TRABAJO ESPECIAL DE GRADO

DESARROLLO DE UN PROTOTIPO DE ADMINISTRACIÓN Y MONITOREO DEL TRÁFICO DE DATOS EN REDES WIFI, BASADO EN SOFTWARE LIBRE, PARA LA GERENCIA DE PLANIFICACIÓN DE CANTV

Presentado ante la Ilustre
Universidad Central de Venezuela
por el Br. Emelys DelV. Obando M.
para optar al título de
Ingeniero Electricista
Mención Comunicaciones

Caracas,2009

TRABAJO ESPECIAL DE GRADO

DESARROLLO DE UN PROTOTIPO DE ADMINISTRACIÓN Y MONITOREO DEL TRÁFICO DE DATOS EN REDES WIFI, BASADO EN SOFTWARE LIBRE, PARA LA GERENCIA DE PLANIFICACIÓN DE CANTV

PROF. GUÍA: ING. ZELVIDAR BRUZUAL

TUTOR INDUSTRIAL: DR. PEDRO BONILLO

Presentado ante la Ilustre
Universidad Central de Venezuela
por el Br. Emelys DelV. Obando M.
para optar al título de
Ingeniero Electricista
Mención Comunicaciones

Caracas, Octubre 2009

CARTA DE APROBACIÓN

CONSTANCIA DE APROBACIÓN

Caracas, 04 de noviembre de 2009

Los abajo firmantes, miembros del Jurado designado por el Consejo de Escuela de Ingeniería Eléctrica, para evaluar el Trabajo Especial de Grado presentado por la Bachiller Emelys Del Valle Obando M titulado:

"DESARROLLO DE UN PROTOTIPO DE ADMINISTRACIÓN Y MONITOREO DEL TRÁFICO DE DATOS EN REDES WIFI, BASADO EN SOFTWARE LIBRE, PARA LA GERENCIA DE PLANIFICACIÓN DE CANTV"

Consideran que el mismo cumple con los requisitos exigidos por el plan de estudios conducente al Título de Ingeniero Electricista en la mención de Comunicaciones, y sin que ello signifique que se hacen solidarios con las ideas expuestas por el autor, lo declaran APROBADO.

Prof. William Jota
Jurado

Prof. Carlos Moreno
Jurado

Prof. Zeldivar Bruzual
Prof. Guía

DEDICATORIA

Este trabajo de grado, lo dedico primero que nada a Dios Todopoderoso por colmarme de salud, fuerzas y bendiciones para hacer realidad este logro, a mi ángel predilecto que desde el cielo siempre me ha cuidado y guiado (a ti abuelito, tu siempre estuviste seguro de este logro).

A ti mamá por darme la vida y enseñarme que con amor, tolerancia y constancia nos hacemos mejores personas cada día. A mi hermano Victor, por darme la fuerza y gracias a tu confianza en mí, hiciste que no dudara de mis fortalezas y así hoy, hacer realidad lo que desde niño imaginábamos, los amo.

A mis ángeles terrenales, que no puedo llamarlos de otra manera, ya que desde siempre me han guiado por el mejor de los caminos, me han brindado su apoyo y ayuda incondicional. Estos ángeles no son más que Carmen Moreno E Yrma Moreno, que son piezas fundamentales en mi vida, gracias ustedes se hizo palpable este proyecto de vida. A Eleazar Moreno por cumplir un papel importante en mi formación, brindarme su apoyo de padre que desde siempre recuerdo y no podía faltar mi ángel respetado, me refiero a Arturo Chaparro ya que fuiste fuente de inspiración para seguir tu modelo a seguir y por ello me convierto en tu colega que más te admira.

También dedico este logro a la persona que con paciencia, amor y tolerancia y frases sabias me dio fuerza y seguridad para hacer posible la culminación de este trabajo, me refiero a ti Daniel Leguízamo, que doy gracias a Dios por ponerte en mi camino. Te Amo.

AGRADECIMIENTOS

Primeramente agradezco a Dios Padre, por ser mi creador guía y salvador, por demostrarme que cada día es una nueva oportunidad para dar lo mejor de nosotros y por llenarme de infinitas bendiciones que puedo palpar a través de personas que has puesto en mi camino, como mis familiares, profesores y amigos.

A mi mamá Cruz Moreno, por toda su dedicación, amistad incondicional, infinitas palabras de aliento, por cuidarme en enfermedad y principal apoyo en mis decisiones que me ha llevado a convertirme en un ser creyente en de la superación, agradezco este trabajo a la persona que con palabras acertadas, amor y compresión hizo que este trabajo se haya realizado a ti Daniel Leguízamo gracias por guiarme y ayudarme en momentos de oscuridad, te adoro.

A mis hermanos: Victor, Luisilma, Nairovys y María Eugenia por su apoyo incondicional en todos los aspectos de mi vida, gracias a sus vivencias y experiencias han demostrado ser unos de mis grandes tesoros.

A mis tíos y primos que con gran amor, paciencia y dedicación me demostraron la esencia de la familia, mil gracias todos por llenar cada parte de mi ser. También quiero agradecer a aquellas personas que con su granito de arena me impulsaron a terminar este camino, en especial A Yrmaris Chaparro, Irsa Moreno y Blanca Moreno, por estar pendiente de los pequeños detalles que para mi son tan apreciados, de corazón las quiero.

Un especial agradecimiento a personas que me tendieron la mano por mucho tiempo, ustedes quienes me acogieron en su techo desde que empezó esta meta como lo fueron: Lourdes Moreno y Noel Carrasquel y a una linda prima que en momentos

de sensibilidad y tristezas me alegraba con un solo “hola linda” a ti Patricia Carrasquel gracias por tu compañía.

A la familia Yeguez Alcázar, que gracias a su recibimiento y apoyo, en momentos de desespero, ustedes son participe de este logro. Mil gracias.

A todos mis profesores de la escuela de ingeniería eléctrica que fueron piezas indispensables para formación con ingeniero de la universidad que vence la sombra. En especial a Zeldivar Bruzual por guiarme y asesorarme en todo momento y hacer posible el desarrollo de este trabajo.

A las personas que conforman el proyecto de Software libre se CANTV, que fueron de gran apoyo para hacer realidad este proyecto en especial a Dr. Pedro Bonillo por darme la oportunidad de iniciar esta investigación, a Jesellys García, Eduardo Morales y José Luis Navas por guiarme y apoyarme en este proyecto.

A mis compañeros de clases: Daniel Rengifo; Jonathan Saltarin, Irán Macias, Francisco Cabeza, Jonathan Tochón, Gabriel Guerrero y Juan Pérez quienes con su ayuda y dedicación me ayudaron a terminar esta meta en común.

A una persona súper especial el cual ha sido un gran amigo desde el comienzo de este camino, él ha sido un gran apoyo, se convirtió en alguien tan especial a quien me siento orgullosa por su fuerza y sabiduría, a ti "Gabriel Peroza”, te aprecio muchísimo y mil gracias por tu compañía en momentos que sentía caer.

A mis amigas: Luisa y Vanessa Liñeira, Sylvie Suzzarinni, Mariyim Alcántara y Enoe Antuárez por escucharme, entenderme y ayudarme a crecer como ser humano, gracias a ustedes el estar en otra cuidad se me hizo mucho más fácil las quiero.

No podía dejar de agradecerles a tres personas que hicieron posibles que este día llegara, a la Doctora Claudia León por apoyarme y ser partícipe de este proyecto, María Auxiliadora por hacerle honor a tu nombre y auxiliarnos en los momentos donde pensamos que no podemos seguir y Wilfredo Bolívar por guiarme y compartir sus conocimientos, en fin doy gracias a muchas personas que con su ayuda y pendiente hicieron posible la finalización de este proyecto.

Emelys Del V. Obando M.

DESARROLLO DE UN PROTOTIPO DE ADMINISTRACIÓN Y MONITOREO DEL TRÁFICO DE DATOS EN REDES WIFI, BASADO EN SOFTWARE LIBRE, PARA LA GERENCIA DE PLANIFICACIÓN DE CANTV

Prof. Guía: Ing. Zeldivar Bruzual. Tutor Industrial: Dr. Pedro Bonillo. Tesis. Caracas. U.C.V. Facultad de Ingeniería. Escuela de Ingeniería Eléctrica. Ingeniero Electricista. Opción: Comunicaciones. Institución: CANTV. **2009. 145 h. + anexos.**

Palabras Claves: WIFI, Administración y Monitoreo, tráfico de datos, sistema operativo LINUX.

Resumen: Se plantea un estudio de los conceptos fundamentales para el monitoreo y administración del tráfico de las redes WIFI. También se realiza la descripción del protocolo SNMP y de cómo éste funciona en el ambiente LINUX y estándares de las redes inalámbricas. También se estudia el sistema operativo LINUX y las facilidades que ofrece para la administración y monitoreo de redes WIFI. Por otra parte, se realiza una ejecución de una serie de comandos del sistema operativo de código abierto que se utilizan para monitoreo y administración de las redes. Además se describe el desarrollo de un prototipo de administración y monitoreo del tráfico de datos para las redes WIFI de CANTV, donde se describen los requerimientos mínimos de Software y Hardware, con los que debe cumplir el *host* donde se instala la aplicación. Luego se describen las pruebas realizadas por el prototipo desarrollado.

INDICE GENERAL

INDICE DE TABLAS

INDICE DE FIGURAS

ACRÓNIMOS

ACK: Acknowledgement (acuse de recibo)

ABM: Asynchronous Balanced Mode

AES: Advanced Encryption Standard

ARM: Asynchronous Response Mode

ASN.1: Abstract Syntax Notation 1

ARP: Address Resolution Protocol

ATA: Advanced Technology Attachment

CIDR: Classless Inter-Domain Routing

CPE: Equipo Local del Cliente

CHAP: Challenge Handshake Protocol

DCN: Dynamic Circuit Network

DHCP: Dynamic Host Configuration Protocol

DNS: Domain Name System

DSSS: Direct Sequence Spread Spectrum

EAP: Extensible Authentication Protocol

EGP: Protocolo de Gateway o Salida Exterior

FHSS: Frecuency Hopping Spread Spectrum

FTP: File Transfer Protocol

GRE: Generic Routing Encapsulation

HDLC: High-Level Data Link Control

HTB: Hierarchical Token Bucket

HTTP: Hiper Text Transfer Protocol

IAB: Internet Activities Board

ICMP: Internet Control Message Protocol

IEEE: Institute Of Electronical And Electronics Engineers

IETF: Internet Enginnering Task Force

IP: Internet Protocol

ISM: Industrial, Scientific and Medical

IR: Infrared, electromagnetic radiation

ISO: International Standards OrganizationRARP: Reverse Address Resolution Protocol

ITU: Unión Internacional de Telecomunicaciones

LAPB: Link Access Procedure, Balanced

LAPD: Link Access Protocol for D-channel

LAN: Local Area Network

LLC: Logical Link Control

MAC: Media Access Control

MAN: Metropolitan Area Network.

ME: Metro Ethernet

MIB: Management Information Base

MTU: Maximum Transfer Unit

NACK: Negative ACKnoledgement, o asentimiento negativo

NAT: Network Address Translation

NetBIOS: Network Basic Input/Output System

NFS: Network File System

NGN: Next Generation Networking

NRM: Normal Response Mode

OFDM: Orthogonal Frequency Division Multiplexing

OSA: Open System Autentication

OSI: Open System Interconnection

PAN: Personal Area Network

PAP: Password Authentication Protocol

PHP: Hypertext Pre Processor

PPP: Point-to-point Protocol

RF: Radio Frecuency

RPC: Remote Procedure Call

RRDTOOL: Ruond Robin Database Tool

RSA: Rivest, Shamir & Addleman

SLIP: Serial Line Internet Protocol

SKA: Shared key Authorization

SMI: Structure of Management Information

SMTP: Simple Mail Transfer Protocol

SNMP: Simple Network Management Protocol

SSID: Service Set IDentifier

TCP: Transmission Control Protocol

TKIP: Temporal Key Integrity Protocol

TMN: Telecommunications Management Network

TTL: Time To Live

UDP: Protocolo de Datagramas de Usuario

UUCP: Unix to Unix CoPy

VLAN*:* Virtual LAN

WAN: Wide Area Network

WEP: Wired Equivalent Privacy

WIFI: Wireless Fidelity

XINETD: Extended Internet Daemon

INTRODUCCIÓN

A través de los años el crecimiento de la red de telecomunicaciones ha sido impresionante, es decir, la cantidad de usuarios cada día es mayor, debido a la necesidad del ser humano de estar comunicado y a la vez informado, por esta razón las redes de cómputo de las empresas de telecomunicaciones (por ejemplo CANTV), se vuelven cada vez más complejas y la exigencia de la operación es cada vez mas demandante. Las redes, cada día soportan aplicaciones y servicios estratégicos realizados por la empresa. Por lo cual la administración y monitoreo de redes se ha convertido en una labor cada vez mas importante y de carácter pro-activo para evitar problemas y ofrecer seguridad en el tráfico de datos.

Por otra parte, el análisis de las diferentes redes ha sido un aspecto importante para el desarrollo eficaz de las telecomunicaciones, en este caso se estudiará el tráfico de datos de las redes WIFI, que forma parte de las llamadas WLAN (*Wireless Lan*, redes de área local inalámbrica) o estándar IEEE 802.11.Cuando hablamos de WIFI nos referimos a una de las tecnologías de comunicación inalámbrica mediante ondas más utilizada hoy en día.

El Proyecto que se presenta a continuación, trata sobre el desarrollo de un prototipo de administración y monitoreo del tráfico de datos de las redes WIFI basado en el sistema operativo LINUX para la Gerencia de Planificación de CANTV. Este prototipo utiliza los comandos de conectividad y administración que el sistema operativo LINUX ofrece.

El documento se encuentra dividido en seis (6) capítulos de desarrollo. En el primer capítulo, se realiza un estudio de los conceptos fundamentales para el monitoreo y administración de las redes WIFI. También se realiza la descripción del protocolo SNMP y de cómo éste funciona en el ambiente LINUX. Por último, se

estudia el sistema operativo LINUX, las facilidades que ofrece para el monitoreo y administración de redes WIFI y los protocolos utilizados para el desarrollo de este prototipo.

En el segundo capítulo, se realiza un estudio de los comandos del sistema operativo LINUX que se utilizan para monitoreo y administración del tráfico en redes WIFI, principales características y servicios sobre TCP/IP

En el tercer capítulo se describe la topología de las redes WIFI de CANTV, haciendo énfasis en los equipos existente en la red y funciones del sistema de administración y monitoreo de redes IP utilizado en CANTV llamado Tivoli Netcool/OMNIbus y las razones del por qué no administra las redes WIFI de dicha empresa.

En el cuarto capítulo se realiza un estudio y evaluación sobre diferentes sistemas de gestión de redes que funcionan en ambiente Linux, para tomar uno de ellos como base para el desarrollo de un prototipo de Administración y Monitoreo del tráfico de datos en redes WIFI.

En el quinto capítulo se describe el diseño del prototipo que permite monitorear y administrar el tráfico de datos de las redes WIFI, lo que describe una serie de comandos para realizar el diseño, descripción de las funciones requeridas por la gerencia y planificación de CANTV.

En el sexto capítulo, se muestran las pruebas realizadas por el programa de monitoreo y administración de tráfico de datos. Además, de los resultados obtenidos en éstas pruebas, limitaciones del prototipo desarrollado y ventajas y desventajas que tiene el prototipo al ser desarrollado bajo el software libre.

