudio sobre los diferentes tipos de software dedicados a Supervisión y Gestión de redes. Con este análisis identificar cuál de ellos se adecua más al contexto de La Red UCLV-WIFI para supervisar nuestra red Inalámbrica.

A continuación les presentaremos una lista de softwares de gestión que están disponibles en Internet: Pandora FMS, WiFi Manager, Zabbix, Zenoss y Genos.

1.14.1 Pandora FMS (nacido en el año 2005) (pandora.sourceforge.net) es un software de Código Abierto que sirve para monitorizar y medir todo tipo de elementos. Monitoriza sistemas, aplicaciones o dispositivos permitiendo saber el estado de cada elemento de este sistema (Aligam, 2008).

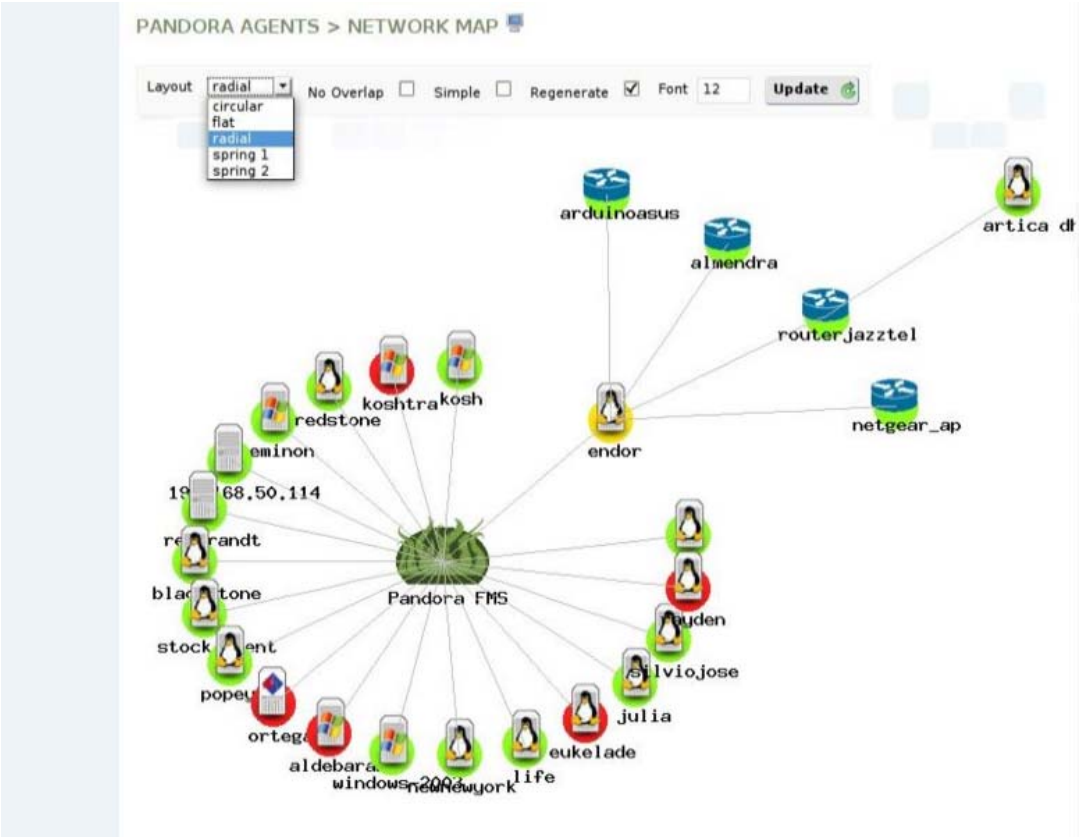
Este sistema dispone de una Base de Datos en la cual reside toda la información de Pandora: datos recolectados por los agentes, configuraciones definidas por el administrador, eventos, incidentes o información de auditoría. De momento sólo está soportada base de datos MySQL (Lorena, 2006).

Puede recoger información de cualquier sistema operativo, con agentes, específicos para cada plataforma, que recolectan datos y los envían al servidor. El desarrollo de sus componentes está hecho íntegramente en Perl, pudiendo funcionar en cualquier plataforma con los módulos requeridos, aunque la plataforma oficial es GNU/Linux.

El trabajo de los agentes es monitorear los detalles de ejecución en las máquinas, reportando datos como E/S y carga del CPU hacia el servidor de Pandora. Pandora FMS también soporta SNMP para recolectar datos o recibir traps.

Pandora FMS es un proyecto OpenSource dirigido y desarrollado por Ártica (Monteagudo, 2009), que tiene aportaciones de desarrolladores de Europa, América y Asia. En la Figura 1. 8 y Figura 1. 9 se muestras imágenes de su interfaz gráfica.

Figura 1. 8. Vista gráfica de Pandora FMS



Figura

Figura 1. 9. Mapa de estado de Pandora

1.14.2 Wi-Fi Manager (Sitio de descarga, 2007) es un software configurado para realizar gestión y seguridad de LAN inalámbricas para redes 802.11 a/b/g, bien como detención y bloqueo de los puntos de acceso de intrusos pero además supervisa las redes inalámbricas y configura los puntos de acceso.

Este software presenta una vista basada en web (Figura 1. 10) de todas las redes inalámbricas que están conectadas a una misma red, bien como los puntos de acceso disponibles para cada red, estado de los puntos de acceso, canales en los que operan, clientes móviles conectados a las mismas y los valores de potencia de señal y ruido histórico de asociación a las redes.

También puede configurar/actualizar el firmware de los puntos de acceso. Y una vez integrado con los sensores de radiofrecuencia, se convierte en un sistema completamente equipado de IDS_inalámbrico, identificando puntos de acceso de intrusos, ataques por

denegación de servicio y puntos vulnerables. No solo detecta automáticamente puntos de acceso como Routers inalámbricos, pasarelas inalámbricas y los supervisa respecto a su disponibilidad, estado de funcionamiento, errores y utilización.

Figura 1. 10 Vista gráfica de WIFI Manager

1.14.3 Zabbix (nacido en el año 2001) (www.zabbix.com), es una solución de monitorización 24x7 de bajo costo, capaz de recoger datos de cualquier aplicación o servidor, con un sistema de envío y captura de datos a través de sus agentes. Es importante señalar que este software es capaz de monitorizar, además, equipos Windows, HP-UX y personalizar sus agentes con parámetros definidos por el usuario (*Corporativa*, 2008).

La ventaja de Zabbix reside en su interface web soportado por una base de datos SQL (MySQL, PostgreSQL o SQLite). Posee un sistema proactivo (Acciones) que permite solucionar automáticamente los problemas, sistema de monitorización, alertas y visualización de gráficos (*Corporativa*, 2008).

1.14.5 Zenoss (nascido en el año 2006) (www.zenoss.com), es ese software que sorprende por su capacidad e interface simplemente echando un vistazo a su página Web. Funciona sobre Linux, de la forma más sencilla posible (*Corporativa*, 2008).

Tiene un interface similar al de Nagios. De hecho, puede importar sus plugins y, aunque su configuración no es todo lo sencilla que debería, es capaz de detectar los equipos de nuestra red automáticamente utilizando (además de SNMP), SSH. Zenoss no necesita agentes en las máquinas remotas, ya que con SSH puede ejecutar de forma segura cualquier comando que deseemos para extraer todo tipo de información.

Para monitorizar máquinas Windows, utiliza un binario que conecta usando WMI para modelar y monitorizar sus servicios (*Corporativa*, 2008).

1.15 Herramienta de Monitoreo actual en UCLV

Actualmente la red UCLV-WIFI tiene instalado el software Nagios versión 3 para el monitoreo de la red.

Nagios (nacido en el año 1999) (www.nagios.org) es una herramienta de monitoreo en código abierto que permite controlar la red, los hosts, switchs y los servicios (SMTP, POP3, HTTP, SSH, DNS)(González, 2005) fue creado para ayudar a los administradores a tener siempre el control de qué está pasando en la red y conocer los problemas que ocurren antes de que los usuarios de la misma los perciban utilizando plug-ins[4] y SNMP(Rasmussen, 2009) para encargar de enviar la información requerida.