PLANTEAMIENTO DEL PROBLEMA

La humanidad ha tenido y tiene la necesidad de estar informada, es por ello que desde hace décadas los medios de comunicación han crecido y evolucionado de manera impresionante con el fin de llevar a cada persona el tipo de información que requiera. Es por ello que las empresas de telecomunicaciones han crecido de manera impactante para poder proveer diferentes vías de información según lo requerido por cada persona.

La comunicación está presente en cada lugar de nuestras vidas, como el uso de telefonía, audiovisuales e Internet entre otros, en principio estos 3 servicios han sido de mucha utilidad para el desarrollo tecnológico de la sociedad, es por esto, que día a día se estudia y trabaja en la arquitectura y mantenimiento de redes mas robustas y seguras para poder prestar numerosos servicios de telecomunicación.

Consecuencia de toda esta evolución, en nuestro país se está planteado un proceso de profundas transformaciones tecnológicas, que se reflejan en una mayor movilización y participación de la población en la búsqueda de mejores plataformas que proveen mayor calidad en el área de las telecomunicaciones.

Por ello el Estado Venezolano, ha impulsado el desarrollo de proyectos en el área de la tecnología de la información y las telecomunicaciones (TIC), que buscan fomentar la aplicación y aprovechamiento de dichas tecnologías de manera apropiada y en función de las necesidades sociales y el contexto socio-político y económico. Para ello la Compañía Anónima Nacional Teléfonos de Venezuela (CANTV), formuló un proyecto de red inalámbrica para suministrar conexión de Internet de banda ancha.

En virtud de lo antes mencionado el Estado Venezolano siempre está en la búsqueda de soluciones para fomentar políticas que permitan satisfacer las necesidades de la población así se expone en el decreto 3390 en Gaceta oficial Nº 38.095 de fecha 28/12/2004, la utilización obligatoria de software libre para la administración pública y servicios públicos, con el fin de desarrollar Estándares Abiertos que permita a la industria del software nacional, aumentar y fortalecer sus capacidades y como consecuencia disminuir costos por licencias de sistemas propietarios.

Las redes de comunicaciones inalámbricas facilitan la operación en lugares donde la computadora no puede permanecer en un solo lugar, como en almacenes o en oficinas que se encuentren en varios pisos. Los beneficios de los sistemas de estas redes son tan grandes que necesitan un nivel de monitoreo tal que se minimice el tiempo de respuesta en caso de alguna falla, ya sea por caída de conexión, problemas con algún Punto de Acceso (AP) ó problemas con la velocidad de conexión, entre otras.

Actualmente en CANTV existe la necesidad de administrar y monitorear el tráfico de datos de las redes WIFI para así poder tener un mayor control de paquetes, conexiones establecidas, rendimientos de memoria de los equipos, promedios y mejoras en la red de telecomunicaciones de dicha empresa. La Gerencia de Planificación de CANTV se ha dado la tarea de realizar de manera progresiva una migración hacia el Software Libre, con la finalidad de disminuir costos y permitir una mayor flexibilidad y futuras mejoras en los Software que se utilizan para administrar y monitorear las redes. Este trabajo forma parte de la migración hacia Software libre de un segmento de las principales redes de CANTV.

Para ello se dispone la utilización de un software libre que cumpla con estas características con la finalidad de automatizar el proceso de monitoreo y minimizar el tiempo de respuesta cuando ocurra un problema en la red inalámbrica.

OBJETIVOS

OBJETIVO GENERAL

Desarrollar un prototipo de administración y monitoreo del tráfico de datos de redes WIFI para la Gerencia de Planificación de la empresa CANTV, utilizando como herramienta principal el Sistema Operativo Linux.

OBJETIVOS ESPECÍFICOS

- Analizar los conceptos fundamentales, las funciones y los procedimientos para la administración y monitoreo de redes WIFI.

- Establecer los lineamientos teóricos, características y funcionamiento del sistema operativo GNU/LINUX y las facilidades que éste ofrece para la administración y monitoreo de redes WIFI.

- Recabar información de las redes WIFI de la Compañía Anónima Nacional Teléfonos de Venezuela (CANTV), haciendo especial énfasis en el tráfico de datos.

- Diseñar un prototipo de administración y monitoreo del tráfico de datos de las redes WIFI de CANTV basado en las herramientas del software libre.

- Evaluar el funcionamiento del prototipo diseñado, considerando las ventajas y desventajas de su desarrollo en Software libre.

JUSTIFICACIÓN

Desde el pasado, ha surgido la necesidad de incrementar y mejorar el uso de las redes de información, lo que a su vez ha provocado que la administración y monitoreo de las mismas sea un factor preponderante en el campo de las telecomunicaciones, esto con la finalidad de que se pueda mantener un adecuado y óptimo funcionamiento. Es aquí donde se hace necesaria una herramienta de rápido acceso, que nos permita realizar de manera eficaz y confiable, la administración y monitoreo del tráfico de datos en redes WIFI.

A pesar de que los actuales enlaces y conexiones a Internet son muy rápidos, es normal encontrar enlaces que tengan distintas necesidades, es decir, con conexiones que sirven de soporte para varios tipos de servicios. Por tal motivo se debe tener bien definido cuales servicios son los fundamentales y el ancho de banda que ellos requieren, para que los administradores de red distribuyan este recurso logrando obtener un servicio mejorado en cuanto a la velocidad de conexión.

Luego, la necesidad de tener un recurso de Software Libre es muy importante en lugares donde la administración y control de redes WIFI resultan muy complejos y costosos, por los paquetes que actualmente existen en el mercado. Estos programas pueden también resultar complejos en su uso para los administradores de red. Es por esto y algunas otras razones que en los últimos años, la empresa CANTV ha estado migrando de manera paulatina los sistemas operativos de sus equipos administradores hacia el Software Libre, mejor conocido como LINUX/GNU.

El sistema operativo LINUX fue desarrollado buscando la portabilidad de las fuentes: casi todo el software gratuito desarrollado para UNIX se compila en LINUX sin problemas. Y todo lo que se hace para LINUX (código del núcleo, controladores, librerías y programas de usuario) es de libre distribución. LINUX también implementa todo lo necesario para trabajar en red con TCP/IP. Desde controladores

para las tarjetas de red más populares hasta SLIP/PPP, que permiten acceder a una red TCP/IP por puerto serial.

Por todo lo antes expuesto, la Gerencia de Planificación de CANTV ha considerado un proyecto que le permita obtener una propuesta factible de un Sistema para Administrar y Monitorear redes WIFI con criterio de mejorar el rendimiento de la red y administración de los paquetes existentes en la red, haciendo uso de las herramientas que pueda ofrecer el software libre, para lo cual es necesario realizar investigación, estudio y análisis de todo lo relacionado con administración de redes WIFI, monitoreo de redes y del sistema operativo LINUX.

La Gerencia de Planificación de CANTV considera que este trabajo proporcionará las bases teóricas y prácticas necesarias para una futura implementación de un Sistema de Administración y Monitoreo de Redes viable y a su vez contribuirá en gran medida con la migración que actualmente se encuentra en marcha dentro de la empresa hacia el sistema operativo LINUX.

FACTIBILIDAD

Para hacer posible este trabajo, la empresa CANTV se hará responsable de prestar material, asesoramiento, cursos, información acerca de la empresa, equipos y espacio físico.

Luego de la migración hacia el software libre, CANTV ha asignado proyectos que involucran el estudio detallado de LINUX y hace que el trabajo sea factible y cumpla con los objetivos y actividades asignadas para desarrollar de manera eficiente el prototipo de administración y monitoreo del tráfico de datos de las redes WIFI CANTV.

CAPÍTULO I

1 MONITOREO Y ADMINISTRACIÓN DE REDES WIFI

1.1 ADMINISTRACIÓN DE RED

La administración de redes consiste en la organización, control, toma de precauciones y supervisión de la red, para mantener su funcionamiento eficiente, mediante el empleo de herramientas de red, aplicaciones y dispositivos.

A continuación se destaca un conjunto de actividades que a corto plazo permiten realizar un seguimiento de las tareas administrativas y elaborar informes periódicos para su posterior estudio:

- Detección y aislamiento de fallas.
- Evaluación del tráfico de datos.
- Mantenimiento de registro histórico de problemas.
- Mantenimiento de configuraciones.
- Contabilidad de red.
- Control de acceso [1].

1.1.1 OBJETIVOS DE LA ADMINISTRACIÓN DE RED

Los objetivos de la administración de red son los siguientes:

- Proporcionar herramientas automatizadas y manuales de administración de red para controlar posibles fallas o degradaciones en el desempeño de la misma.
- Disponer de estrategias de administración para optimizar la infraestructura existente, optimizar el rendimiento de aplicaciones y servicios. Además,

prever los crecimientos en la red esperados debido al cambio constante en la tecnología [2].

1.1.2. FUNCIONES DE ADMINISTRACIÓN DE RED

Las funciones de administración de red se basan en dos procedimientos que ayudan a llevar a cabo numerosas tareas, estos procedimientos son los siguientes:

- **Monitoreo**

El monitoreo es un proceso eminentemente pasivo, el cual se encarga de observar el estado y comportamiento de la configuración de red y sus componentes. También se encarga de agrupar todas las operaciones para la obtención de datos acerca del estado de los recursos de la red.

- **Control**

El control es un proceso que se lo considera activo, debido a que permite tomar información de monitoreo y actuar sobre el comportamiento de los componentes de la red administrada. Abarca la configuración y seguridad de la red, como por ejemplo, alterar parámetros de los componentes de la red [3]

1.2. DEFINICIÓN Y OBJETIVOS DEL MONITOREO DE REDES.

1.2.1 MONITOREO

Monitoreo es la realización del estudio del estado de los recursos. Las funciones del monitoreo de red se llevan a cabo por agentes que realizan el seguimiento y registro de la actividad de red, la detección de eventos y la comunicación de alertas.

El monitoreo de una red abarca 4 fases:

- Definición de la información de administración que se monitorea.
- Acceso a la información.
- Diseño de políticas de administración.
- Procesamiento de la información.

Los tipos de monitoreo son:

- Local.
- Remoto.
- Automático.
- Manual.

Los elementos monitoreados pueden ser:

- En su totalidad.
- En segmentos.

El monitoreo puede ser realizado en forma:

- Continua.
- Eventual.

1.2.2 OBJETIVOS DEL MONITOREO

Los objetivos del monitoreo son los siguientes:

- Identificar la información a monitorear.
- Utilizar la información obtenida dentro de las distintas áreas funcionales de la administración de red.

- Tomar nuevas medidas sobre aspectos de los protocolos, colisiones, fallas, paquetes, etc.
- Almacenar la información obtenida en Bases de Información de gestión para su posterior análisis.
- Dentro del monitoreo de la actividad de la red, los eventos típicos que son monitoreados suelen ser:
    - Registro del estado de finalización de los procesos que se ejecutan en la red.
    - Registro de las entradas y salidas de los usuarios en la red.

En función de la prioridad que tengan asignados los eventos y de la necesidad de intervención, se pueden utilizar diferentes métodos de notificación o alerta tales como:

- **Mensajes en la consola**: método en el que se suele codificar en función de su importancia.
- **Mensajes por correo electrónico**: método mediante el cual se envía contenido el nivel de prioridad y el nombre del evento ocurrido.
- **Mensajes a móviles**: método utilizado cuando el evento necesita intervención inmediata del administrador de red.

1.2.3. ASPECTOS FUNCIONALES DE LA ADMINISTRACIÓN DE RED

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

Ésta arquitectura de administración, se encuentra dividida en cinco categorías de servicios de administración denominadas Áreas Funcionales Específicas de Administración, las cuales se muestran a continuación:

- Administración de prestaciones.
- Administración de fallas.
- Administración de contabilidad.
- Administración de configuraciones.
- Administración de seguridad.

Los aspectos o categorías funcionales de la administración de red brindan servicio a las actividades de Monitoreo y Control de red. Se las puede ubicar de la siguiente manera:

a. **Monitoreo de la red**: obtiene información de los elementos.

- Administración de prestaciones.
- Administración de fallas.
- Administración de contabilidad.
- Administración de configuraciones.

b. **Control de la red**: actúa sobre los elementos.

- Administración de configuraciones.
- Administración de seguridad.

1.3 ADMINISTRACIÓN DE PRESTACIONES O RENDIMIENTO

Es medir la calidad de funcionamiento, proveer información disponible del desempeño de la red (hardware y software), asegurar que la capacidad y prestaciones de la red correspondan con las necesidades de los usuarios, analizar y controlar

parámetros como: utilización, rendimiento, tráfico, cuellos de botella, tiempo de respuesta, tasa de error, etc; esto de los distintos componentes de red como conmutadores, enrutadores, *hosts*, entre otros, para poder ajustar los parámetros de la red, mantener el funcionamiento de la red interna en un nivel aceptable, poder efectuar análisis precisos y mantener un historial con datos estadísticos y de configuración, predecir puntos conflictivos antes de que éstos causen problemas a los usuarios.

El conocimiento de esta información nos permite en el futuro, tomar acciones correctivas como balanceo o redistribución de tráfico, establecer y reportar tendencias para ser utilizadas en la toma de decisiones y planificación del crecimiento.

Se deben definir claramente los parámetros de funcionamiento o desempeño alrededor de los cuáles, se van a organizar las tareas de Administración de prestaciones como las siguientes:

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

1.4 ADMINISTRACIÓN DE FALLAS

Los objetivos de esta área son: detección, aislamiento, corrección, registro y notificación de los problemas existentes en la red, sondeo periódico en busca de mensajes de error y establecimiento de alarmas.

Las consecuencias de estas fallas pueden causar tiempo fuera de servicio o la degradación inaceptable de la red, por lo que es deseable su pronta detección y corrección.

La diferencia entre falla y error está en que, un error es un evento aislado como la pérdida de un paquete o que éste no llegue correctamente, pero una falla es un funcionamiento anormal que requiere una intervención para ser corregido. La falla se manifiesta por un funcionamiento incorrecto o por exceso de errores.

Las acciones o procedimientos para esta corrección son:

- Determinar exactamente dónde está la falla.
- Aislar el resto de la red, para que pueda seguir operando sin interferencia.
- Reconfigurar la red para minimizar el impacto de operar sin el componente averiado.
- Reparar o reemplazar el componente averiado para devolver la red al estado inicial.
- Registrar la detección y la resolución de fallas.
- Hacer seguimiento de la reparación de fallas**.**

Una buena política de Administración, es la prevención, es decir, debe adelantarse a los posibles problemas y resolverlos antes de que se produzcan.

1.5 ADMINISTRACIÓN DE LA CONFIGURACIÓN

Es el proceso de preparación de los dispositivos, puesto que la configuración de éstos, determina el comportamiento de los datos en la red.

Las funciones de ésta administración son: inicialización, desconexión o desactivación ordenada de la red o de parte de ella, mantenimiento y adición de componentes, reconfiguraciones, definición o cambio de parámetros de configuración, denominación de los elementos de la red, conocimiento de que dispositivos hay en la red, hardware y configuraciones de software de dichos dispositivos.

Las tareas que se presentan en la administración de configuración son:

- Definir información de configuración de recursos.
- Mantener ésta información, por si se sufre un ataque, poder realizar una comprobación de la información de configuración para asegurar que permanece en un estado correcto.
- Modificación de propiedades de recursos e información al usuario de estos cambios.
- Establecer qué usuarios pueden utilizar qué recursos.
- Inicialización y finalización de servicios de red.

Las herramientas típicas para ésta administración son: monitorear la red para ver qué elementos hay activos y con qué características obtener la información, para saber de qué modo están conectados entre sí los diferentes elementos, ésta información se mantiene para ayudar a otras funciones de administración.