Nagios es una aplicación escrita por Ethan Galstad, programada en C y esta liberado bajo licencia GPL por lo que no está sometido a costo de licenciamiento.

Utiliza una interfaz basada en la web (Figura 1. 11) que permite rápidamente descubrir problemas y rastrear sus causas, y puede proveer fácil acceso a todas las informaciones que necesitas sobre los hosts y permite al programador en el tiempo los chequeos a maquinas o servicios previamente configurados. Se puede además saber el estado de la red a través de un mapa (González, 2005).

Este software permite monitorear la web, el correo, la memoria, la cantidad de espacio en el disco duro usado en los hosts, puede también enviar notificaciones a través de e-mail,

[4] son los comandos encargados de realizar toda la monitorización (chequeos de hosts y de servicios).

mensajería instantánea o SMS. El servidor Nagios se instala bajo Linux, sin embargo, también se puede ejecutar sobre Windows o UNIX.

Nagios está formado por un núcleo de aplicación que forma la lógica de control de la aplicación, contiene el software necesario para realizar la monitorización de los servicios y equipos de la red que han sido definidos y también con el SSH puede ejecutar sus comandos.

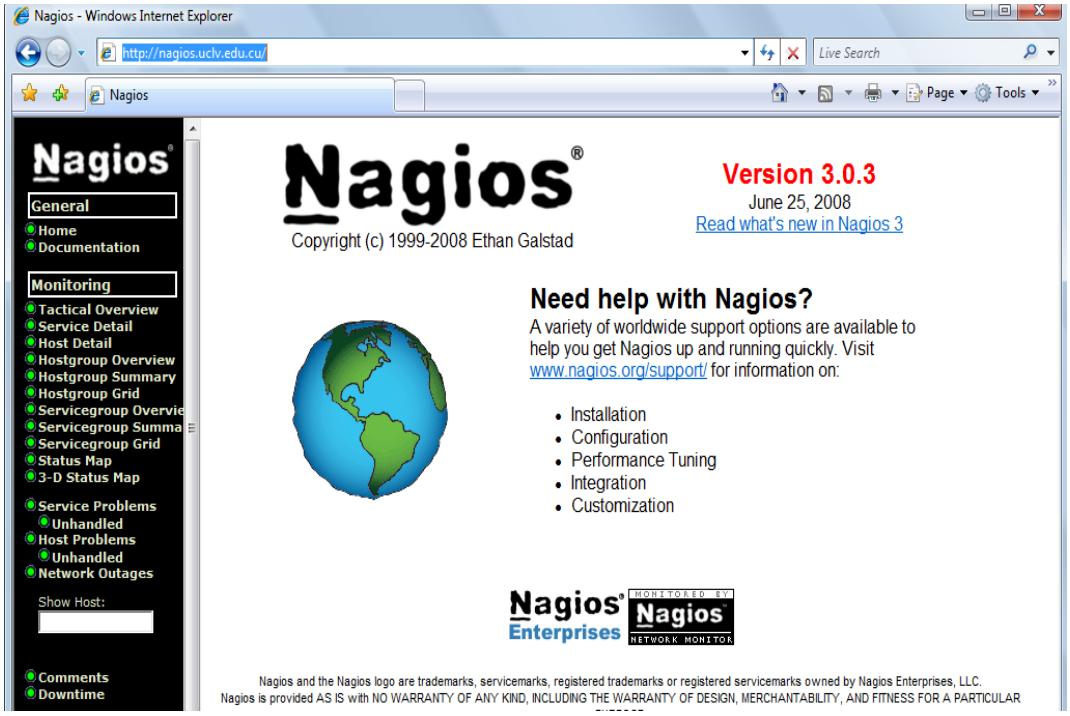


Figura 1. 11. Interfaz web de Nagios

Actualmente la configuración de Nagios en La UCLV para monitorear los AP's instalados solo utiliza una herramienta muy simple: *ping* para detectar la conectividad de estos dispositivos, dejando fuera el monitoreo del funcionamiento de la parte inalámbrica. El Nagios ejecuta sus comandos con SSH por el puerto 22.

1.15.1 Ventajas y desventajas del Nagios frente los demás softwares

Los sistemas que presentamos no presentan grandes ventajas con respecto a Nagios tal y como se pudo constatar analizando las características que ofrecen de los mismos. Hay que tener en cuenta que Nagios es uno del primer software de monitorización y presenta algunas desventajas. Su punto negativo se encuentra en la configuración, debido a que se debe realizar manualmente. Sin embargo Nagios es una solución robusta, escalable y

económica para la monitorización de equipo y redes informáticas, muy flexibles y adaptables a cualquier situación o necesidad. Tiene capacidad de desarrollar plugins de forma sencilla que permite a los usuarios programar sus propios chequeos y de definir una topología o jerarquía de red que permita distinguir entre servicios caídos o inaccesibles.

La Figura 1. 12 muestra el mapa que representa el estado del Nagios actualmente.

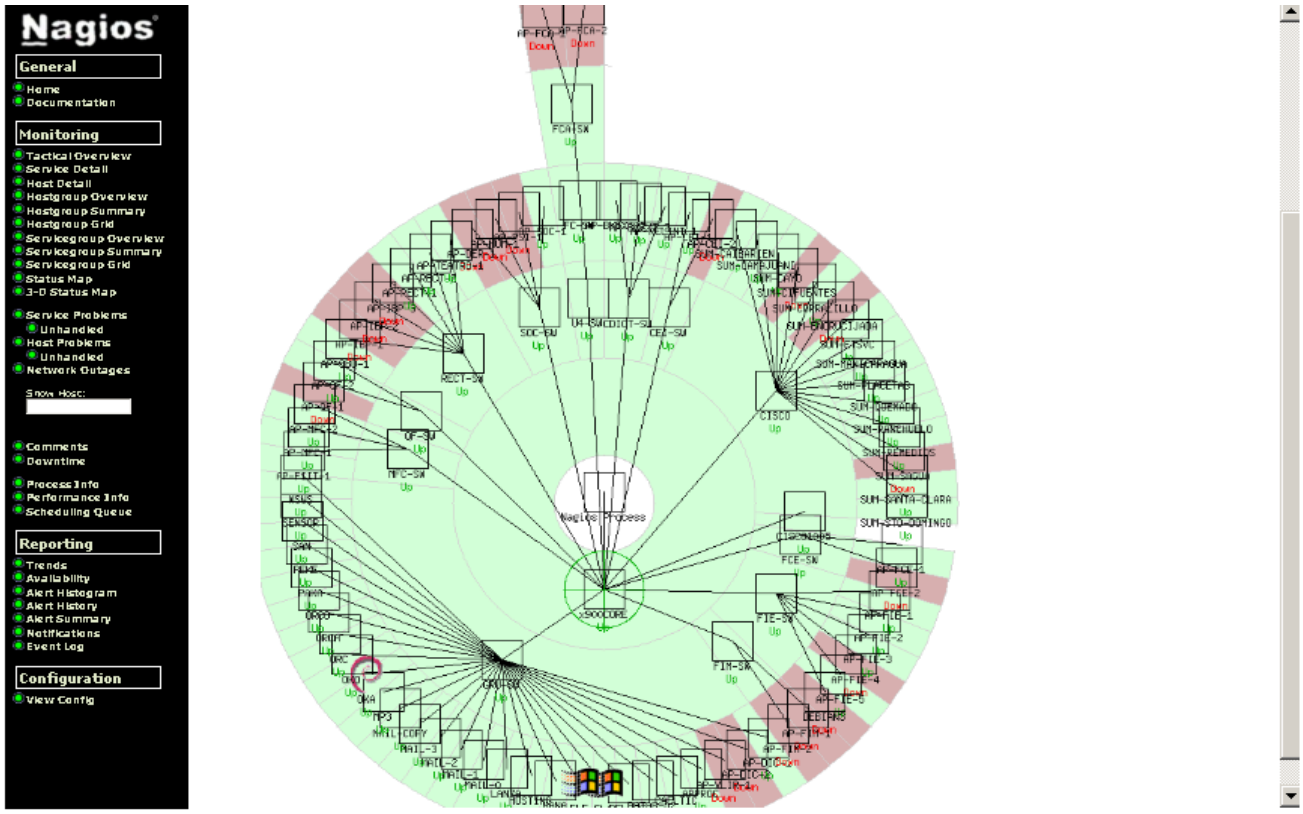


Figura 1. 12. Mapa de estado de Nagios

1.16 Conclusión del capítulo

En este capítulo se han analizados varios sistemas de gestión y monitoreo, algunos de ellos superiores a Nagios en cuanto a sencillez de configuración e información visual. A pesar de las ventajas que puedan tener estos sistemas, ninguno tiene grandes diferencias con respecto a Nagios, plataforma sobre la cual se encuentra el sistema de monitoreo de la universidad. Es por ello que adaptaremos la solución de nuestro problema a esta plataforma.

CAPÍTULO 2. Supervisión de los Puntos de Acceso (AP)

En el capítulo anterior se analizaron los diferentes sistemas de supervisión existentes, los que demostraron sus ventajas y desventajas. Sin embargo ninguno posee grandes diferencias con respecto al utilizado en La Universidad: Nagios.

En este capítulo veremos en detalles la implementación de la solución del problema en Nagios.

2.1 Ficheros de configuración de Nagios

El fichero más importante de Nagios es, nagios.cfg, en él entre otras informaciones se definen los archivos de configuración que el sistema tendrá en cuenta.

Entre ellos se pueden citar los siguientes:

- Cgi.cfg: Regula el acceso al Nagios desde un navegador.
- Resource.cfg: Define las variables y macros que utiliza Nagios. Puede ser utilizado para almacenar directivas de configuración de recursos externos como conexiones a MySQL.
- Generic-host.cfg: Define una plantilla genérica para los host.
- Hostgroups.cfg: Permite agrupar estaciones que compartan características diferentes.
- Services.cfg: Contiene la declaración de los servicios que se desean monitorear.
- Contacts.cfg: Define los nombres y los datos básicos de los responsables que existen en la red.

- Contactgroups.cfg: Agrupa todos los contactos para simplificar a la hora de enviar notificaciones.
- Commands.cfg: Contiene la definición de los comandos a ejecutar, estos comandos son los que informan el estado de los servicios
- Timeperiods.cfg; Es el rango horario que se asigna para cada día de la semana durante la monitorización.
- Checkcommands.cfg: Se chequea los servicios que están definidos.

En la Figura 2. 1 se muestra un diagrama que ilustra la relación entre los objetos que intervienen en la configuración de Nagios.

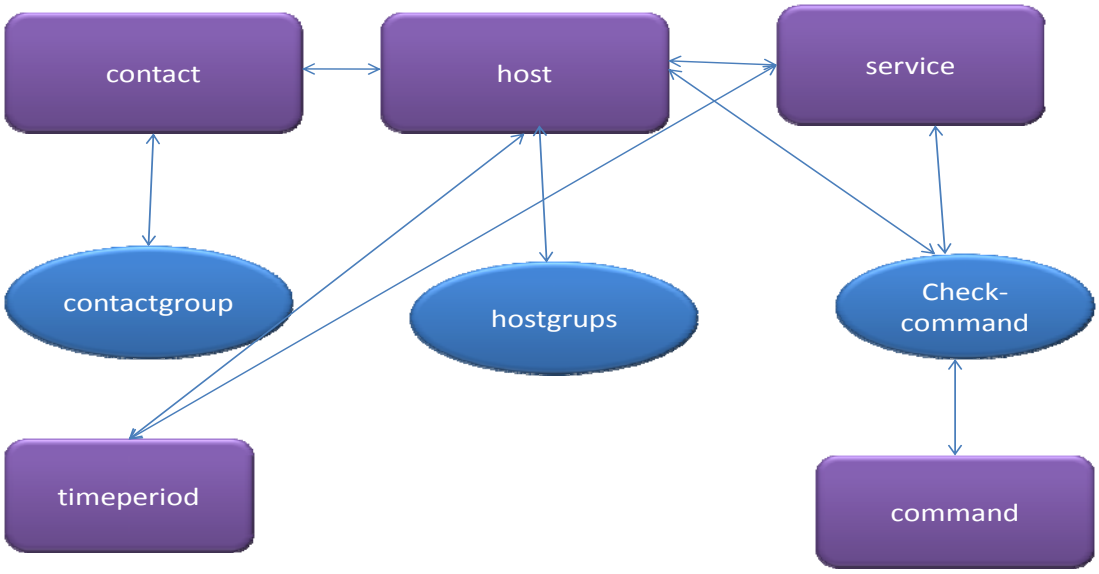


Figura 2. 1 Diagrama contextual de los objetos que intervienen en la configuración del Nagios

2.2 Configuración de Nagios

A continuación se muestra una pequeña representación de los ficheros anteriormente descritos para lograr una mayor comprensión de ellos.

Comenzamos por agregar los contactos (personas quien notificar) de manera que cuando ocurra una falla o cuando se resuelve, se pueda notificar a las personas responsables.

Contacts.cfg

```
define contact{
        contact_name            Izaite
        use                     generic-contact
        alias                   Izaite Franca Almeida da Vera Cruz
        email                   ialmeida@uclv.edu.cu
}
```

Contactgroups.cfg

```
define contactgroup{
        contactgroup_name               aps
        alias                           Administradores AP
        members                         Izaite, miriel
}
```

Configurados los contactos, pasamos a definir los Hosts, que en este caso serán los AP's. Primeramente se crea una estructura genérica para agrupar las características comunes de todos y posteriormente cada uno independientemente.

Generic-host.cfg

```
define host{
        name                            generic-host
        notifications_enabled           1
        event_handler_enabled                   1
        flap_detection_enabled                  1
        failure_prediction_enabled      1
        process_perf_data               1
        retain_status_information       1
        retain_nonstatus_information            1
        check_command                   check-host-alive
        max_check_attempts              10
        notification_interval           0
        notification_period             24x7
        notification_options            d,u,r
        register                        0
}

define      host{
        name                    wifi-trendnet
        use                     generic-host
        check_period            24x7
        check_interval          20
        retry_interval          1
        check_command           check-host-alive
        notification_interval   30
        hostgroups              wifis-uclv
```

```
        contact_groups              aps
        statusmap_image             base/trendnet.pn
}
```

Host.cfg

```
define host{
        use                         wifi-trendnet
        host_name                   AP-BKEXT1
        alias                       AP-BKEXT1
        address                     10.12.34.253
        parents                     SW-U4
}
```

Para el resto de los AP's es necesario repetir el bloque anteriormente descrito, variando el valor de host_name, alias, address y parents. El valor de **use** no varía porque todos parten de usar los valores genéricos definidos en **wifi-trendnet**.

Los dispositivos se agrupan para facilitar las labores de gestión de los mismos.