1.6 ADMINISTRACIÓN DE LA CONTABILIDAD

Su objetivo es controlar el grado de utilización de los recursos de red, controlar el acceso de usuarios y dispositivos a la red, obtener informes, asignar privilegios de acceso a los recursos.

Finalmente se debe hacer un seguimiento del uso de recursos de la red por parte de un usuario o grupo de usuarios. Todo esto para regular apropiadamente las aplicaciones de un usuario o grupo y además permitir una buena planificación para el crecimiento de la red.

1.7 ADMINISTRACION DE LA SEGURIDAD

Su objetivo es controlar el acceso a los recursos de la red, y protegerla de modo que no pueda ser dañada (intencional o involuntariamente), y que la información que es vulnerable pueda ser utilizada con una autorización apropiada. Comprende el conjunto de facilidades mediante las cuales, el administrador de la red modifica la funcionalidad que proporciona la red frente a intentos de acceso no autorizados.

En la Administración de Seguridad se pueden tener dos tipos de ataques:

- Ataques Activos.
- Ataques Pasivos.

1.7.1. ATAQUES ACTIVOS

En este tipo de ataques existe evidencia del hecho por mal funcionamiento de componentes o servicios, o por sustitución de usuarios en ejecución de tareas orientados a tratar de conseguir información privilegiada o interrumpir un servicio crítico para la organización, puede ser desde el interior o del exterior.

Ejemplos de estos ataques son: modificación del contenido de los datos que circulan por la red, alteración del orden de llegada de los datos, supresión de mensajes con un destino particular, saturación de la red con datos inútiles para

degradar la calidad de servicio, engaño de la identidad de un *host* o usuario para acceder a datos confidenciales, desconfiguraciones para sabotaje de servicios.

1.7.2. ATAQUES PASIVOS

Ataques difíciles de detectar, ya que no se produce evidencia física del ataque pues no hay alteración de datos ni mal funcionamiento o comportamiento fuera de lo habitual de la red, escucha o "intercepción del tráfico de la red y los servicios involucrados", estudio de parámetros de configuración de manera ilegal por parte del intruso, robo de información sensible para las organizaciones.

Para cualquiera de los tipos de ataques se puede prevenir o solucionar a través de las siguientes actividades:

- Fortalecer políticas de administración y asignación de claves.
- Historiales de seguridad, para posterior análisis.

- Localizar la información importante.
- Registrar los usuarios que consultan dicha información y durante qué períodos de tiempo, así como los intentos fallidos de acceso.
- Señales de alarma**.**
- Configurar de manera segura los elementos y servicios de red.

1.8. REDES DE COMPUTADORAS

Es una colección interconectada de computadores autónomos.

Las redes se utilizan para:

- Compartir recursos, especialmente la información (los datos)

- Proveer la confiabilidad: más de una fuente para los recursos
- La escalabilidad de los recursos computacionales: si se necesita más poder computacional, se puede comprar un cliente más, en vez de un nuevo *mainframe*
- Comunicación

1.8.1. CLASIFICACIÓN GENERAL

Las posibles clasificaciones de las redes de computadoras pueden ser muchas, atendiendo cada una de ellas a diferentes propiedades, siendo las más comunes y aceptadas las siguientes:

a) Clasificación según su tamaño y extensión:

Redes de área personal (*PAN: Personal Area Network*). Las redes de área personal son una categoría en redes que incluye distancias pequeñas y cerradas. El alcance típico de una PAN es de unos pocos metros. Su aplicación principal radica en la comunicación entre dispositivos personales.

Redes de área local *(LAN: Local Area Network)*. Las redes de área local son redes de computadores cuya extensión es del orden de 10 metros a 1 kilómetro. Son redes pequeñas, habituales en oficinas y empresas pequeñas. Las velocidades de transmisión típicas son de 10 a 100 Mbps.

Redes de área metropolitana *(MAN: Metropolitan Area Network)*. Las redes de área metropolitana son redes de computadores de tamaño superior a una red LAN, soliendo abarcar el tamaño de una ciudad. Son típicas de empresas y organizaciones que poseen distintas oficinas distribuidas en una misma área metropolitana, por lo que, comprenden un área alrededor de 10 kilómetros.

Redes de área amplia *(WAN: Wide Area Network)*. Las redes de área amplia tienen un tamaño superior a una MAN, y consisten en una interconexión de redes LAN. Estas redes están interconectadas por medio de enrutadores *(routers)*, dispositivos de red encargados de dirigir los paquetes de un enrutador a otro hacia la red LAN o computador adecuado. Su tamaño puede oscilar entre 100 y 1000 kilómetros.

Redes Internet. La red Internet es una red de redes, vinculadas mediante enrutadores de compuerta *(router gateway).* Una compuerta es un dispositivo especial que puede traducir información entre sistemas con formato de datos diferentes. El alcance de una red Internet puede ser desde 10000 kilómetros en adelante.

1.8.2. SISTEMA DE INTERCONEXIÓN ABIERTA *(OSI: Open System Interconnection)*

Todas las redes de computadoras, por ser de naturaleza abierta, es decir, sistemas que se comunican con otros sistemas de comunicaciones, deben mantener la compatibilidad a pesar de las variedades de tecnologías relacionadas con la comunicación de datos. Para ello, la Organización Internacional de Estándares *(ISO: International Standards Organization)* definió un modelo de referencia teórico llamado Sistema de Interconexión Abierta *(OSI: Open System Interconnection),* el cual permite a los diferentes fabricantes mantener dicha compatibilidad. El modelo está definido por capas, facilitando de esta manera, las soluciones de interconexión de los equipos. En la figura 1, se muestra esquemáticamente la estructura del modelo OSI, y la función asociada a cada una de las capas.

7. - Capa de Aplicación	Aloja el programa de red que interactúa con el usuario
6. - Capa de Presentación	Maneja los datos de la aplicación y los acomoda en un formato que pueda ser transmitido en un red
5. - Capa de Sesión	Establece conexiones lógicas entre puntos de la red
4. - Capa de Transporte	Maneja la entrega entre un punto y otro los mensajes de una sesión
3. - Capa de Red	Maneja deestinos. rutas, congestión en rutas, alternativas de enrutamiento, etc.
2. - Capa de Enlace	Entrega los datos entre un nodo y otro en un enlace de red
1. - Capa Física	Define la conexión física de la red

Figura 1. Estructura del modelo OSI

A pesar de que dicho modelo de referencia nació con el objetivo primordial de estandarizar la forma de interconexión en todos los sistemas de comunicaciones, actualmente en el área de las comunicaciones en redes de computadoras, dicho modelo es poco usado. Esto es así, puesto que luego nació un nuevo modelo de referencia denominado TCP/IP (*Transmission Control Protocol/ Internet Protocol*), el cual, debido a su amplia aceptación a nivel mundial, es el modelo más ampliamente usado para la interconexión de redes de computadoras. Dicho modelo será descrito a continuación.

1.8.4. PROTOCOLOS UTILIZADOS.

TCP/IP (*Transmission Control Protocol/Internet Protocol***)**

Para que los computadores enlazados en una red puedan entenderse, es necesario que manejen un lenguaje común independiente del tipo de computador y del sistema operativo. La diversidad que existe entre cada dispositivo enlazado provoca numerosos conflictos, los cuales se resuelven con el empleo de diferentes protocolos de comunicaciones. Un protocolo es una serie de códigos y formatos que definen como se transmite y se recibe la información por la red, y además se encargan

de realizar las tareas de corrección de errores para verificar que la información sea transmitida correctamente.

Para la comunicación a través de las redes de computadora se ha desarrollado el conjunto de protocolos TCP/IP (*Transmission Control Protocol/ Internet Protocol*). Este grupo de protocolos, incorporan una técnica que permite segmentar la información. Así, cada mensaje es dividido en pequeños paquetes de datos, impidiendo que una transmisión, por grande que ésta sea, monopolice los servicios de la red, permitiendo además, que por una misma línea de datos, se pueda transportar paquetes de información correspondientes a diferentes comunicaciones.

A continuación se describirán brevemente los protocolos que conforman cada una de las capas TCP/IP, empezando por los niveles inferiores.

a). Protocolos de Acceso a la Red:

Protocolo de Resolución de Direcciones *(ARP: Address Resolution Protocol)***.** El protocolo ARP realiza dos funciones: obtener una dirección física dada una dirección IP, utilizando una tabla que indica la correspondencia entre ellas, y contestar peticiones realizadas por otras máquinas.

Protocolo de Resolución de direcciones inverso *(RARP: Reverse Address Resolution Protocol)***.** Este protocolo actúa en caso inverso al protocolo ARP, convirtiendo una dirección física en una dirección IP. El RARP es una adaptación del ARP y usa el mismo formato de mensaje.

b) Protocolo de Internet *(IP: Internet Protocol)*

El Protocolo de Internet **IP** es el más utilizado para la interconexión entre redes, su trabajo es proporcionar un medio de transporte modo datagrama. IP está implementado en todos los computadores y dispositivos de encaminamiento,

transmite datos de un computador a otro, pasando por uno o varios dispositivos nodo a nodo.

Servicios Básicos**:** El protocolo IP presenta dos servicios básicos en la interfaz con la capa superior: envío y entrega. El servicio *Envío,* se utiliza para solicitar la transmisión de una unidad de datos. El servicio *Entrega,* se utiliza para notificar al usuario la llegada de la unidad de datos.

Datagramas**:** Es un grupo de datos autocontenidos, que de manera independiente llevan información suficiente para ser encaminada desde el computador de origen a uno de destino. El formato de los datagramas IP, consiste en una parte de cabecera y en una parte de datos proveniente de las capas superiores cuyo tamaño es variable. La longitud máxima de un datagrama IP es de 65535 *bytes*. En la Figura 2 se aprecia la forma básica del formato de un datagrama IP.

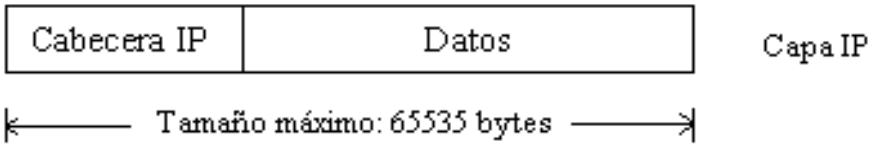

Figura 2. Formato del datagrama IP

Direcciones IP**:** Cada computador y cada dispositivo de encaminamiento tendrá una dirección única cuya longitud será de 32 *bits*; esta será utilizada en los campos dirección origen y dirección destino de la cabecera IP. La dirección consta de un identificador de red y de un identificador de computador *(Host).* La dirección IP más pequeña es la 0.0.0.0 y la mayor es 255.255.255.255.

Existen varias clases de redes teniendo en cuenta la longitud del campo de red y del campo computador. La clase a la que pertenece una dirección puede ser determinada por la posición del primer 0 en los cuatro primeros bits. La Figura 3 muestra dichas clases.

Figura 3. Direcciones IP según la clase de red.

Clase A: Pocas redes, cada una con muchos computadores. 7 *bits* (red) y 24 bits (computador).

Clase B: Un número medio de redes, cada una con un número medio de computadores. 14 *bits* (red) y 16 bits (computador).

Clase C: Muchas redes, cada una con pocos computadores. 21 *bits* (red) y 8 *bits* (computador).

Clase D*:* Multidifusión *(Multicasting),* en la cual el datagrama se dirige a múltiples computadores.

Clase E: Reservado para el futuro.

La Tabla 1 muestra el número de redes y de computadores por red en cada una de las tres clases primarias de direcciones IP:

Tabla 1. Máximas redes y computadores permitidas según la clase de red.

Clase	**Bits en el prefijo**	**Máx. Nº Redes**	**Bits en el sufijo**	**Max. Nº Computadores por red**
A	7	128	24	16777216
B	14	16384	16	65536
C	21	2097152	8	256

1.9 PROTOCOLO SIMPLE DE GESTIÓN DE RED SNMP (*SIMPLE NETWORK MANAGEMENT PROTOCOL*).

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

La simplicidad que presenta produce deficiencias para transferir grandes cantidades de información, poca o ninguna seguridad, entre otras cosas. El protocolo SNMP funciona en la capa de aplicación. SNMP ofrece un entorno de trabajo estandarizado y un lenguaje común empleado para el monitoreo y gestión de los dispositivos de una red, éste entorno consta de tres partes:

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

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

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

1.9.1 GESTORES Y AGENTES

La gestión se realiza a través de una sencilla interacción entre un gestor y un agente.

El agente almacena información de sistema, de interfaces, etc, en una base de información de gestión, mientras que el gestor tiene acceso a los valores de esta base.

Los agentes también pueden enviar al gestor mensajes de advertencia (denominados *traps*), si el programa que se ejecuta en el agente detecta algún error en el entorno.

1.9.2 ARQUITECTURA DE SNMP

Se muestra a continuación los componentes del protocolo SNMP:

- Una estación de gestión.
- Un agente de gestión (incluidos agentes proxy).
- Una base de información de gestión (MIB).
- Protocolo de gestión de red.

Los elementos de la estación de gestión son los siguientes:

- Aplicaciones (para análisis de datos, etc.)
- Interfaz de usuario.
- Capacidad de convertir las solicitudes del usuario a peticiones de monitoreo.
- Control a los elementos remotos y base de datos con información de las MIBs de los elementos de la red gestionados.

1.9.3 TIPOS DE MENSAJES SNMP

Los diferentes tipos de mensajes se describen a continuación:

GetRequest: el gestor pide al agente el valor de un dato.

GetNextRequest es similar al GetRequest, permitiendo extraer datos de una tabla.

SetRequest: el gestor pide al agente que modifique los valores de las variables que especifique. El agente modificará todos o ninguno de los valores.

GetResponse: Respuesta del agente a las peticiones GetRequest, GetNextRequest y SetRequest.

Trap: Mensaje generado por el agente en respuesta a un evento que afecte a la MIB o a los recursos gestionados. El gestor no confirma la recepción de un trap al agente.

1.9.4 COMUNIDADES SNMP

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

- Cada agente es responsable de su MIB local, controlando sus estaciones gestoras.
- Control de acceso a la MIB de un agente: concepto de comunidad.

- Comunidad es la relación que se tienen entre un agente SNMP y un conjunto de estaciones de gestión SNMP, definen unas características de autentificación y control de acceso.

- El agente establece una comunidad para cada combinación deseada de autentificación y control de acceso, y a cada comunidad se le da un nombre de comunidad (*community name*) que es su nombre único dentro del agente. Este nombre las estaciones de gestión pertenecientes a una comunidad la emplean en todas las operaciones GetRequest, GetNextRequest y SetRequest.

- El agente puede establecer cualquier número de comunidades. Y a su vez una estación de gestión puede pertenecer a varias comunidades.

- Una estación de gestión debe almacenar los nombres de comunidad asociados a cada agente.

1.10 EVOLUCIÓN

Las primeras soluciones tecnológicas de Redes Inalámbricas de Área Local definidas mediante el estándar 802.11 eran soluciones de baja velocidad que estaban entre 1 y 2 Mbps (mega bits por segundo), aun así, la flexibilidad y movilidad de esta tecnología permitieron su crecimiento en los mercados tecnológicos.

Después de pasar la mayor parte de los años 90 en discusiones técnicas, en 1997 el *Institute Of Electronical And Electronics Engineers* (IEEE) ratificó el protocolo 802.11 como el estándar para las comunicaciones de las redes inalámbricas.