Hostgroups.cfg

```
define hostgroup{
        hostgroup_name              wifis-uclv
        alias                       AP Red WIFI-UCLV
}
```

Una vez definidos los host, contactos y los grupos, es necesario definir los servicios encargados de monitorear nuestros dispositivos. Partimos como se ha hecho hasta ahora de una plantilla general:

Generic-service.cfg

```
define service{
        name                        generic-service
        active_checks_enabled       1
        passive_checks_enabled      1
        parallelize_check           1
        obsess_over_service         1
        check_freshness             0
        notifications_enabled       1
        event_handler_enabled       1
        flap_detection_enabled      1
        failure_prediction_enabled  1
        process_perf_data           1
        retain_status_information   1
        retain_nonstatus_information        1
        notification_interval       0
```

```
        is_volatile                     0
        check_period                    24x7
        normal_check_interval           5
        retry_check_interval            1
        max_check_attempts              4
        notification_period             24x7
        notification_options            w,u,c,r
}
```

Definiremos los servicios que el Nagios controlará en el grupo de equipos ya definido.

```
define service{
        name                            lan-service
        active_checks_enabled           1
        passive_checks_enabled          1
        parallelize_check               1
        obsess_over_service             1
        check_freshness                 0
        notifications_enabled           1
        event_handler_enabled           1
        flap_detection_enabled          1
        failure_prediction_enabled      1
        process_perf_data               1
        retain_status_information       1
        retain_nonstatus_information    1
        is_volatile                     0
        check_period                    24x7
        max_check_attempts              3
        normal_check_interval           5
        retry_check_interval            1
        notification_options            w,u,c,r
        notification_interval           60
        notification_period             24x7
        register                        0
 }
```

Ahora se configuran los servicios que se desean aplicar. En este caso, debido a que los AP's no cuentan con el protocolo SNMP solo se van a monitorear utilizando del comando ping para detectar su presencia en la red y para verificar el funcionamiento del WIFI se chequearan los eventos que los AP's generan en el servidor de Radius.

Cada AP genera dos eventos fundamentales en el servidor de Radius, separados en ficheros independientes (Access-Request y Access-Accept). Estos ficheros se nombran con la siguiente nomenclatura:

Para cada uno de los AP's se crea una carpeta que se identifica con el número IP del mismo, dentro se crean dos ficheros: auth-detail-20090212 y reply-detail-20090212. El valor numérico en el nombre del fichero identifica la fecha en la que fue generado.

```
define service{
        use                         lan-service
        hostgroup_name              wifis-uclv
        service_description         PING
        check_command               check_ping!300.0,20%!900.0,60%
        contact_groups              todos
 }
```

La orden **check_ping!300.0,20%!900.0,60%**, significa que es permitido un retardo entre 300 y 900 milisegundos con una tolerancia de un 20% para el intervalo inferior y un 60% de tolerancia por el intervalo superior antes de lanzar la alarma.

Para verificar la ocurrencia de eventos de autenticación se monitorea la existencia del fichero **reply-detail-xxxxxx** definiendo el siguiente servicio:

```
define service{
        use                         lan-service
        hostgroup_name              wifis-uclv
        service_description

        max_check_attempts          1
        is_volatile                 1
        check_command               check_logap
        contact_groups              aps
}
```

En este caso en la instrucción **check_command** se llama al comando **check_logap** definido en el fichero **commands.cfg**. En este caso específico por lo compleja de la orden a ejecutar y para que quede de una forma más clara es necesario definir un comando que se encargue de ejecutar nuestro plugins.

Para chequear el estado del fichero de eventos se va a utilizar el plugins **check_logfile**. Este plugins permite escanear los ficheros de eventos en busca de patrones que disparen las alarmas. Antes que nada es necesario descargarlo de su web oficial (http://www.consol.com/opensource/nagios/check-logfiles/) e instalarlo, pues no forma parte de los plugins estándares que ofrece Nagios. El proceso de instalación es relativamente sencillo y se encuentra bien documentado en su sitio Web por lo que no será detallado.

Después de instalado el plugins es posible definir en el fichero de **commands.cfg** lo siguiente:

```
define command{
        command_name    check_logap
        command_line    $USER1$/check_logfiles $$ -noprotocol -okpattern="Access-Accept" logfile="/home/log/$HOSTADDRESS$/reply-detail-`(date +%Y%m%d)`"
}
```

La sentencia command_line tiene el siguiente significado:

- $USER1$/check_logfiles: $USER1$ es una macro que tiene definido el PATH donde se encuentra el plugins.
- -Noprotocol: Normalmente, todas las ocurrencias de errores son escritas en un fichero temporal. Con el uso de esta instrucción se anula esta posibilidad.
- -Okpattern: Retorna la alarma a su estado normal. Esto quiere decir que el plugins buscará dentro del fichero especificado el patrón “Access-Accept”, de no ser encontrado disparará la ocurrencia de un error.
- Logfile: Contiene el nombre del fichero que será monitoreado.

2.3 Resultados de la configuración

Después de terminado todo el proceso de configuración, se puede ver el resultado del mismo en forma de mapa en el cliente Web haciendo clic en **status map** (Figura 2. 2).

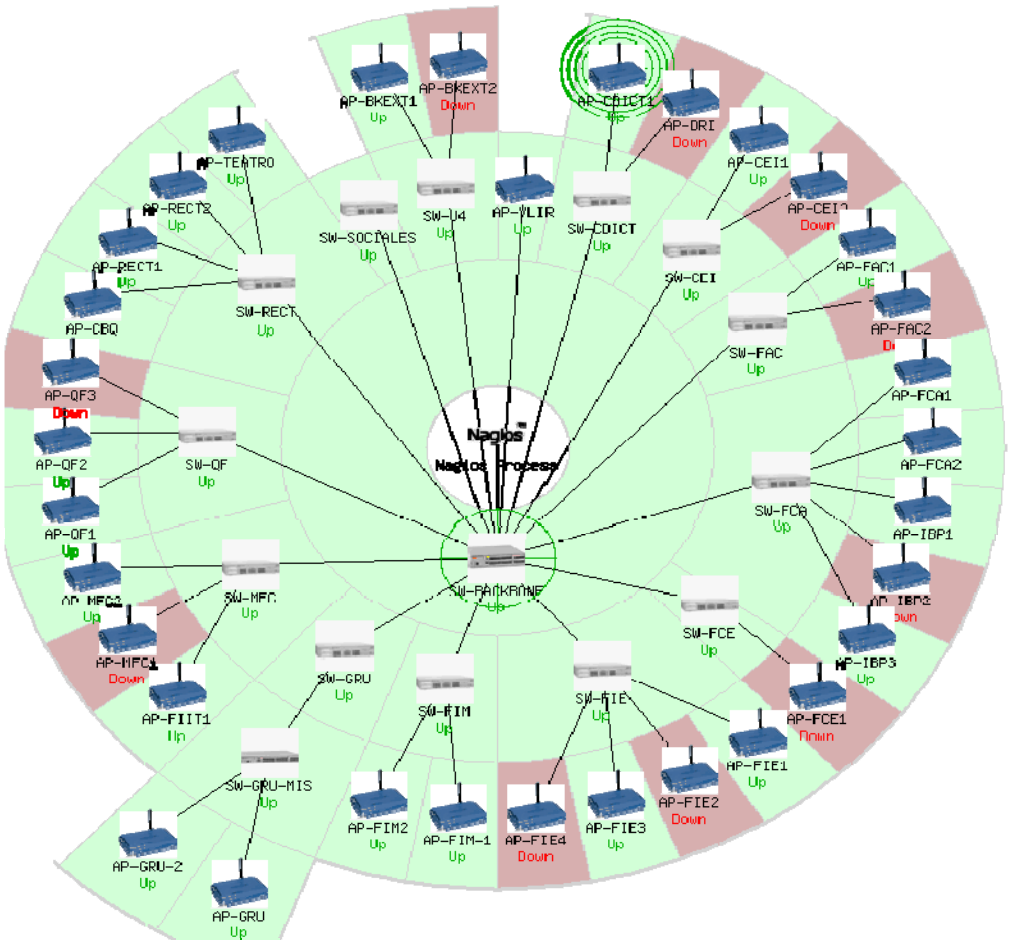


Figura 2. 2. Mapa con la representación de la Red UCLV.

En la Figura 2. 2, todos los dispositivos que se encuentran resaltados con fondo rojo representan equipos que por alguna razón (pueden estar apagados, desconectados a la red, etc.) no han respondido al comando check_ping y necesitan ser inspeccionados físicamente.