El estándar 802.11 define dos tecnologías de radio difusión: espectro ensanchado por secuencia directa (DSSS), espectro ensanchado por saltos de frecuencia (FHSS). Al desarrollar 802.11 se usó al máximo la tecnología para proveer una buena calidad de servicio más que para el aprovechamiento del ancho de banda, como el uso de la multiplexación por división de frecuencia ortogonal (OFDM *Orthogonal Frequency Division Multiplexing*) en 802.11a, una de las mejores formas

conocidas de enviar información por el aire en forma binaria, y el uso de espectro ensanchado (*spread spectrum*) una tecnología de transmisión de uso militar, que garantiza seguridad y confiabilidad.

Spread spectrum está diseñado para dar seguridad, integridad y confiabilidad dejando de lado la eficiencia en el uso del ancho de banda, con lo que se consume un mayor ancho de banda en relación a una transmisión de banda estrecha *(narrow band*), en redes inalámbricas se usa para minimizar la probabilidad o el impacto de las colisiones, ya que no pueden detectarse, se dividen en dos tipos:

FHSS: Espectro ensanchado por saltos de frecuencias (*frecuency Hopping Spread Spectrum):*

- Se transmite en diferentes bandas de frecuencias, saltando de una frecuencia a otra en forma aleatoria pero predecible
- Emisor y receptor deben compartir un generador de números pseudo aleatorio y semilla.802.11 establece 75 bandas de 1 Mhz.

DSSS: Espectro ensanchado por secuencia Directa (*Direct Sequence Spread Spectrum*):

- El espectro se expande al transmitir varios bits por cada bit de información real
- Para cada bit, enviamos el XOR de el y de n bits aleatorios *(chippingcode*):
  Para enviar un 0: 00100100010
  Para enviar un 1: 10010100110

- El estándar IEEE 802.11 define tres fases por las cuales deben pasar todos los clientes o estaciones de trabajo antes de obtener el acceso a la red:

- Sondeo o búsqueda de la red Inalámbrica.
- Autenticación.
- Encriptación

1.10.2. ESTÁNDARES DE LA IEEE PARA REDES INALÁMBRICAS

Del estándar 802.11 existen muchas normas pues ha sido un estándar en constante evolución y tiene un proceso de desarrollo que durará mucho tiempo pues la adaptación ha sido a medida que se requiere una mejora y han aparecido más letras, b, a, g, i, d, f, h, n.

Es un estándar IEEE que establece especificaciones para los dispositivos y las comunicaciones en redes inalámbricas de área local (WLAN), incluyendo espectros de frecuencias utilizados, velocidades de transmisión y demás parámetros que determinan esta tecnología. La norma IEEE.802.11 fue diseñada para sustituir a las capas físicas y MAC3 de la norma 802.3 (Ethernet4). Esto quiere decir que en lo único que se diferencia una red WIFI de una red Ethernet, es en la forma como los ordenadores y terminales en general acceden a la red; el resto es idéntico.

Por tanto una red local inalámbrica 802.11 es completamente compatible con todos los servicios de las redes locales de cable 802.3 (Ethernet).

1.10.3. DESCRIPCIÓN DE LOS ESTÁNDARES 802.11X

IEEE 802.11

Estándar de operación de las primeras WLAN con anchos de banda de 1 a 2 Mbps. En la banda ISM (industrial, medica y científica) en los 2.4 GHz, año de aprobación 1997.

IEEE 802.11a

Estándar que describe las especificaciones de la capa de enlace lógico y físico para las redes inalámbricas que están en la banda de los 5 GHz de la infraestructura nacional sin licencias (UNII), pero utilizando la técnica OFDM, de modulación con 52 canales, alcanzando tasas de transmisión de hasta 54 Mbps, que se pueden corresponder con un rendimiento real de 20Mbps.

Dado que la banda de 2.4 GHz tiene gran uso (pues es la misma banda usada por los teléfonos inalámbricos y los hornos de microondas, entre otros aparatos), el utilizar la banda de 5 GHz representa una ventaja del estándar 802.11a, porque se presentan menos interferencias.

Sin embargo, la utilización de esta banda también tiene sus desventajas, ya que restringe el uso de los equipos 802.11a a únicamente puntos en línea de vista, con lo que se hace necesario la instalación de un mayor número de puntos de acceso, esto significa también que los equipos que trabajan con este estándar no pueden penetrar tan lejos como los del estándar 802.11b dado que sus ondas son más fácilmente absorbidas, características de seguridad del estándar es a través de cifrado WEP, fue aprobado en 1999.

IEEE 802.11b

Estándar para WLAN entre 1 y 11 Mbps en la banda ISM a 2.4 GHz, aprobado en 1999, la norma divide el espectro en 14 canales que se traslapan, a una distancia de 5 MHz cada uno de ellos. Esto provoca que cada canal interfiera con los dos adyacentes a cada lado, ya que el ancho de banda es 22 MHz, a partir de donde la señal cae 30 dB como mínimo, características de seguridad del estándar es a través de cifrado WEP.

IEEE 802.11h

Estándar que sigue las recomendaciones hechas por la ITU que fueron motivadas principalmente a raíz de los requerimientos que la Oficina Europea de Radiocomunicaciones (ERO) estimó convenientes para minimizar el impacto de abrir la banda de 5 GHz, utilizada generalmente por sistemas militares, a aplicaciones ISM. La especificación 802.11h es una modificación sobre el estándar 802.11 para WLAN desarrollado por el grupo de trabajo 11 del comité de estándares LAN/MAN del IEEE (IEEE 802) y que se hizo público en octubre de 2003.IEEE 802.11h intenta resolver problemas derivados de la coexistencia de las redes 802.11 con sistemas de Radares y Satélite.

IEEE 802.11g

Estándar que evoluciona del estándar 802.11b, utiliza la banda de 2.4 GHz (al igual que el estándar 802.11b) pero opera a una velocidad teórica máxima de 54 Mbps, que en promedio es de 22.0 Mbps de velocidad real de transferencia similar a la del estándar 802.11a. Es compatible con el estándar b y utiliza las mismas frecuencias. El estándar se empezó a normalizar en Noviembre del 2001 y se termino en Junio del 2003. Utiliza el cifrado WEP de hasta 256 bit como medidas de seguridad.

IEEE 802.11i

Está dirigido a combatir las vulnerabilidades las redes inalámbricas para protocolos de autenticación y de codificación. El estándar abarca los protocolos 802.1x, TKIP (Protocolo de Claves Integra – Seguras – Temporales), y AES (Estándar de Cifrado Avanzado). Se implementa en WPA2.

IEEE 802.11n

En enero de 2004, el IEEE anunció la formación de un grupo de trabajo 802.11, para desarrollar una nueva revisión del estándar 802.11. La velocidad real de transmisión podría llegar a los 600 Mbps (lo que significa que las velocidades teóricas de transmisión serían aún mayores), y debería ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g, y cerca de 40 veces más rápida que una red bajo el estándar 802.11b. Mejoras en 802.11 para acceso de control al medio (MAC) para mejorar y manejar calidad de servicios, proveer clases de servicios, mejoramientos en la seguridad y los mecanismos de autentificación. Estas mejoras deben proveer la calidad requerida por servicios como telefonía IP y video en demanda. En la figura 4 se muestra la arquitectura general IEEE 802.11 y en los anexos se muestran el *stack* de protocolos IEEE 802.11**y** muestran las capas bajas IEEE 802.11

Arquitectura IEEE 802.11

Figura 4. Arquitectura IEEE 802.11

LLC: *Logical Link Control*

MAC: *Media Access Control*

FHSS: *Frecuency Hopping Spread Spectrum*

DSSS: *Direct Sequence Spread Spectrum*

IR: ***Infrared**, electromagnetic radiation*

Las opciones para monitorear una red inalámbrica WIFI son:

1. **Por medio de computadores / PC:** Es evidente que esta solución es la más económica tanto si se usan computadores "dedicados" como si se usan computadores ya existentes de usuarios. La desventaja es que es la menos eficiente y generalmente sólo resulta útil para PYMES.

2. **Por medio de Puntos de Accesos:** Esta metodología es mejor que la de los computadores pero también tiene sus limitaciones pues sólo se podrá monitorear el área cubierta por el Punto de Acceso y, además, si se lanza un ataque de Denegación de Servicio (DoS) sobre ese Punto de Acceso, se perderán las 2 funciones: la de conexión y la de monitoreo.

3. **Por medio de Sensores:** Este es el método más fiable, pero por supuesto el más costoso y también requiere mayores tiempos de instalación.

De todos modos, cualquiera sea el sistema que se elija para monitorear el espacio de RF, estas son las opciones para recolectar información en tiempo real sobre lo que está sucediendo en cada rincón de nuestra red WIFI.

1.11 ESTRUCTURA TCP / IP

Al igual que en el modelo OSI, TCP/IP está modelado en capas. Dichas capas, los protocolos que emplea y su correspondencia con las capas del modelo OSI se aprecian en la Figura 5.

Figura 5. Capas TCP/IP, protocolos TCP/IP y correspondencia con las capas OSI

Las capas física y de acceso a la red proporcionan la interacción entre el sistema final y la red, mientras que las capas de aplicación y transporte albergan los protocolos denominados "extremo a extremo", ya que facilitan la interacción entre los dos sistemas finales. En la capa Internet, los sistemas origen y destino proporcionan a la red la información necesaria para realizar el encaminamiento de la información, pero a la vez, deben proporcionar algunas funciones adicionales de intercambio entre los dos sistemas finales.

1.12 SEGURIDAD EN REDES

En la actualidad el uso de redes inalámbricas se ha extendido por sus ventajas de movilidad, flexibilidad y productividad.

Sin embargo, junto con su funcionalidad y demás ventajas, este tipo de implementaciones trae consigo importantes riesgos de seguridad que afrontar, en su mayoría asociados a la inexistencia de delimitación física de forma clara, y otros más importantes asociados a la carencia de mecanismos de seguridad suficientemente fuertes que protejan el acceso a los recursos tecnológicos y a la información.

A medida de la evolución de esta tecnología se han propuesto varias recomendaciones para dotar de un nivel de seguridad adecuado, actualmente se están desarrollando propuestas más concretas de mecanismos que permiten mejorar este nivel.

Entre las soluciones de seguridad más eficientes para el control de acceso a los recursos y la protección de la información en redes inalámbricas, se describe una de las más eficientes, la cual se basa en el uso de autenticación para el acceso a la red y en el uso del encriptado en las comunicaciones sobre este tipo de redes, por ello debemos empezar por el conocimiento del control de acceso a las redes inalámbricas.

1.12.1. CONTROL DE ACCESO

El control de acceso, en sistemas de información, es la capacidad de controlar la interacción de un elemento activo (usuario, dispositivo, servicio) con un recurso informático (red de datos, sistema, servicio).

Adicionalmente, el control de acceso implica procedimientos de identificación, autenticación y autorización para permitir o denegar el uso de los recursos así como para llevar un registro de este.

1.12.2. IDENTIFICACIÓN

La identificación es el procedimiento mediante el cual un elemento presenta su identidad a otro componente. Generalmente la identificación puede estar dada por un nombre de usuario, número de identificación o número de cuenta. Este parámetro no solo permite realizar la identificación, si no que habilita al sistema a relacionar la

identidad con el uso de los recursos, donde dicho individuo es responsable de sus acciones.

1.12.3. AUTENTICACIÓN

Es el proceso de validar la identidad de quien accede o provee un servicio, mediante la verificación de ciertas credenciales o parámetros que debe proveer la entidad que se autentica. Entre los métodos más comunes de autenticación se encuentra el uso de una contraseña o clave personal, sin embargo cada vez es más requerido el uso de otros factores de autenticación como *tokens* o Biometría. A nivel de enlace de datos, y de acuerdo al método y características de seguridad, existen diversos tipos de autenticación entre los cuales podemos citar:

PAP (*PASSWORD AUTHENTICATION PROTOCOL*): Este protocolo realiza la validación cuando se establece la conexión entre el cliente y el servidor. Utiliza el nombre de usuario y contraseña como credenciales, las cuales son enviadas en texto plano sobre el enlace, por lo que se considera un método poco seguro.

CHAP (*CHALLENGE HANDSHAKE PROTOCOL*): Provee un mejor nivel de seguridad, ya que realiza una validación de tres vías entre cliente y servidor, donde este último envía un parámetro de control a quien se autentica, este lo encripta con su contraseña y lo reenvía al servidor, donde se realiza el mismo procedimiento con la contraseña almacenada y se verifica si se obtiene el mismo resultado.

EAP (*EXTENSIBLE AUTHENTICATION PROTOCOL*): Es un protocolo que permite elevar aún más el nivel de seguridad de la autenticación, permitiendo diversos métodos autenticación y tipos de credenciales a utilizar (incluyendo la capacidad de manejar certificados digitales). De acuerdo a esto, diversos tipos de EAP se pueden implementar conforme a las características y condiciones propias de cada infraestructura donde se la requiera.

1.12.4. AUTORIZACIÓN

Establece lo que un usuario puede o no hacer una vez haya sido identificado y autenticado.

1.13 ENCRIPTADO

El encriptado en sistemas de información, es el proceso mediante el cual, utilizando una llave o un valor de control, un mensaje (generalmente datos en texto plano) es codificado para evitar que su contenido sea accedido y/o entendido por personal no autorizado. Para poder acceder al mensaje cifrado es necesario desencriptar el mensaje, proceso mediante el cual, utilizando la llave indicada, se recupera la información del mensaje en su estado original. Existen 2 tipos de encriptación:

- **Encriptado simétrico**: Es el proceso de cifrado de datos, en el cual se realiza el encriptado y desencriptado utilizando la misma llave. La encriptación simétrica es un procedimiento rápido, que provee mecanismos para asegurar la confidencialidad e integridad de la información que protege. En la figura 6 se muestra en esquema de encriptado simétrico.

Por otro lado el hecho de utilizar la misma clave en los procesos mencionados implica realizar una distribución segura de llaves por vías alternas a la que se quiere proteger. Por lo anterior también es recomendado utilizar la llave la menor cantidad de veces posible, idealmente una sola vez. Algunos de los estándares de encriptación simétrica más conocidos son:

- DES (*Data Encription Standard*).

- Triple DES y AES (*Advanced Encription Standard*).

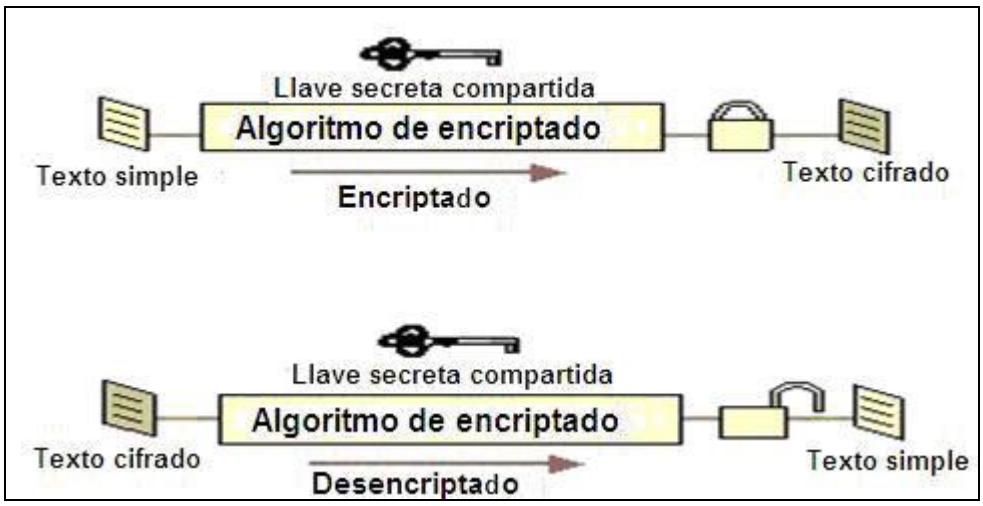

Figura 6 Encriptado Simétrico.

- **Encriptado Asimétrico**: Es el proceso de cifrado de datos, en el cual se utiliza llaves diferentes para la encriptado y desencriptado, una de estas de carácter privado o secreto y la otra es de acceso público (dentro de un sistema).

También se le conoce como encriptación de clave pública y se dice que se implementa bajo una infraestructura de clave pública. Este tipo de encriptación fue desarrollado a finales de los años 70's y adicionó nuevas funcionalidades a los mecanismos de encriptación como la posibilidad de realizar autenticación fuerte, no repudio, y el hecho de mejorar y facilitar los esquemas de confidencialidad e integridad (ver figura 7).

Algunos de los estándares de encriptación asimétrica más conocidos son:

RSA (Rivest, Shamir & Addleman), Diffie- Hellman y El Gamal.

Figura 7: Encriptación asimétrica.

1.14 MODELOS DE ADMINISTRACIÓN DE RED

Es la estandarización del empleo de una variedad de herramientas de red, aplicaciones y dispositivos para la administración de red. Para permitir que los componentes (de distintos fabricantes o proveedores) que conforman una red, y los sistemas operativos de los *hosts* puedan interoperar con el Sistema de Administración de Red.

Para la Administración de Red existen tres modelos fundamentales:

- Administración de Red OSI
- Administración Internet.
- Arquitectura TMN (*Telecommunications Management Network*).

Administración de Red OSI: Definido por ISO, con el objetivo de lograr la administración de los recursos según el modelo de referencia OSI.

Administración Internet: Definido por la Fuerza de Tareas de Ingeniería de Internet IETF (*Internet Enginnering Task Force*) y la IAB (*Internet Activities Board*), para administrar según la arquitectura de red TCP/IP.

Arquitectura TMN (Red de Administración de Telecomunicaciones): Definida por la ITU-T (Unión Internacional de Telecomunicaciones). Más que un modelo de red, define una estructura de red basada en los modelos anteriores.

Los modelos OSI e Internet se refieren a redes de *hosts*, mientras que el modelo TMN es de utilidad para los grandes operadores de redes de telecomunicaciones.

1.14.1. MODELO DE ADMINISTRACIÓN INTERNET

El Modelo de Administración Internet depende de la existencia en cada dispositivo de Agentes SNMP, que principalmente se encargan de la recolección de la información sobre dicho dispositivo, ésta información se puede dividir en tres tipos:

- Información de estado
- Advertencias
- Alarmas.

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

Para la gestión en Internet, el protocolo SNMP trabaja con otros componentes que cooperan con éste. Así, en el nivel superior, en la gestión se tiene:

- Estructura de Información de Gestión (SMI, *Structure of Management Information*), y

- Base de Información de Gestión (MIB, *Management Information Base*).

- SNMP utiliza los servicios ofrecidos por estos dos componentes para realizar su trabajo componentes del modelo de Administración de Internet.

1.15. ESTRUCTURA E IDENTIFICACION DE LA INFORMACION DE GESTION SMI (*STRUCTURE AND IDENTIFICATION OF MANAGEMENT INFORMATION*).

El SMI define las reglas para describir los objetos gestionados y cómo los protocolos sometidos a la gestión pueden acceder a ellos. La descripción de los objetos gestionados se hace utilizando ASN.1 (*Abstract Syntax Notation 1*, estándar ISO 8824), que es un lenguaje de descripción de datos.

1.15.1. BASE DE INFORMACION DE GESTION (MIB)

Una MIB define un modelo conceptual de la información requerida para tomar decisiones de administración de red. La información que la MIB incluye tiene número de paquetes transmitidos, número de conexiones intentadas, datos de contabilidad, entre otros.

1.15.2. ESPECIFICACIONES DE LA MIB

La MIB define tanto los objetos de la red operados por el protocolo de administración de red, como las operaciones que pueden aplicarse a cada objeto La MIB no incluye información de administración para aplicaciones como Telnet, FTP o

SMTP, debido a los inconvenientes que se presentan al instrumentar aplicaciones de este tipo para la MIB por parte de las compañías fabricantes. Para definir una variable u objeto MIB es necesario especificar lo siguiente:

Sintaxis: Especifica el tipo de datos de la variable, un valor entero, etc.

Acceso: Especifica el tipo de permiso como: Leer, leer y escribir, escribir, no accesible.
Estado: Define si la variable es obligatoria u opcional.

Descripción: Describe textualmente a la variable.

1.15.3. GRUPOS DE LA MIB

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

Grupo de Sistemas

Usado para registrar información del sistema, por ejemplo:

- Compañía fabricante del sistema.
- Tipo de Software.
- Tiempo que el sistema ha estado operando.

Grupo de Interfaces

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

Grupo IP

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

Grupo TCP

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

Grupo de ICMP y UDP

Lo mismo que el grupo IP y TCP.

Grupo EGP

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

Base de Información de Gestión II (MIB-II)

La MIB-II se crea para extender los datos de administración de red empleados en redes Ethernet y WAN (*Wide Area Network*) usando enrutadores para un enfoque a múltiples medios de administración en redes LAN y WAN. Se agregan dos grupos:

Grupo de Transmisión

Soporta múltiples tipos de medios de transmisión, como cable coaxial, cable UTP, cable de fibra óptica y sistemas T1/E1.

Grupo SNMP

Incluye estadísticas sobre tráfico de red SNMP.

CAPITULO II

2. SOFTWARE LIBRE.

2.1 GNU/LINUX, SISTEMA OPERATIVO DE REDES

GNU/LINUX se ha desarrollado según las normas POSIX (*Portable Operating System Interface*) y en base al sistema UNIX; es capaz de ejecutar aplicaciones en modo gráfico, aplicaciones TCP/IP, edición de texto, transferencia de archivos entre sistemas Unix, software de correo, etc.

Cabe mencionar que el sistema gráfico de GNU/LINUX no es tan potente como el de texto pero puede ofrecer un ambiente más simple y cómodo para el usuario. GNU/LINUX es un sistema operativo compatible UNIX. Se caracteriza porque es libre lo que implica que no hay que pagar ningún tipo de licencia para su uso, y es un sistema abierto, lo que significa que su código es público. El sistema está conformado por el núcleo o kernel y una serie de programas y bibliotecas que hacen posible su utilización. GNU/LINUX y gran parte de sus aplicaciones, bibliotecas y programas son distribuidos bajo la licencia GPL (Licencia Pública GNU).

El Software Libre proporciona la libertad de:

1.- Ejecutar el programa, para cualquier propósito;
2.- Estudiar el funcionamiento del programa, y adaptarlo a sus necesidades;
3.- Redistribuir copias;
4.- Mejorar el programa y poner sus mejoras a disposición del público, para beneficio de toda la comunidad. Como consecuencia de estas 4 libertades, el Software Libre

ofrece la libertad de aprender, libertad de enseñar, libertad de competir, libertad de expresión y libertad de elección.

***OpenSource*:** El término "*Open Source*" se refiere a tener acceso al código fuente. Pero el acceso al código fuente es apenas un pre-requisito para dos de las cuatro libertades que definen al Software Libre. Muchas personas no entienden que el acceso al código fuente no es suficiente. "Software Libre" evita caer en esa confusión. **UNIX-Like** UNIX es un sistema operativo desarrollado por Bell Labs de AT&T en el 1969. Aunque el termino UNIX se utiliza liberalmente al discutir éstos sistemas operativos, y GNU/Linux es uno de ellos, no todos los sistemas operativos parecido a UNIX son considerados UNIX Like. UNIX es una marca registrada del Open Group, y sólo los sistemas operativos que pasan completamente su prueba pueden ser etiquetados y certificados UNIX (Solaris de Sun Microsystems, es UNIX). Linux es UNIX-Like en su funcionamiento y en su estructura, pero no contiene código del AT&T UNIX.

2.2 HISTORIA DE LINUX

En 1991, Linus Benedict Torvalds, estudiante de la Universidad Helsinki, estrenó la primera versión pública de su sistema operativo Linux, la 0.02. Desde entonces, millones de usuarios de todo el mundo poseen éste sistema gratuito y miles de ellos contribuyen a su continuo desarrollo aportando ideas, programas, información sobre fallos del sistema ya sea en hardware/software, ayuda, tutoriales, etc.

Linux nació de la idea de crear un sistema clon de UNIX basado en GNU (*General Public License*, Licencia General Pública) y el código fuente disponible gratuitamente. Esta idea nació en 1991 cuando Linus Torvalds estudiaba la carrera de Ciencias Informáticas. Torvalds se encontraba especialmente interesado en Minix, el

único sistema UNIX disponible en aquél entonces de fácil acceso para los estudiantes y profesores.

Este sistema gratuito fue creado por Andrew Tanenbaum con el propósito de facilitar a los alumnos de la universidad el estudio y diseño de sistemas operativos. Minix era un UNIX más, tanto en apariencia como en el kernel (núcleo del sistema operativo), pero distaba mucho de ser comparable a uno de los grandes. Es a partir de aquel momento que Torvalds decidió crear un sistema que excediera los estándares de Minix, poniendo en marcha el proyecto personal Linux.

Torvalds tomó sus primeras clases de C y UNIX en 1990 y en poco tiempo empezó a utilizar el sistema operativo Minix en su nuevo 386. Linux evolucionó desde el simple programa "Hola, Mundo" a una terminal.

Durante mucho tiempo Torvalds trabajó en la soledad de sus ideas, hasta la mañana del 3 de julio de 1991 cuando pidió ayuda a través del Internet. Al principio fueron unos pocos los que le apoyaron, pero al poco tiempo muchos otros cibernautas se unieron al proyecto. En uno de los primeros emails enviados por Torvalds a la comunidad del ciberespacio respecto a Linux, informaba sobre su proyecto como si fuera un hobby, nada tan grande ni comparable con GNU.

Durante el desarrollo Torvalds se encontró con muchos problemas a lo largo de la programación del kernel. Pero Linux empezó a disponer de controladores para los dispositivos internos de la PC y un funcionamiento correcto del disco aproximadamente el 3 de julio, unas horas después de enviar su primer email informado sobre su proyecto. Dos meses más tarde Linux empezaba a funcionar y el código fuente de la primera versión 0.01 ya estaba disponible.

Muy pronto Linux se convirtió en un sistema mucho más fácil de instalar y configurar, y empezó a coger fama en todo el mundo. Al tener en muy poco tiempo miles de usuarios, las nuevas versiones de Linux salían casi semanalmente.

Linux había nacido para ser un sistema operativo del tipo POSIX (sistema variante de UNIX), totalmente gratuito para el usuario y con libre acceso al código fuente. Estas tres ideas fueron las que lo han convertido en el sistema con mejor rendimiento, más fiable, veloz y con más desarrolladores del mundo. En poco tiempo se ha colocado cerca de los grandes sistemas operativos como UNIX en el ámbito de servidores de comunicaciones, especialmente utilizado en empresas proveedoras de acceso a Internet.

Las versiones más recientes de Linux ofrecen la posibilidad de convertir nuestro ordenador personal en una potente estación de trabajo. Puede funcionar como estación de trabajo personal dándonos la posibilidad de acceder a las prestaciones que ofrece UNIX y cualquier otro sistema operativo. Además, gracias al aporte de muchas empresas hoy en día cuenta con potentes entornos gráficos que ayudan significativamente a elegir Linux. Puede además configurar para funcionar como estación de desarrollo y/o aprendizaje, proveer acceso a Intranets e Internet y muchas otras opciones.

GNU/Linux como estación de desarrollo y/o aprendizaje es uno de los mejores sistemas ya que dispone de muchos lenguajes de programación gratuitos como: GNU C, GNU C++, GNU Fortran 77, ADA, Pascal, TCL/Tk, etc. y muy pronto tal vez las versiones conocidas de Delphi para Linux de Borland Inc. las cuales esperemos que también sean de fácil acceso por los usuarios o en todo caso a un costo razonable que permita contar con esta valiosa

2.3 CARACTERÍSTICAS DEL SISTEMA OPERATIVO LINUX.

El sistema operativo LINUX fue desarrollado buscando la portabilidad de las fuentes: casi todo el software gratuito desarrollado para UNIX se compila en LINUX sin problemas. Y todo lo que se hace para LINUX (código del núcleo, controladores, librerías y programas de usuario) es de libre distribución.

LINUX implementa todo lo necesario para trabajar en red con TCP/IP. Desde controladores para las tarjetas de red más populares hasta SLIP/PPP, que permiten acceder a una red TCP/IP por puerto serial. También se implementan PLIP (para comunicarse por el puerto de la impresora) y NFS (para acceso remoto a archivos). Y también soporta los clientes de TCP/IP, como FTP, Telnet, y SMTP. Entre las características tenemos:

2.3.1. MULTITAREA

La palabra multitarea describe la capacidad de ejecutar muchos programas al mismo tiempo sin detener la ejecución de cada aplicación. Se le denomina **multitarea prioritaria o preventiva** ya que posibilita la ejecución simultánea de varios programas, siempre que las características del *host* lo permitan, es decir, cada programa tiene garantizada la oportunidad de ejecutarse, y se ejecuta hasta que el sistema operativo da prioridad a otro programa para su ejecución. Así, los programas se ejecutan hasta que permiten voluntariamente que otros programas también lo hagan.

El microprocesador sólo es capaz de hacer una tarea a la vez, pero las realiza en tiempos tan cortos que se escapan a nuestra comprensión, es por eso que en los momentos que no esté trabajando para determinada tarea, se dedica a ejecutar otras que se le hayan pedido.

Es fácil ver las ventajas de disponer de multitarea prioritaria. Además de reducir el tiempo muerto (tiempo en el que no puede seguir trabajando en una aplicación porque un proceso aún no ha finalizado), da la flexibilidad de no tener que cerrar las ventanas de las aplicaciones antes de abrir y trabajar con otras.

2.3.2. MULTIUSUARIO

La idea de que varios usuarios pudieran acceder a las aplicaciones o la capacidad de proceso de un único *host* era una utopía hace relativamente pocos años. La capacidad de LINUX para asignar el tiempo de microprocesador simultáneamente a varias aplicaciones ha derivado en la posibilidad de ofrecer servicio a diversos usuarios a la vez, ejecutando cada uno de ellos una o más aplicaciones. La característica que más resalta de LINUX es que un grupo de personas puede trabajar con la misma aplicación al mismo tiempo, desde el mismo terminal o desde terminales distintos.

2.3.3. MULTIPLATAFORMA

Las plataformas de hardware en las que en un principio se puede utilizar LINUX son 386-,486, Pentium Pro, Pentium II/III/IV. También existen versiones para su utilización en otras plataformas, como Alpha, ARM, MIPS, PowerPC y SPARC.

2.3.4. CONVIVENCIA CON OTROS SISTEMAS OPERATIVOS

Pueden estar juntos pero no funcionar al mismo tiempo. Cada vez que arrancamos un *host*, podemos elegir cuál de ellos se debe cargar, y a partir de este

momento sólo podremos utilizar aplicaciones destinadas al Sistema Operativo que estamos ejecutando.

2.3.5. SOPORTE EN REDES

LINUX soporta la mayoría de los protocolos comunes de Internet, incluyendo correo electrónico, noticias, telnet, web, ftp, ntp, nfs, dns, snmp y muchos más. LINUX puede operar como cliente o servidor para todo lo nombrado y ha sido ampliamente usado y probado.

LINUX dispone de los dos principales protocolos de red para sistemas UNIX: TCP/IP y UUCP (*Unix to Unix Copy Protocol*).

Con LINUX, TCP/IP y una conexión a la red, puede comunicarse con usuarios y *hosts* por toda Internet mediante correo electrónico, noticias, transferencias de archivos con FTP y mucho más.