Si desplaza el puntero del mouse por encima de los íconos puede apreciar en la parte superior izquierda una ventana rectangular con fondo en amarillo con un resumen del estado del equipo sobre el cual tenga el puntero, tal y como se muestra en la Figura 2. 3

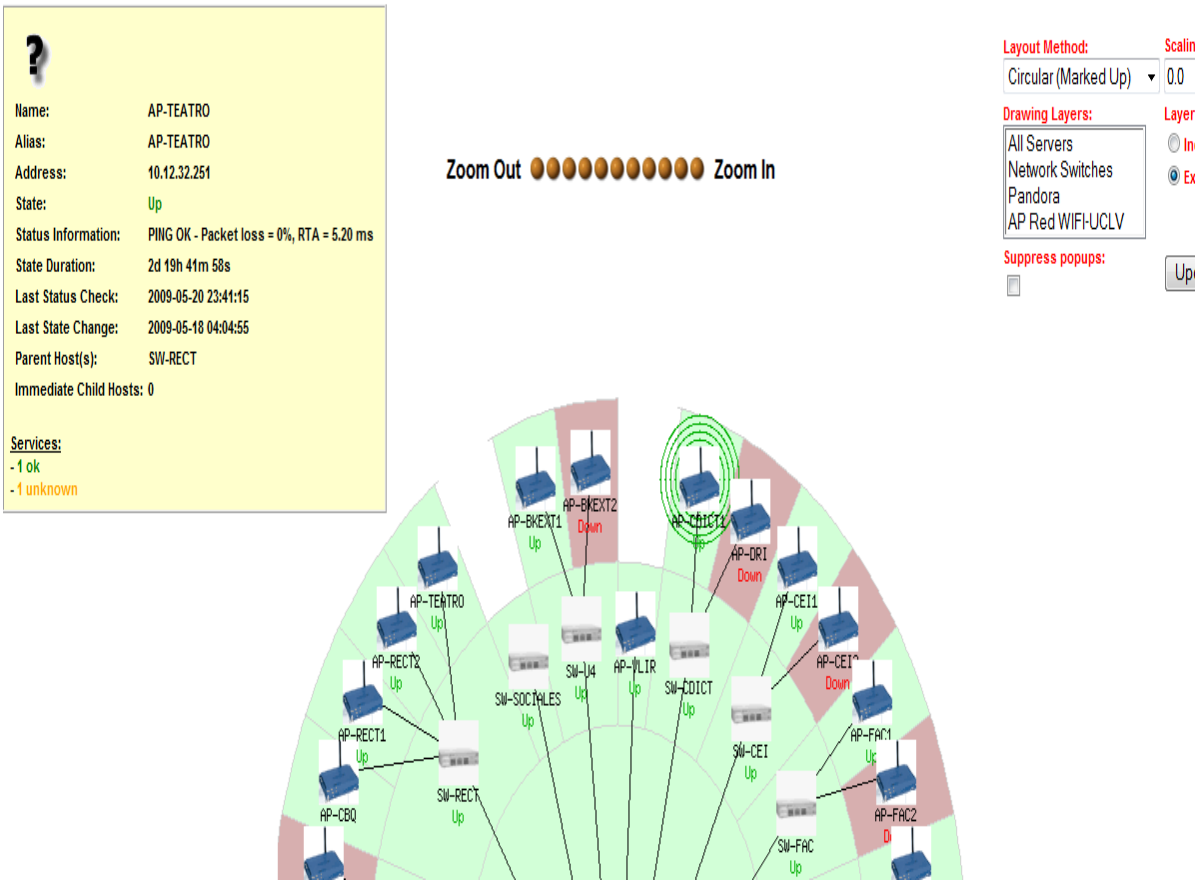


Figura 2. 3. Descripción del estado de un equipo seleccionado.

Es posible ver también el estado de todos los equipos haciendo clic sobre **View Status Detail For All Hosts** tal y como muestra la Figura 2. 4

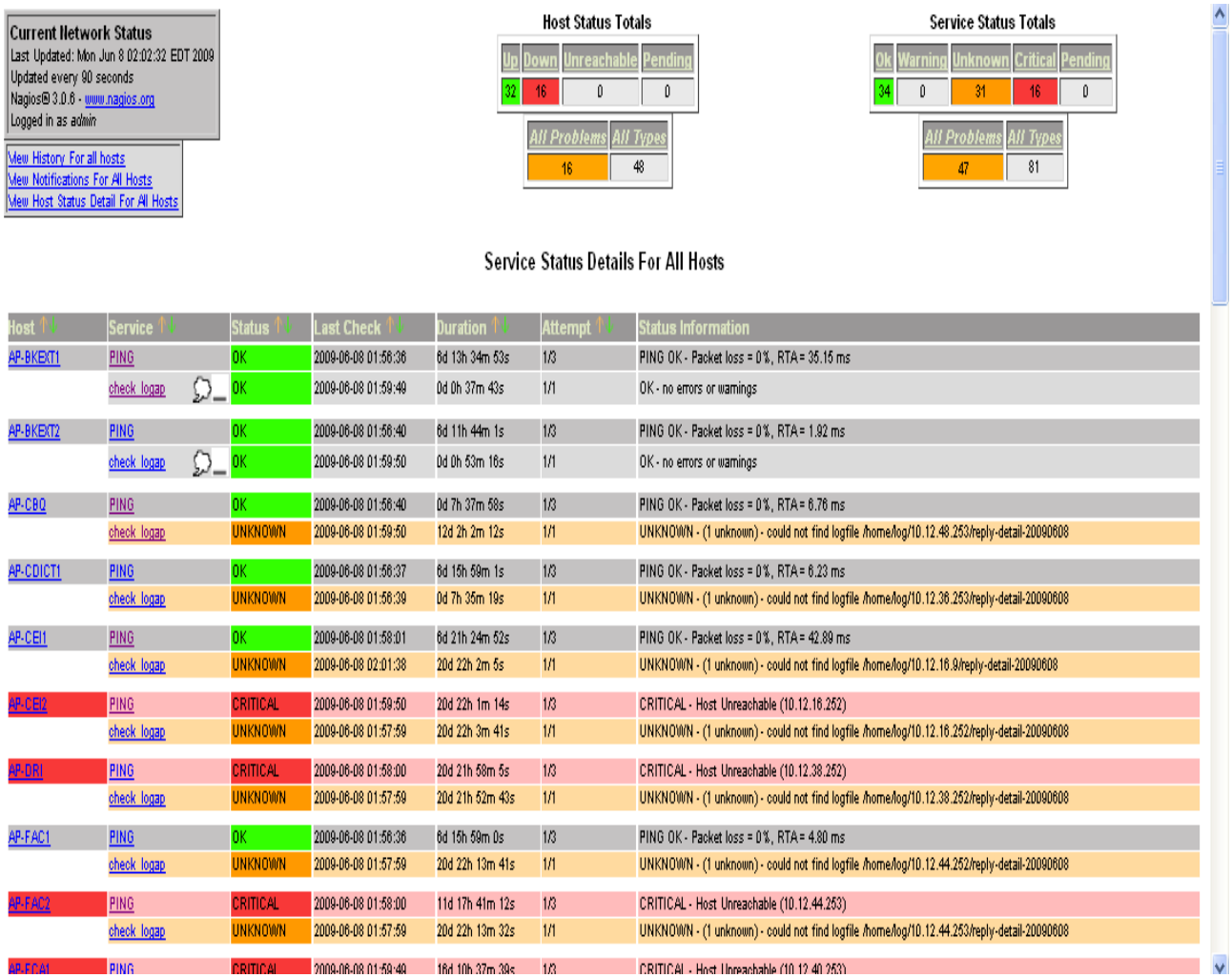


Figura 2. 4. Estado de todos los equipos monitoreados

En la Figura 2. 4 se pueden apreciar los dos servicios definidos para los AP's: Ping y check_logap: El primero puede estar en dos estados CRITICAL u OK y el segundo en UNKNOWN u OK.

Cuando check_logap se encuentra en UNKNOWN está alertando que no ha encontrado el fichero de eventos a monitorear lo cual se traduce en que la interfaz WIFI del AP no está funcionando por alguna causa que tendrá que ser investigada.

Haciendo clic sobre cualquiera de los servicios mostrados el usuario puede tener acceso a una ventana (Figura 2. 5) donde se muestran todos los detalles, entre los que se encuentran, el estado actual, una información sobre ese estado, última vez en que fue chequeado, próxima vez en que será chequeado, etc.

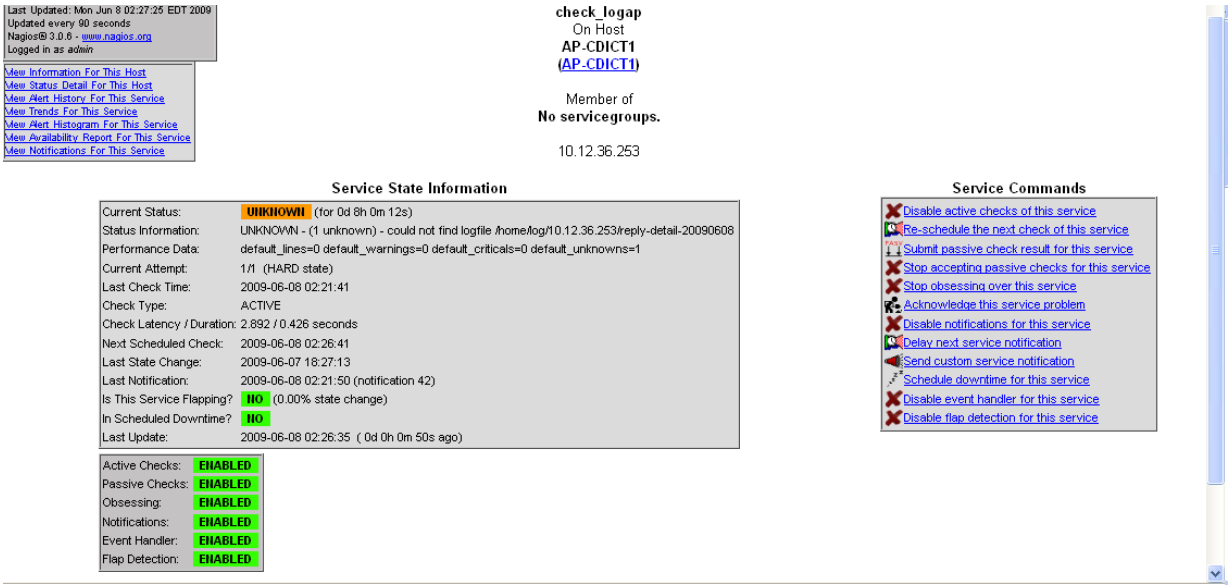


Figura 2. 5. Detalles de un servicio

2.4 Características del AP TEW-430APB5 (TrendNet)

Nuestro centro actualmente cuenta con alrededor de 40 AP's TEW-430APB distribuidos por todo el campus, como se ilustra en la Figura 2. 6.

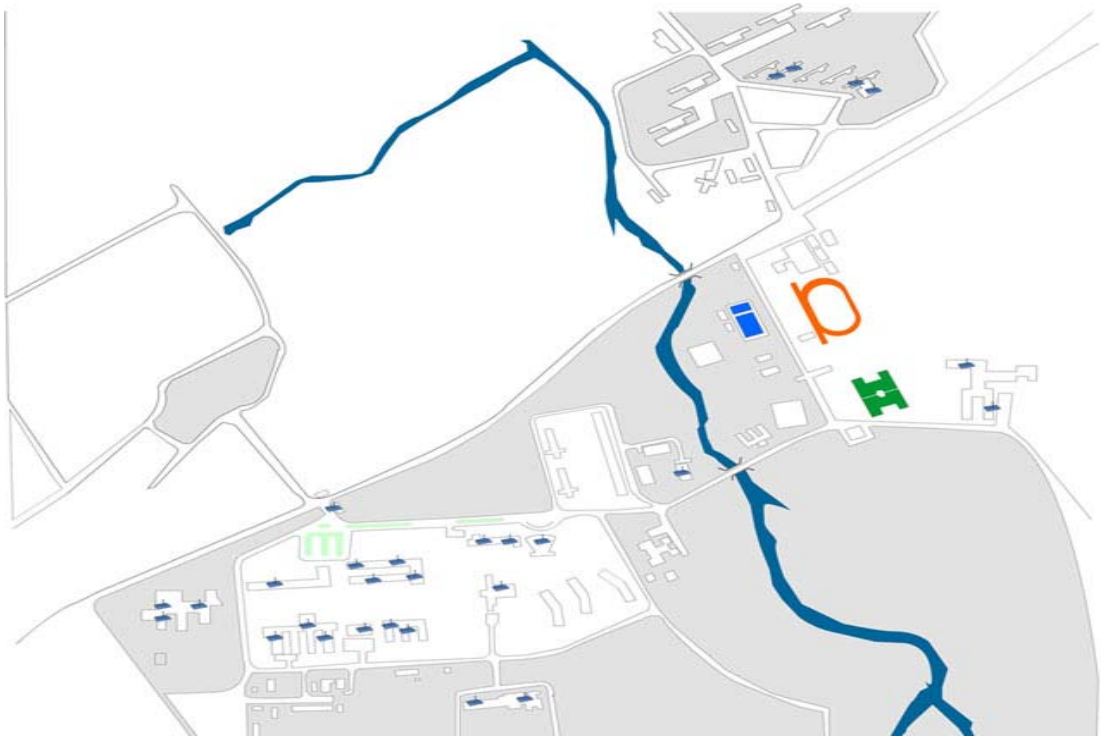


Figura 2. 6. Distribución de AP's por el Campus Universitario.

Estos equipos permiten velocidades hasta 54Mbps y trabajan sobre el estándar 802.11g y cuentan con una interfaz de configuración sencilla e intuitiva, las especificaciones del equipo se puede ver en el **Anexo I**.

Como hemos señalado anteriormente su punto más débil es el de no contar con el protocolo SNMP lo cual limita las posibilidades de su gestión.

2.5 Características de la Antena TEW-AI75OB(TrendNet)

Con el objetivo de aumentar el rango de cobertura de los AP's se utiliza la antena **Omni TEW-AI75OB** de TRENDnet. Esta antena ofrece mayor potencia y rango de distancia para la conexión inalámbrica. Como una antena opcional para los equipos de red inalámbrica IEEE 802.11b/g 2.4GHZ ó 802.11a5GHZ, mejora la calidad y potencia de la señal y amplia el área de cobertura (www.trendnet.com). Las especificaciones de la antena se muestran en **Anexo II**.

2.6 Análisis económico

Aunque el sistema analizado no requiere costo se hizo un análisis económico con respecto a los equipos monitorizados por el mismo. La compra se realizó a la empresa Copextel de Villa Clara, sumando una cantidad de 40 AP's y 40 antenas adicionales de 5dbi porque la que trae el AP's es solo de 2dbi.

Estos equipos son los más baratos que se comercializan en Cuba debido fundamentalmente a su sencillez. Es importante señalar que en algunas áreas de la universidad existen otros modelos funcionando de mejores prestaciones adquiridos por diversas vías.

Teniendo en cuenta las condiciones económicas del país actualmente, este proyecto pudo ser ejecutado gracias al proyecto de Colaboración que tiene la universidad con el Consejo de Universidades Flamencas Belgas conocido como proyecto VLIR con un monto total de 3 095 CUC. Con él se pudieron abarcar todas las áreas universitarias. Se muestran en el **Anexo III y IV** las áreas donde se montaron los AP's y la factura de compra.

En la Tabla 2. 1 se muestra un resumen de los costos de estos equipos.

Tabla 2. 1. Precios de los Aps y la Antena (Trendnet).