La mayoría de las redes TCP/IP usan Ethernet como tipo de red física de transporte. LINUX da soporte a muchas tarjetas de red Ethernet e interfaces para *hosts* personales, incluyendo adaptadores para hosts portátiles.

Dado que no todo el mundo tiene una conexión Ethernet, LINUX también proporciona el protocolo Internet sobre líneas Seriales SLIP (*Serial Line Internet Protocol),* el cual permite conectarse a Internet a través de un módem. Si un sistema LINUX dispone de conexión Ethernet y de módem, puede ser configurado como servidor de SLIP para otros usuarios.

El sistema proporciona la interfaz estándar de programación por "*sockets*", lo que virtualmente permite que cualquier programa que use TCP/IP pueda ser llevado a

LINUX. El servidor de modo gráfico de LINUX también soporta TCP/IP, permitiendo ver aplicaciones que están corriendo en otros sistemas sobre su pantalla.

UUCP (*Unix to Unix CoPy*) es un viejo mecanismo usado para transferir archivos, correo electrónico y noticias entre *hosts* UNIX. Clásicamente los *hosts* UUCP se conectan entre ellos mediante líneas telefónicas y módem, pero UUCP es capaz de funcionar también sobre una red TCP/IP.

2.4 CONCEPTOS BÁSICOS DE LINUX

Los conceptos fundamentales que se utilizan en el sistema operativo LINUX son los siguientes:

2.4.1. PROCESO

Es un algoritmo interpretado o compilado que está ejecutándose en un sistema y se encuentra residente en la memoria RAM. También es la representación de cualquier programa en ejecución el cual puede ser auditado, analizado, terminado, etc.

2.4.2. SERVICIO

Es un tipo de proceso que está a la escucha, es decir, no está haciendo nada a no ser que sea requerido, en cuyo caso atiende convenientemente la petición. Un servicio suele cargarse de forma permanente en memoria hasta que sea terminado o el Sistema Operativo lo cierre.

2.4.3. DEMONIO

Es un tipo especial de servicio que escucha a otros servicios o procesos. El demonio es un "programa que escucha a otro programa". Un ejemplo claro de esto sería XINETD (*extended Internet daemon*) en sistemas Unix, que se encarga de escuchar a los procesos o servicios que soliciten conexión de red, y atiende esas peticiones.

2.4.4. INTERFAZ DE USUARIO (SHELL)

Es un programa encargado de comunicar el entorno de aplicaciones con el *kernel* o núcleo del sistema. Un *shell* puede ser tanto una interfaz gráfica como intérprete de comandos.

Un *shell* interpreta y ejecuta instrucciones que le hemos proporcionado por medio de una línea de comandos (*prompt*). Es decir, el intérprete de comandos recibe lo que se escribe en la terminal (sinónimo de *shell* o interfaz) y lo convierte en instrucciones para el sistema operativo.

El *prompt* es una indicación que muestra el intérprete para anunciar que espera una orden del usuario. Cuando el usuario escribe una orden, el intérprete la ejecuta. En dicha orden, puede haber programas internos o externos: Los programas internos son aquellos que vienen incorporados en el propio intérprete, mientras que los externos son programas separados.

Hay muchas interfaces posibles como el sistema Windows, el cual permite ejecutar comandos usando periféricos como el ratón y el teclado.

2.4.5. INODO

Se puede definir como un descriptor de una entrada de un sistema de archivos o archivos. Todo archivo tiene asociado un único inodo. Un inodo también puede ser definido como una clave numérica para el acceso al sistema plano de archivos, donde cada punto es capaz de recibir o entregar información.

2.4.6 .SISTEMA DE ARCHIVOS (FILESYSTEM)

Es una colección de todos los archivos y directorios de un sistema organizados en una jerarquía en forma de árbol.

2.4.7. SISTEMA DE DIRECTORIOS

Los sistemas de archivos UNIX se caracterizan generalmente por tener una estructura jerárquica, dar tratamiento consistente a la información de los archivos y a la protección de ellos.

El primer sistema de directorios que se aplicó a LINUX en su momento cumplió con las necesidades básicas, pero se volvió restrictivo, ya que en los archivos, el nombre no podía superar los 14 caracteres y los 64 MB de espacio. Para resolver este problema surgió el primer sistema de archivos especialmente diseñado para LINUX, el ext2 (*extended filesystem*). En el desarrollo del sistema extendido (ext2) surgió un importante cambio en lo que respecta a sistemas de archivos, el sistema virtual de archivos (VFS, *virtual filesystem*) que existe entre el sistema real de archivos y el sistema operativo y sus servicios.

El logro del sistema virtual de archivos (VFS*),* es que a LINUX le permite montar una serie de sistemas de archivos diferentes y variados; es decir, todos los

detalles de los sistemas de archivos son tratados por programas de modo que parezcan lo mismo tanto para el *kernel* como para las demás aplicaciones que se ejecutan en el sistema, en términos prácticos, es un modo de unificar los sistemas de archivos para poder ser manipulados por LINUX de un modo uniforme.

a) Representación de dispositivos

Se debe conocer como se representa un dispositivo en LINUX. Aquí encontramos el directorio /dev, el cual contiene a los dispositivos del sistema.

b) Organización de los directorios

La distribución de los directorios es en forma de árbol (tabla 2), el cual comienza en el directorio "/", también conocido como "directorio raíz". Directamente por debajo de "/" hay algunos subdirectorios importantes.

Tabla 2. Organización de directorios

Bin	Archivos binarios de comandos esenciales.
Boot	Archivos estáticos de arranque.
Dev	Archivos de dispositivos (virtuales).
Etc	Archivos de configuraciones locales-globales
Home	Directorio donde se contienen las cuentas de usuarios
Lib	Bibliotecas compartidas
Media	Punto de montaje de dispositivos.
Proc	Sistema de archivos virtual.

Root	Directorio del administrador.
Sbin	Archivos binarios esenciales del sistema
Tmp	Archivos temporales
Usr	Segunda jerarquía mayor.
Var	Archivos de información (variables).

A continuación se describen cada uno de los diferentes tipos de directorios:

BIN Y SBIN

Los archivos localizados en estos directorios corresponden a archivos *ejecutables*; la diferencia es que dentro del directorio *sbin* estarán sólo los ejecutables por el administrador.

BOOT

Contiene todos los elementos necesarios para arrancar el sistema. Aquí se encuentra todo lo que se ejecutará antes de que el *kernel* ejecute */sbin/init*.

DEV

Los archivos (especiales) ubicados en este directorio representan los dispositivos a los que LINUX puede acceder y utilizar. Cabe mencionar que estos archivos realmente no existen, sino que son la vía de acceso a los dispositivos.

ETC

Los contenidos de éste directorio son muy importantes para el normal funcionamiento tanto de las aplicaciones como del los **demonios**. Aquí residen todos los archivos de configuración global ya sea de los **demonios** (programa que escucha a

otro programa), así como las configuraciones globales de aplicaciones utilizables por todos los usuarios. Bajo este directorio se encuentra también el archivo de contraseñas del sistema.

HOME

Bajo este directorio residen todas las cuentas de usuario. Cuentas que serán subdirectorios contenidos de la forma: /home/usuario.

LIB

En este directorio residen todas las bibliotecas compartidas requeridas por los comandos en el sistema raíz.

MEDIA

Este directorio es el punto de montaje para sistemas de archivos montados temporalmente. Este directorio no influye en el normal funcionamiento del sistema y puede contener puntos de montaje para dispositivos removibles y otros.

PROC

Corresponde a un sistema de archivos virtual muy peculiar, pues si bien pueden listarse archivos contenidos en dicho directorio, éstos realmente no existen. Cuando el sistema requiere información de alguno de los contenidos de éste directorio y el sistema virtual de archivos solicita inodos, a medida que los archivos se abren /proc crea dichos archivos con información del *kernel* del sistema.

ROOT

La ubicación de este directorio es arbitraria, bien puede residir bajo el directorio raíz o dentro del directorio de cuentas de usuario.

TMP

Este directorio contiene los archivos temporales del sistema, es un modo de utilizar memoria física para el procesamiento de algunos datos. La información contenida en /tmp no se debe considerar permanente. Este directorio está asociado al uso de la memoria RAM.

USR

Corresponde a la segunda jerarquía mayor de archivos del sistema. Suele contener información compartible, pero de sólo lectura. Suele contener directorios similares a los ubicados bajo el directorio raíz, tales como /bin, /sbin, /lib, /etc pero que contienen binarios o configuraciones no esenciales para el normal funcionamiento del sistema.

VAR

Contiene archivos de información variable, cuyo ejemplo son los archivos de registro, los cuales cambian constantemente. Otros archivos contenidos en este directorio son los correos entrantes, algunos archivos temporales, etc.

2.7 ADMINISTRACIÓN DE USUARIOS Y GRUPOS

2.7.1 .LA CUENTA ROOT

Los usuarios normales están restringidos comúnmente para que no puedan alterar los archivos de otro usuario en el sistema. Los permisos de los archivos en el sistema están preparados para que los usuarios normales no tengan permitido borrar o modificar archivos en directorios compartidos por todos los usuarios (como son /bin y /usr/bin).

Estas restricciones desaparecen para *root*. El usuario *root* puede leer, modificar o borrar cualquier archivo en el sistema, cambiar permisos y pertenencias en cualquier archivo, y ejecutar programas.

2.7.2. USUARIOS

Como se mencionó anteriormente, *root* es usuario especial que se distingue de los demás usuarios en los privilegios que tiene sobre el sistema. Este no tiene ninguna restricción sobre lo que puede hacer. Cuando se instala LINUX por primera vez la única cuenta que debe existir en el sistema es la del *root*. Debido al poder de este usuario, es peligroso utilizarlo habitualmente para tareas cotidianas que no necesiten privilegios especiales, ésta cuenta se debe dejar para las tareas de administración y mantenimiento del sistema.

2.7.3. GRUPOS

La utilidad de un grupo de usuarios es la de permitir una administración ordenada de permisos sobre un conjunto de archivos. Cada usuario debe tener al menos un grupo que es el principal, pero podemos agrupar en varios grupos a un mismo usuario. Estos serían grupos secundarios.

Cada usuario pertenece a uno o más grupos. La única importancia real de las relaciones de grupo es la perteneciente a los permisos de archivos, cada archivo tiene

un "grupo propietario" y un conjunto de permisos de grupo que define de qué forma pueden acceder al archivo los usuarios del grupo.

2.7.4. PERMISOS

LINUX, es multiusuario, por lo que, los permisos de los archivos están orientados a dicho sistema. Los permisos de cualquier archivo tienen tres partes: permisos del propietario, permisos del grupo y permisos para el resto de usuarios. Así, un archivo pertenece a un determinado propietario y a un determinado grupo y, dependiendo de los permisos que tenga asociado dicho archivo, se podrá tener o no acceso a él.

2.8 REDES DE DATOS EN LINUX

2.8.1. SERVICIOS SOBRE TCP/IP

Los servicios más frecuentes de TCP/IP para el usuario en la actualidad son la conexión remota a otros *hosts* (Telnet, SSH *Secure Shell*), la utilización de ficheros remotos (*Network File System* NFS) o su transferencia (*File Transfer Protocol* FTP, *HiperText Transfer Protocol*, HTTP).

Estos servicios se describen a continuación:

- **Transferencia de archivos**: el protocolo FTP permite obtener/enviar archivos de un *host* hacia otro. Para ello, el usuario debe tener una cuenta en el *host* remoto e identificarse a través de su nombre (*login*) y una palabra clave (*password*), o en *hosts* donde existen un repositorio de información en donde el usuario se conectará como anónimo (*anonymous*) para transferir estos archivos al *host* local.

Conexión (*login*) remota: el protocolo de terminal de red (Telnet) permite a un usuario conectarse a un *host* remotamente. El *host* local se utiliza como terminal del *host* remoto y todo es ejecutado sobre éste permaneciendo el *host* local invisible desde el punto de vista de la sesión. Este servicio en la actualidad se ha reemplazado por el SSH por razones de seguridad. En una conexión remota mediante Telnet, los mensajes circulan tal cual (texto plano), o sea, si alguien "observa" los mensajes en la red, es similar a mirar la pantalla del usuario. SSH codifica la información, mediante la cual, hace que los paquetes en la red sean ilegibles a un nodo extraño.

Sistemas de archivos en red NFS (*Network File Systems*): permite a un sistema acceder a los archivos sobre un sistema remoto en una forma más integrada que FTP. Los dispositivos de almacenamiento (o parte de ellos) son exportados hacia el sistema que desea acceder y éste los puede "ver" como si fueran dispositivos locales. Este protocolo permite a quien exporta poner las reglas y la formas de acceso, lo que (bien configurado) hace independiente del lugar donde se encuentre la información físicamente.

Ejecución remota: permite que un usuario ejecute un programa sobre otro *host*. Existen diferentes maneras de realizar esta ejecución: a través de un comando (*rsh*, ssh) o a través de sistemas con RPC (*Remote Procedure Call*) que permiten a un programa en un *host* local ejecutar una función de un programa sobre otro *host*.

- **Servidores de nombre (***name servers*): En grandes instalaciones existen un conjunto de datos que necesitan ser centralizados para mejorar su utilización, por ejemplo, nombre de usuarios, palabras claves, direcciones de red, etc. Todo ello facilita que un usuario disponga de una cuenta para todos los *hosts* de una organización. El DNS (*Domain Name System*) es otro servicio de nombres pero guarda relación entre el nombre del host y la identificación lógica de este (dirección IP).

Servidores de terminales gráficas (*network-oriented window systems***):** Permiten que un *host* pueda visualizar información gráfica sobre una pantalla que está conectado a otro *host*.

2.8.2. TCP/IP

TCP/IP son protocolos que permiten la comunicación entre *hosts*. IP es el principal protocolo de la capa de red. Es un protocolo que permite la entrega de paquetes (llamados datagramas IP), cuya característica principal es de ser un protocolo no orientado a conexión, debido a que cada uno de los paquetes puede seguir rutas distintas entre el origen y el destino, es no fiable porque los paquetes pueden perderse, dañarse o llegar retrasados.

TCP es un protocolo orientado a conexión, es decir, la comunicación se trata como un flujo de datos (*stream*). Para la operación de TCP es necesaria la sincronización del intercambio de señales de tres vías, y significa que antes de comunicarse entre dos dispositivos, deben llevar a cabo el proceso de sincronización para establecer una conexión virtual para cada sesión. Este proceso siempre lo inicia el cliente y para lo cual usa un puerto conocido del servicio que desea contactar.

El proceso ocurre así: primero el cliente inicia la sincronización enviando un paquete SYN para iniciar la conexión, en el siguiente paso el otro dispositivo recibe el paquete y responde con un acuse de recibo ACK, como último paso el dispositivo que inició la conversación responde con un ACK indicando que recibió el ACK enviado por el otro dispositivo y finaliza el proceso de conexión para esta sesión.

El protocolo UDP (*User Datagram Protocol***):** Es un protocolo no orientado a conexión (el *host* destino no debe necesariamente estar escuchando cuando un *host* establece comunicación con él). No proporciona mecanismos de control de flujo ni

recuperación de errores y tiene la ventaja de que ejerce una menor sobrecarga a la red que las conexiones TCP, pero la comunicación no es fiable.