Descripción	**Precio CUC**	**Cantidad**	**Total CUC**	**Total MN**
AP(Trendnet TEW-430APB)	$54.36cuc	40	$ 2174.40	
Antena(Trendnet TEW-A1750B)	$23.03cuc	40	$921.20	
Subtotal			**$3095.60**	**$639.12**

2.7 Conclusión del capítulo

Como se ha visto, la no existencia del protocolo SNMP en los AP's instalados en La UCLV nos ha llevado a buscar una solución alternativa para detectar irregularidades en el funcionamiento WIFI de los AP's. En este caso ha sido el análisis de los ficheros de eventos generados por el servidor Radius.

En esta primera etapa se ubicaron los puntos de acceso fundamentalmente en laboratorios de uso colectivo y en los salones de reuniones.

CONCLUSIONES

Como resultado del trabajo realizado y argumentado por este proyecto de tesis se ha llegado a las conclusiones siguientes:

1. Actualmente existen varias soluciones Opensource dedicadas al monitoreo de dispositivos conectados a la red, pero las diferencias existentes entre ellos no son grandes.
2. Nagios se mantiene como una solución robusta y estable, aunque aún sigue siendo una debilidad la necesidad de realizar su configuración manualmente.
3. Los AP's instalados en La UCLV carecen de un protocolo de gestión, siendo accesibles solamente a través de una interface web, por lo cual solo es posible monitorear su estado en la red a través de un *ping* y analizar los eventos que genera en el servidor de autenticación Radius para ver si está procesando peticiones WIFI.
4. Aprovechando las flexibilidades que ofrece Nagios, utilizando un *plugins* llamado check_logfile se logró analizar los eventos que son generados en el servidor de Radius para evaluar el funcionamiento WIFI del AP's.

RECOMENDACIONES

Con el presente trabajo, se intentó buscar una solución a la problemática del monitoreo de los AP's instalados en la UCL. Sin embargo existen algunas recomendaciones:

1. Trabajar en la creación un plugins que permita acceder a través de la interface web de los AP's a la configuración de los mismos, facilitando la configuración de estos, que actualmente es necesario realizarla individualmente.
2. Estudiar las nuevas soluciones web que se están presentando en el mercado para proporcionar una forma gráfica más amigable de configurar Nagios.

REFERENCIAS BIBLIOGRÁFICAS

Albalate, R. P., (2007) *Propuesta de un sistema de Monitoreo y Gestion de la Red de Cobre Presurizada en ETECSA.* Tesis de Maestría. Santa Clara, Departamento de Telecomunicaciones y Electrónica, Universidad Central de Las Villas.

Aligam, E., (2008) *Introducción a Pandora FMS.* [En línea]. Disponible en: http://pandoramon.sourceforge.net/es/ [Accesado el día 7 de febrero de 2009]

Corporativa, (2008) *Monitorización/Comparativa.* [En línea]. Disponible en: http://www.corporativa.com [Accesado el dia 5 de maio de 2009]

DOMÍNGUEZ, M. O., (2004) *Diseño de una Red de Área Local Inalámbrica*. Tesis de Maestría. Santa Clara, Departamento de *Telecomunicaciones y Electrónica,* Universidad Central de las Villas.

COMER, D. E., (2005) *Redes Globales de Información con Internet y TCP/IP, Principios Básicos, Protocolos y Arquitectura.* Tercera Edición, Tomo II.

FLEITES, A., (2007) Diseño de una red de área local inalámbrica. Tesis de Maestría. Santa Clara, *Departamento de Telecomunicaciones y Electrónica,* Universidad Central de Las Villas.

Fernández, J. et al., (2008) *Seguridad en la Familia de protocolos SNMP*. [En línea]. Disponible en: http://www.rediris.es/difusion/publicaciones/boletin/50-51/ponencia16.html [Accesado el día10 de Abril 2009]

GONZÁLEZ, E., (2005) *Nagios Herramienta libre para la monitorización de Sistemas*. [En línea]. Disponible en: www.nagios.org [Accesado el día 2 de abril de 2009]

INCHAUSPE, I. E., (2001) *Monitoreo de redes*. [En línea]. Luján, disponible en: http://www.unlu.edu.ar/~tyr/tyr/TYR-trab/monitred/TF-Inchauspe.htm [Accesado el día 8 de abril de 2009]

LORENA, S., (2006) *Introducción a Pandora FMS*. [En línea]. Disponible en: http://www.osalt.com/es/pandora [Accesado el día7 de Febrero de 2009]

MARTINEZ, E., (2000) *El ABC de las redes inalámbricas* [WLANs]. [En línea]. Disponible en: http://www.eveliux.com/mx/estandares-wlan.php [Accesado el día 18 de enero del 2009]

MEMBER, H., (2006) *Protocolos de Comunicación!, Para Principiantes... Una Medio Introducción*. [En línea]. Disponible en: http://foros.hackerss.com/t585/protocolos-de-comunicacion-33 [Accesado el día 18 de enero del 2009]

MONTEAGUDO, M., (2009) *Mantenga sus sistemas bajo control*. [En línea]. Madrid, disponible en: http://www.artica.es/docs/pandora_whitepaper_es.pdf [Accesado el día 19 de abril de 2009]

Oliver, M. y A.Escudero, (1999) *REDES DE ÁREA LOCAL INALÁMBRICAS SEGÚN EL ESTÁNDAR IEEE 802.11. Eveliux.com, 6.* [En línea]. Disponible en: http://nmg.upc.es/intranet/qos/9/9.3/9.3.19.pdf [Accesado el día 18 Enero de 2009]

OROZCO, V. R. M., (2009) *Configuración Protocolo SNMP*. [En línea]. Guatemala, disponible en: http://carlos8rg.files.wordpress.com/2008/08/onto_snmp.pdf [Accesado el día 10 de abril de 2009]

PUENTES, J. L. A., (2004) *Estrategia para la Gestión de una Intranet*. Tesis de Trabajo de Diploma .Santa Clara, Departamento de Telecomunicaciones y Electr*ónica.* Santa Clara, Universidad Centra de las Villas.

RASMUSSEN, A. I., (2009) *Nagios 2.9.* [En línea]. Disponible en: http://www.osalt.com/es/nagios [Accesado el día 11 de Marzo de 2009]

RIOS, D., (2009) *Conocer y configurar SNMP*. [En línea]. Disponible en: http://www.seguridadinformatica.es/profiles/blogs/conocer-y-configurar-snmp [Accesado el día 10 de Abril de 2009]

Sitio de descarga, (2007) *Gestor WiFi ManageEngine (ManageEngine WiFi Manager) 5.5.* [En línea]. Disponible en: http://www.fredownloadmanager.org/es/downloads/dir/go.php [Accesado el dia 7 de febrero de 2009]

STALLINGS, W., (1999) *Conceptos básicos de SNMP*. [En línea]. Disponible en: http://www.seguridadinformatica.es/profiles/blogs/conocer-y-configurar-snmp [Accesado el día 10 de abril de 2009]

ANEXOS

Anexo I LAS ESPECIFICACIONES TÉCNICAS del AP TEW-430APB5

Standards	IEEE 802.11b/g IEEE 802.3u 10/100BASE-TX Fast Ethernet
Signal Type	DSSS (802.11b) OFDM (802.11g)
Modulation	QPSK / BPSK / CCK / OFDM
LED Indicators	Power, LAN (Link/Activity), WLAN (Link)
Frequency	2412 MHz ~ 2462 MHz (FCC) 2412 MHz ~ 2472 MHz (ETSI) 2400 MHz ~ 2484 MHz (Japan)
Channel	1~ 14 Channels *Local Regulatory Restrictions May Apply
Data Encryption	64bit / 128 bit WEP Encryption, WPA, WPA2, WPA-PSK, WPA2-PSK
Data Transfer Rate	Fast Ethernet: 10/100Mbps Wireless:Up to 54Mbps (with Automatic Scale Back)
Receiver Sensitivity	54Mbps Typical -68 dBm @10% PER 11Mbps: Typical -81 dBm @8% PER
Transmit Power	802.11g:Minimum 13dBm typically

	802.11b: Minimum 15dBm typically
Transmission Range	Outdoor: 100~300M (depends on environment) Indoor: 50~100M (depends on environment)
Network Cables	2-pair UTP/STP Cat. 3,4,5 (100 m)
Interface	1 x 10/100Mbps RJ45 port
Antenna	1 x 2 dBi Dipole Antenna
DC inputs	DC 7.5V /1A
Power Consumption	4.2W (Max)
Temperature Operating	0 ~ 40 °C, Storage: -10 ~ 70 °C
Humidity	Operating:10% ~ 90%, Storage: 5% ~ 90%
Dimensions	140 x 98 x 30 mm (W x H x D) without Antenna
EMI	FCC Class B, CE Mark B

Anexo II Especificaciones del Hardware de la antena TEW-AI750B

Rango de Frecuencia: 802.11 a :4.9~5.875GHZ 802.11b/g: 2.4~2.5GHZ	**Ganancia:** 802.11 a : 7 dBi 802.11b/g:5dBi
VSWR: 2.0:1	**Polarización:** Linear, Vertical
HPBW/Horizontal: 360°	**HPBW/VERTICAL:** 802.11 a :25° 802.11b/g:35°
Power Handling: 2W(cw)	**Impedance:** 50hms
Connector: Reverse	**Cable Length:** 100 cm (3.ft.)