Existe otro protocolo alternativo llamado ICMP (*Internet Control Message Protocol*). ICMP se utiliza para mensajes de error o control en la red. Por ejemplo, si uno intenta conectarse a un *host*, el *host* local puede recibir un mensaje ICMP indicando *"host unreachable*". ICMP también puede ser utilizado para extraer información sobre una red. ICMP es similar a UDP, ya que maneja datagramas, pero es más simple que UDP, ya que no posee identificación de puertos (los puertos son buzones donde se depositan los paquetes de datos y desde donde las aplicaciones servidoras leen dichos paquetes) en el encabezamiento del mensaje.

Existen otros protocolos dentro de TCP/IP como ARP (*Address Resolution Protocol* que utiliza mensajes de *brodcast* o difusión para determinar la dirección MAC correspondiente a una dirección de red particular (dirección IP). Y RARP *(Reverse Address Resolution Protocol)* que utiliza mensajes de tipo *broadcast* para determinar la dirección de red asociada con una dirección de hardware en particular.

Configuración de la interfaz de Red (NIC, *Network Interface Card***)**

Los dispositivos de red se configuran automáticamente cuando se inicializa el hardware correspondiente. Por ejemplo, el controlador de Ethernet configura las interfaces *eth*[0..*n*] secuencialmente cuando se localiza el hardware correspondiente.

A partir de este momento, se puede configurar la interfaz de red, lo cual implica dos pasos: asignar la dirección de red al dispositivo e inicializar los parámetros de red al sistema. El comando utilizado para ello es el *ifconfig* (*interface configure*). Un ejemplo será: ifconfig eth0 192.168.110.23 netmask 255.255.255.0 .

Lo cual indica configurar el dispositivo *eth0* con dirección IP 192.168.110.23 y máscara de red 255.255.255.0. El *up* indica que la interfaz pasará al estado activo (para desactivarla debería ejecutarse *ifconfig eth0 down*). El comando asume que si algunos valores no se indican, son configurados por defecto. En este caso, el *kernel* configurará este *host* como Tipo-C con la dirección IP 192.168.110.23 y la dirección de *broadcast* con 192.168.110.255.

Por ejemplo:
ifconfig eth0 192.168.110.23 *netmask* 255.255.255.0 up

2.8.3. CONFIGURACIÓN DEL SISTEMA DE RESOLUCIÓN DE NOMBRES

El siguiente paso es configurar el sistema de resolución de nombres que convierte nombres tales como *linuxero.com* en 192.168.110.23. El archivo /etc/resolv.conf es el utilizado para realizar esa tarea. Su formato es muy simple (una línea de texto por sentencia). Existen tres palabras clave para tal fin: *domain* (dominio local), *search* (lista de dominios alternativos) y *name server* (la dirección IP del DNS (*Domain Name Server).*

Un archivo importante es el /etc/*host*.conf, que permite configurar el comportamiento del sistema de resolución de nombres. Su importancia reside en indicar dónde se resuelve primero la dirección o el nombre de un nodo. Esta consulta puede ser realizada al servidor DNS o a tablas locales dentro del host actual *(/etc/hosts*).

Ésta configuración indica que primero se verifique el */etc/hosts* antes de solicitar una petición al DNS y también indica que retorne todas las direcciones válidas que se encuentren en /*etc/hosts*. Por lo cual, el archivo */etc/hosts* es donde se

colocan las direcciones locales o también sirve para acceder a nodos sin tener que consultar al DNS.

La consulta es mucho más rápida, pero tiene la desventaja de que si el nodo cambia, la dirección será incorrecta. En un sistema correctamente configurado, sólo deberán aparecer el nodo local y una entrada para la interfaz *loopback*. En referencia a la interfaz *loopback*, éste es un tipo especial de interfaz que permite realizar al nodo conexiones consigo misma (por ejemplo, para verificar que el subsistema de red funciona sin acceder a la red). Por defecto, la dirección IP 127.0.0.1 ha sido asignada específicamente al *loopback* (un comando telnet 127.0.0.1 conectará con el mismo *host*).

Para el nombre de un host pueden utilizarse alias, que significa que ese *host* puede llamarse de diferentes maneras para la misma dirección IP.

El orden de consulta de las bases de datos para obtener el IP del nodo o su nombre será primero el servicio de DNS (que utilizará el archivo */etc/resolv.conf* para determinar la IP del nodo DNS) y en caso de que no pueda obtenerlo, utilizará el de las bases de datos local (/*etc/hosts*).

CAPITULO III

3 TOPOLOGIA DE LAS REDES WIFI CANTV

Desde hace 5 años CANTV, se hizo acreedor de la licencia del software que lleva por nombre Tivoli Netcool/OMNIbus**,** con el fin de proveer de servicios de administración y monitoreo de las redes IP de la empresa, a través de una serie de aplicaciones que contiene Netcool. Este sistema está operando bajo el sistema operativo Solaris 2 debido a la estabilidad y gran gama de funcionamiento que le proporciona al gestionar las redes, este sistema también puede ser operado bajo otros sistemas operativos como Windows XP, Windows Vista y Linux en una versión que requiere de gran soporte y desarrollo.

Tivoli Netcool es un software diseñado bajo el sello de la IBM, una de sus funciones es ayudar a proveedores a dar servicios de administración inalámbrica, proveer de servicios de telecomunicaciones, cable e Internet, enfrentar los desafíos de telecomunicaciones actuales y brindar una solución a requerimientos futuros.

Sin embargo, en el momento de adquirir el software, la empresa se enfocó en las redes alámbricas y por ello no se hizo acreedor del módulo inalámbrico, por esta razón actualmente las redes WIFI se monitorean mediante una alarma que solo le proporciona la información acerca de los puntos de accesos que están o no están operando.

Por esta razón, hoy en día la empresa no posee un sistema que permita obtener mayor información acerca de las redes inalámbricas, sin embargo CANTV tiene 2 maneras de monitorear las alarmas de las redes WIFI:

Vía trap: Consiste en que los elementos de la red le envían directamente a Netcool la información mediante una alarma. (Por medidas de seguridad esta vía no está operativa).

Vía Master Controller: Consiste en que el controlador maestro (*master controller*) envía la información a Netcool de manera inmediata y con un código de seguridad más riguroso. Esta es la manera en la que actualmente se están monitoreando las redes WIFI en CANTV.

Hay que tomar en cuenta que Netcool, proporciona una amplia cobertura de los protocolos a utilizar, un descubrimiento automatizado que permite la visualización de la topología de la red tanto de manera cualitativa como cuantitativa. Unos de sus principales protocolos a utilizar es el SNMP. Su funcionamiento dependerá de la administración de todos los módulos que conforman el manejo de una red.

La gestión del rendimiento proporciona a los administradores de red analizar e informar todo lo que se relacione con el suministro de servicios de la empresa con respecto a los equipos que conforman la red NGN, que a través de la gestión de operaciones pueden detectar y corregir las tendencias que amenazan al suministro de servicios y por ende le permite dar el mantenimiento a equipos existentes en la topología de la red que provienen de diferentes fabricantes, tales como:

- N2000
- Nortel (MDM)
- Alcatel SDH
- Alcatel SAM
- Alcatel 5620
- Huawei T2000
- Huawei N2000 UMS
- Huawei N2000 BMS

Es decir, Netcool es un sistema que permite gestionar redes robustas y de alto rendimiento y su uso va destinado a proveedores de servicios de grandes empresas, como es el caso de CANTV que utiliza este sistema para gestionar todas las redes que proveen servicios de datos teniendo compatibilidad con los fabricantes de los equipos utilizados en la topología de las redes existentes en dicha empresa.

A continuación los componentes Tivoli Netcool/OMNIbus:

- **Servidores**: Por medidas de seguridad se utilizan dos servidores, uno es el llamado *Objectserver,* que es el principal y se encuentra en el CNT (Centro Nacional de Telecomunicaciones), y existe un servidor secundario que se utiliza en caso de presentarse una falla de operación en *el Objectserver*, el cual respalda toda la información del *Objectserver*. Este servidor secundario se encuentra en la central de los Palo Grandes (Centro de Operaciones de Red, COR). El *ObjectServer* es la base de datos, es decir, es la memoria en el núcleo del servidor de Tivoli Netcool / Omnibus.

- **Probes**: Su función es detectar y adquirir datos de eventos, y transmitir los datos al *ObjectServer* como eventos.

- **Gateway:** Permiten el intercambio de eventos entre *ObjectServer* y aplicaciones de terceros, tales como bases de datos servicios de asistencia. Permite integrar las distintas funciones de la empresa, por ejemplo; puede configurar una puerta de enlace para enviar la información del evento a un sistema de ayuda. También puede utilizar una puerta de entrada a los eventos de un archivo de la base de datos.

- **Herramientas de escritorios**: Integrada por herramientas gráficas utilizadas para ver y gestionar eventos.

- **Herramientas de administración**: Tivoli Netcool / Omnibus incluye herramientas que los administradores pueden utilizar para configurar y administrar el sistema, por ejemplo una interfaz SQL interactivo que permite la importación, exportación y control del proceso.

En la actualidad, la empresa CANTV monitorea y administra las redes WIFI a través de un sistema licenciando llamado Netcool, este sistema cuenta con aplicaciones gráficas en el módulo alámbrico, las cuales hacen que lleve de manera versátil el tráfico de datos. Este sistema solo manda alarmas de notificación de las redes inalámbricas cuando estas tienen algún problema.

La empresa no obtuvo la licencia para el monitoreo de las redes WIFI, debido a que en el momento de instalar dicho sistema no se tomaron en cuenta dichas redes, ya que estaban como un proyecto a largo plazo, es por ello que hoy en día no se obtiene ninguna información detallada de estas redes y es de gran necesidad un sistema que brinde información del tráfico de datos de estas redes inalámbricas.

Netcool gestiona las redes IP de manera que puede servir a su vez para monitorear tanto redes WIFI como redes LAN, característica de la cual se puede sacar ventaja en éste proyecto.

Por otro lado debemos de tener en cuenta que el proyecto de desarrollar otro sistema para monitoreo de redes WIFI viene dado debido al decreto 3390 de la Gaceta oficial Nº 38.095 de fecha 28/12/2004, el cual se refiere a realizar la migración de la empresa, del software licenciado al software de código abierto, de modo que actualmente la empresa está en proceso de cambio a esta nueva forma de compartir los conocimientos, mejor conocido como Linux. Cabe destacar que se requiere de diferentes sistemas en código abierto que permitan realizar el trabajo de monitoreo con nuevas aplicaciones para el que el trabajo sea eficiente y óptimo.

Es por ello que el sistema fue desarrollado bajo el código abierto con aplicaciones importantes y versátiles que son de gran ayuda a los operadores en el momento de implantarse totalmente el sistema de código abierto.

Netcool gestiona de manera sencilla las redes inalámbricas de CANTV debido a las razones ya expuestas, por ello hay que tomar en cuenta que una de las soluciones inmediatas es obtener el tráfico de datos a través de la instalación de un nuevo sistema de fácil gestión y que cumpla con los requerimientos de la empresa. Otra manera de solucionar esta carencia de información sería la instalación de Netcool bajo el sistema Linux el cual sería una solución a largo plazo debido al cambio de muchos equipos, configuración de nuevos servidores que tendrían que estar administrados por operadores con alto aprendizaje en el nuevo sistema operativo, es decir, este sistema seria versátil y delicado debido a los numerosas aplicaciones y funciones que tiene, tomando en cuenta que en software libre la manera de instalar, configurar y gestionar las redes es diferente a software licenciados ya que requiere de mayor conocimiento en el área de programación e informática.

Por esta razón, es más sencillo gestionar todas las redes con Netcool y buscar una solución nueva e inmediata para la administración y monitoreo del tráfico de datos de las redes WIFI.

Luego de conocer el sistema de administración y monitoreo de las redes IP de CANTV, también es momento de conocer la arquitectura y funcionamiento de las redes WIFI de la empresa las cuales son las que se necesitan conocer para tener en cuenta de qué manera se gestionarán.

Arquitectura:

Arquitectura de las redes WIFI de CANTV:

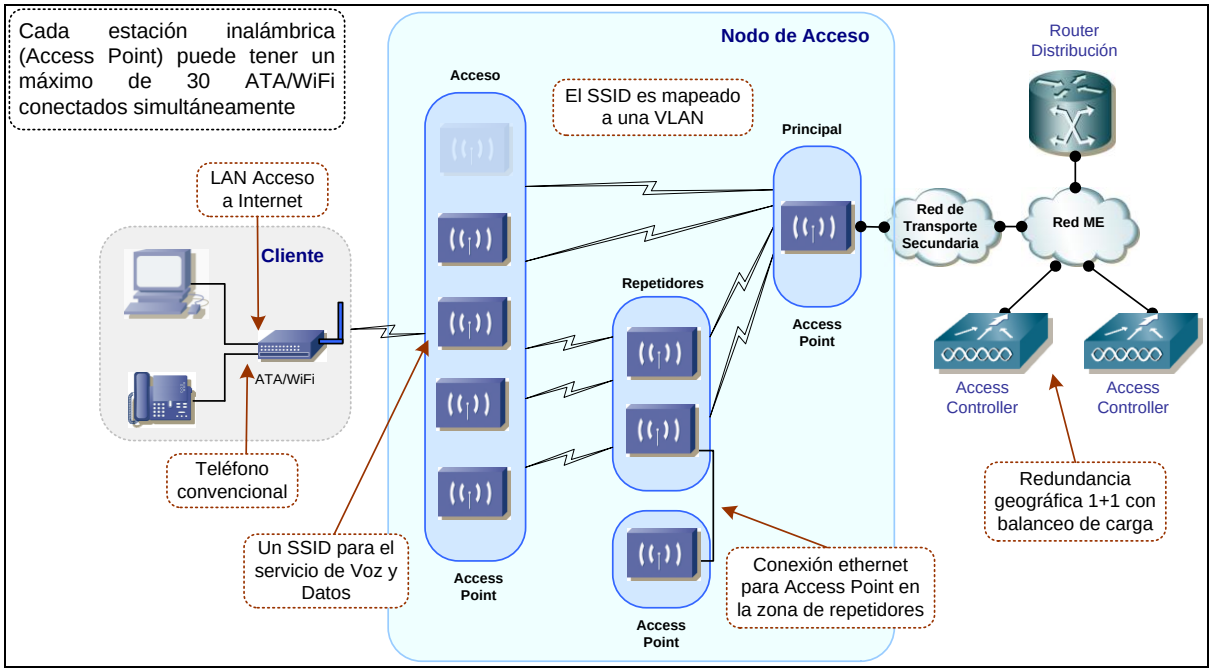

Figura 8. Arquitectura de las redes WIFI de CANTV[13]

La arquitectura presentada se desarrolla de la siguiente manera:

- Los "*Access Point*" proveerán conectividad inalámbrica WIFI a los "CPE ATA/WIFI"
- El nodo de acceso inalámbrico podrá estructurarse en puntos de acceso (*Access Point*), repetidor y principal.
- Los "CPE ATA/WIFI" dispondrán de puntos de acceso LAN para acceso a Internet y telefonía convencional en las premisas de los usuarios.
- Los "CPE ATA/WIFI" deben estar configurados en modo *routing*.

El "*Access Controller*" realizará las siguientes funciones principales:

- Actúa como puerta por defecto (*Default Gateway*) de los clientes.