Dimensión: Antenna: 217*28* 14mm	**Weight:** Antenna: 40g (1.4oz.) Base: 82g (2.9oz)
Temperature: -10°C ~55°C 5°(14°F ~131° F)	**Humidity:** 95% at 25 C(77°F)

Anexo II Factura de compra de AP y Antena

C O T I Z A C I O N orge Valiño Cedré

Página 1

UEN 3 INGENIERIA Y SISTEMAS AUTOMATIZADONo. Orden : 803001993 27/9/08 Válido Hasta : 26/10/08 Orden No.
Dpto.031US Forma de Pago Crédito a 30 días 803001993
NIT-30000520523 REEUP 60215

CLIENTE : 2068190303 MES, PROGRAMA IVC UCLV Comprador :
V714-00US Carretera a Camajuani Km 5
Vendedor: JVC

Orden Descrip. :

Art.	Código	Cod. de Cadena	Descripción	U/M	Por Despachar	Desp.	Precio	Importe	Almacen
1	RP-15.06.079		AP TREDNET TEW-430APB 54 Mbps 11g Wir	UNO	40.00	____	54.36	2174.40	Ctral X
2	RP-15.06.103		TREDNET Indoor Omni Antenna 5 dBi	UNO	40.00	____	23.03	921.20	Ctral X

Esta mercancía no se podrá recoger después de las 4:00PM $3095.60
Hora Actual: 4:20pm Desc en Venta $0.00
Total en CUC: $3095.60
¡¡¡---Solo para Clientes que Operan en USD---!!! Importe en USD: $3095.60

Este documento pierde su valor a partir de los 30 días posteriores a su emisión. IMPORTE EN MONEDA NACIONAL: 639.12
PARA EFECTUAR LA COMPRA, SE DEBE PRESENTAR ESTA COTIZACION JUNTO CON EL INSTRUMENTO DE PAGO

Elaborado por: Jorge Valiño Cedré Nombre y Firma del Cliente:
Firma : C. de Identidad
Cargo :
Despachado por: Firma :
Nombre y Firma Forma de Pago Crédito a 30 días

Dirija sus pagos en CUC a: Corporación Copextel, S.A. a la cuenta 0300000002606322 en el BFI Orden No. 803002279
En MN a: SAC Corporación Copextel S.A -División Centro a la cuenta 0643301007700115 en BANDEC Cliente 2068190303
27/10/08 4:20pm

Anexo IV Distribución de los Puntos de Accesos (AP) en el Campo Universitario

Ubicación	Cantidad	Ubicación	Cantidad	Total
Rectorado	2	**SUC**	4	
Rel. Internacionales	1	**QF**	2	
DIC	2	**Puerta**	1	
Teatro	2	**Casa VLIR**	1	
CDICT	1	**FCE**	2	
MFC	2	**U_4**	2	
CEI	1	**FCA**	1	
FIE	4	**IBP**	3	
FI M	2	**FC**	2	
CBQ	1	**FCIE**	1	
FIIT	2	**BK43**	2	
Total	**20APs**	**Total**	**20 APs**	**40APs**

Glosario

AP (*Access Point*) Punto de Acceso, dispositivo encargado de establecer la comunicación entre una estación en una WLAN con la red local correspondiente.

ATM (Asynchronous Transfer Mode) Modo de transferencia Asíncrono.

BSD (Berkeley Software Distribución) Berkeley Software Distribution.

CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) Acceso Múltiple por Detección de Portadora Evitando Colisión.

DNS (Domain Name Server) Servidor de nombres de Dominio.

GNU Sistema operativo compatible con UNIX **.**

HP-UX (Hewlett Packard UniX).

HTTP(Protocol For the Transfer of Hypertexts) Protocolo Para la Transferencia de Hipertextos

IEEE (Institute of Electrical and Electronics Engineers) Instituto de Ingenieros Eléctricos.

IEEE 802 Comité de la IEEE organizado para crear los estándares de las Redes de Área.

LAN (*Local Area Network*) Red de Área Local.

LDAP (Lightweight Directory Access Protocol) Protocolo de Acceso al Directorio de Peso. Ligero.

Local. La IEEE 802.11 especifica las normas para la redes LAN inalámbricas.

MAC (*Medium Access Control*) Control de Acceso al Medio.

MAC (Media Access Control address) Dirección de control de acceso al medio **.**

MAN (*Metropolitan Area Network*) Red de Área Metropolitana.

MRTG (Multi Router Traffic Grapher).

MySQL sistema de gestión de base de datos relacional, multihilo y multiusuario. Se ofrece bajo la licencia GNU GPL.

PDU (*Protocol Data Unit*) Unidades de datos de protocolo.

POP3 (Post office versión 3) El correo versión 3.

PostgreSQL(system of administration of database relacional guided to objects of free software, published under the license BSD) sistema de gestión de base de datos relacional orientada a objetos de software libre, publicado bajo la licencia BSD

RADIUS (Remote Aunthentication Dial In User Service) Servicio de Usuario de Acceso

RPM (Package Manager) sistema de administración e instalación de paquetes de software característico de varias plataformas GNU/Linux, fundamentalmente basadas o afines a Red Hat.

SNMP *(Signaling Network Main Protocol)* Protocolo Principal de Señalización de Red.

SQL (Structured consultation language) Lenguaje de consulta estructurado.

SQLite (system of administration of databases compatible relacional with ACID) sistema de gestión de bases de datos relacional compatible con ACID.

SSH (Secure Shell), intérprete de órdenes seguro.

TCP (*Transport ControlProtocol*) Protocolo de Control de Transporte.

Telefónico de Autentication Remota.

TKIP (*Temporal Key Integrity Protocol*) Protocolo de integridad de clave temporal.

UDP *(User Datagrama Protocol)* Protocolo de Datagrama de Usuario.

UNIX Sistema operativo desarrollado por Bell Laboratories que soporta operaciones multiusuario y multitrabajo.

UTP Par Trenzado No apantallado(LAN).

WAN (*Wide Area Network*) Red de Área Extendida.

WEP (*Wired Equivalent Privacy*) Equivalente a Privacidad Cableada, protocolo de seguridad en redes WLAN.

Wi-Fi (*Wireless Fidelity*) Fidelidad Inalámbrica certificación a los productos de redes WLAN.

Wi-Fi (*Wireless Fidelity*) Fidelidad Inalámbrica certificación a los productos de redes WLAN.

Wimáx (*Worldwide Interoperability for Microwave Access*) Interoperabilidad Mundial para Acceso por Microondas.

WLAN (*Wireless Local Area Network*) Red de Área Local Inalámbrica.

WMI (Administrative instrumentation of Windows) Instrumentación Administrativa de Windows.

WPA (*Wi-Fi Protected Access*) Acceso Protegido Wi-Fi, protocolo de seguridad altamente y electrónicos.