- Concentra los túneles GRE originados de los “Puntos de Accesos”.
- La entrada de los clientes en su tabla ARP (agregando el servicio).
- Asocia el SSID para los servicios voz e Internet en una VLAN, transportando el servicio a través de la red ME al “*Router* de Distribución”.
- Actúa como cliente *Radius* para la autenticación de los usuarios.
- Maneja la lista negra para denegación de clientes. Administra la configuración de los “Puntos de Acceso”.
- DHCP relay.
- Maneja la calidad de servicio en los “*Access Controller*”. Se habilitará redundancia geográfica 1+1 con balanceo de carga.
- Los “Puntos de Acceso” podrán conectarse al “*Router* de Distribución” a través de una red de transporte secundaria (radios IP o enlaces satelitales) y/o la red ME.
- Los “*Access Controller*” estarán ubicados en nodos de Distribución de la Red Troncal IP
- La conectividad entre el “*Access Controller*” y el “*Route*r de Distribución” será a través de la Red ME.
- El “*Router* de Distribución” proveerá acceso a la Red Troncal IP e Internet, anunciando vía BGP las redes IP asignadas a los clientes.
- Los “Puntos de Acceso” se conectarán al “*Access Controller*” con túneles GRE por medio de la Red Troncal IP.

  Especificación de los *Access Controller*. Ver figura 9.

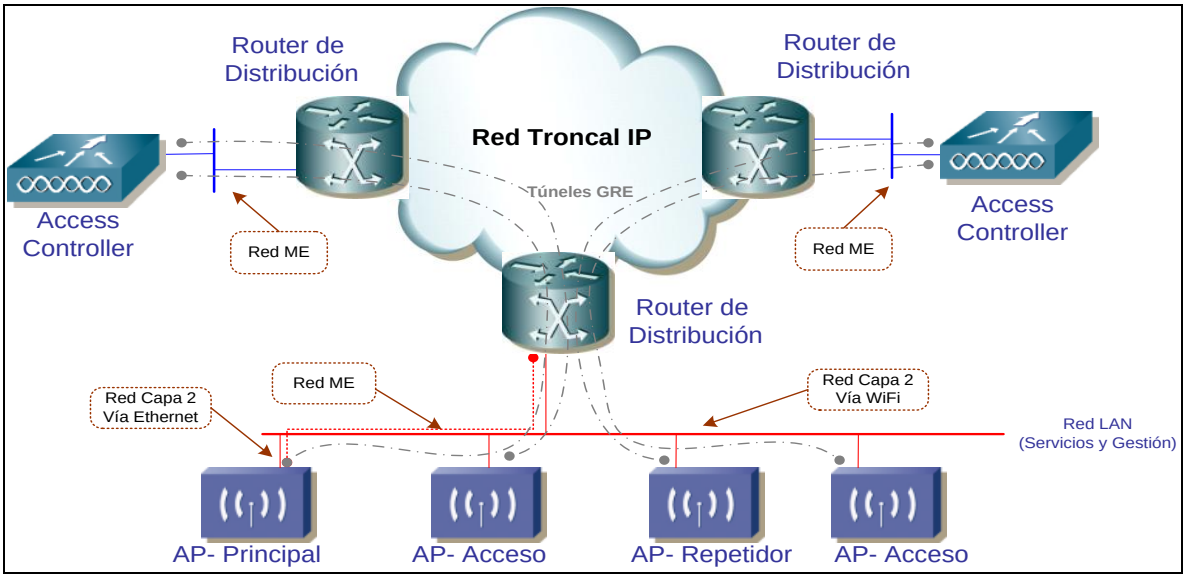

Figura 9. Especificación de los Access Controller [13]

- El "CPE ATA/WIFI" se asocia inalámbricamente al SSID de servicios del "*Access Point*".
- El "Access Point" valida la existencia de la dirección MAC del "CPE ATA/WIFI" en la lista negra del "*Access Controller*" (seguridad a nivel de capa 2).
- El "CPE ATA/WIFI" genera solicitud de dirección IP vía DHCP y el "*Access Controller*" retransmite la solicitud al servidor DHCP.

Autenticación de usuarios para el servicio de Internet: En la figura 10 se muestra el esquema general del proceso de autenticación de usuarios para el servicio de Internet.

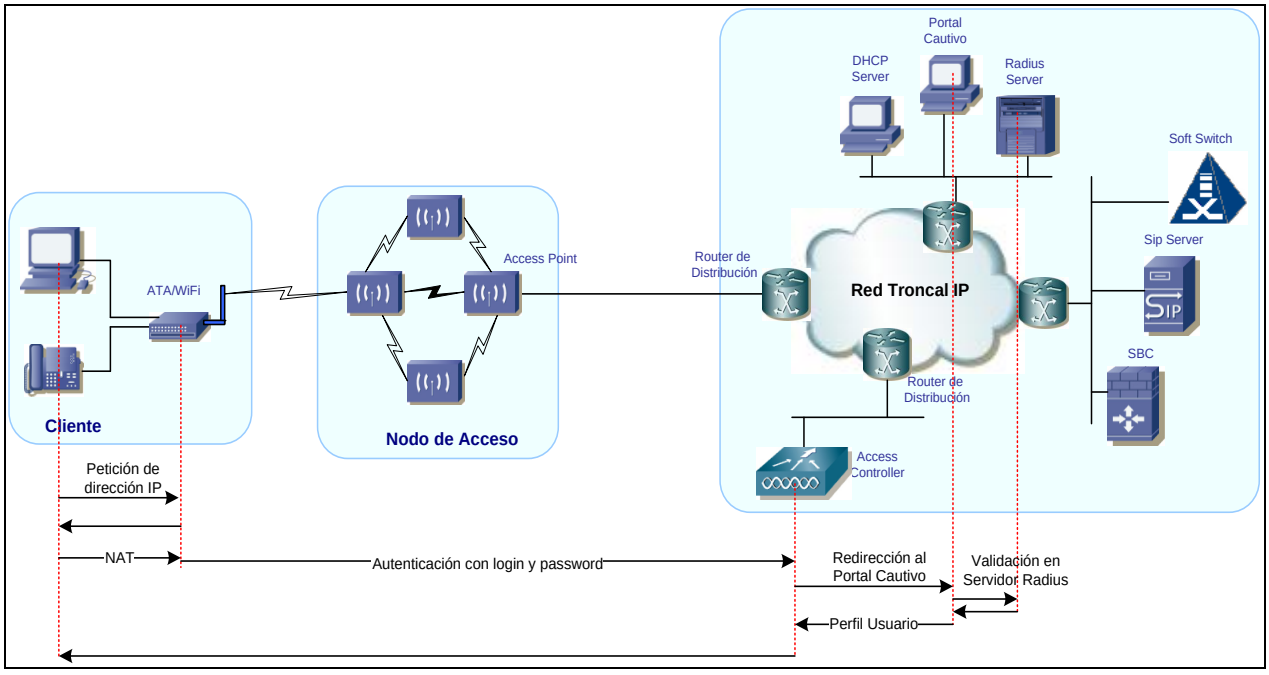

Figura 10. Autenticación de usuarios para el servicio de Internet [13]

- El computador del cliente genera petición de dirección IP vía DHCP, el "CPE ATA/WIFI" le asigna una dirección IP privada.
- Para proveer acceso a Internet, el "CPE ATA/WIFI" realiza NAT de la dirección IP del computador contra su dirección IP válida (recibida vía DHCP) .
- El "*Access Controller*" redirecciona la primera solicitud de acceso a Internet al Portal Cautivo, para que el usuario ingrese los datos de su cuenta.
- El servidor *Radius* establecerá y enviará el perfil de los usuarios para manejar su ancho de banda y manejo del tiempo de la sesión al "*Access Controller*".
- El portal para autenticación del cliente puede estar alojado en el "*Access Controller*" (aplicación web sencilla) o en un servidor destinado para ello (aplicación web con mayor cantidad de contenidos) .
- Luego que el computador este registrado, la solicitud de acceso a Internet llega al "*Access Controller*" y este lo redirecciona a la Red Troncal IP.

- El “CPE ATA/WIFI” solicita el registro de su número telefónico y contraseña al SBC y este lo redirecciona al Sip Server para el servicio de VoIP.
- Luego que el “CPE ATA/WIFI” está registrado, la solicitud de llamada llega al SBC y lo redirecciona al Sip Server, este la distribuirá internamente o a través de la red NGN.

Esquema de conectividad, diagrama físico: En la figura 11 se muestra un diagrama físico del esquema de conectividad WIFI.

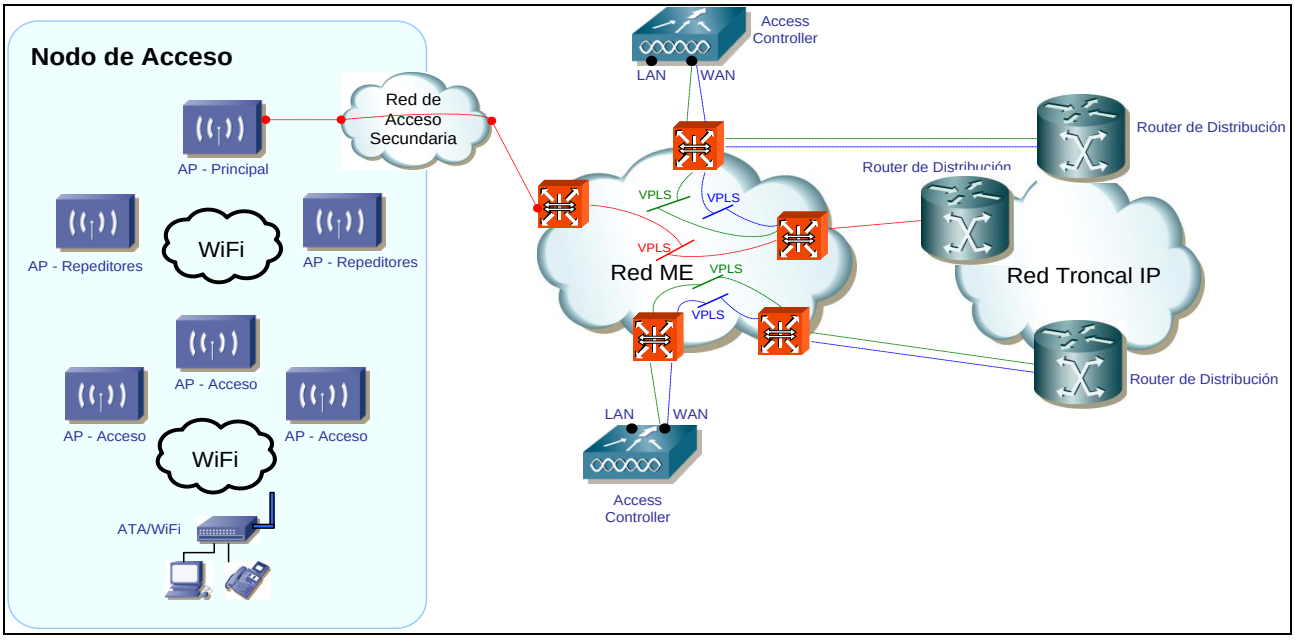

Figura 11. Esquema de conectividad WIFI. [13]

- Se debe generar un (01) servicio ME VPLS desde el “*Access Point* Principal” hasta el “*Router* de Distribución” para gestión y servicio de la red de acceso inalámbrica.
- Se debe utilizar la interfaz WAN del “*Access Controller*” para acceso a la Red Troncal IP y la interfaz LAN para gestión de la plataforma.
- Se debe generar un (01) servicio ME VPLS desde el “*Access Controller*” hasta el “*Router* de Distribución”, para concentración de túneles GRE y manejo de “*Access Point*”

- Se debe generar un (01) servicio ME VPLS desde el "*Access Controller*" hasta el "*Router* de Distribución" para acceso a Internet
- Configurar a 100 Mbps FullDuplex todas las conexiones Ethernet del "*Access Controller*" y los "*Access Point*"
- Se debe generar un túnel GRE desde cada "Access Point" hasta el "*Access Controller*".

A Continuación se muestra el esquema de conectividad, diagrama lógico: (Figura 12)

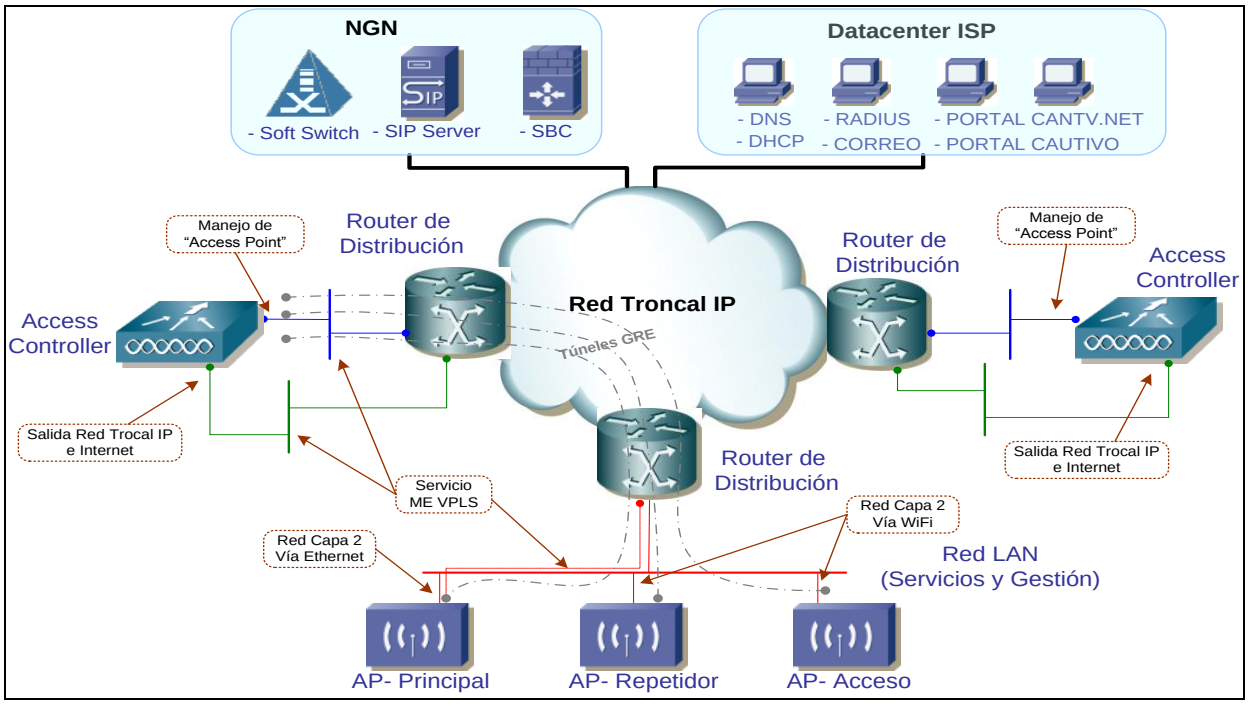

Figura 12. Esquema de conectividad WIFI. Diagrama Lógico [13]

- Se debe asignar (01) segmento IP privado equivalente a un CIDR "/27" por nodo de distribución, a ser aprovisionado en el "*Route*r de Distribución" y en los "Puntos de Accesos".

- Se debe asignar (02) segmentos IP privados equivalentes a un CIDR "/28" por nodo de distribución, a ser aprovisionado en el "*Router* de Distribución" y en el "*Access Controller*", para acceso a la Red Troncal IP y manejo de los "*Access Point".*
- Se debe asignar dos (01) segmento IP público equivalente a un CIDR "/22" por "*Access Controller*", a ser aprovisionado en el servicio DCHP de CANTV.NET y configurado en el "*Access Controller*", para direccionamiento IP de los "CPEATA/WIFI".
- Se debe aprovisionar (01) dirección IP privada de la Red DCN en el "*Access Controller*" para gestión de la plataforma.
- Cada "CPE ATA/WIFI" solicitará (01) dirección IP válida a la plataforma DHCP de CANTV.NET.
- Los "CPE ATA/WIFI" asignarán direcciones IP privadas a los computadores, vía DHCP local.

Diagrama lógico de la gestión del servicio. (Ver Figura 13)

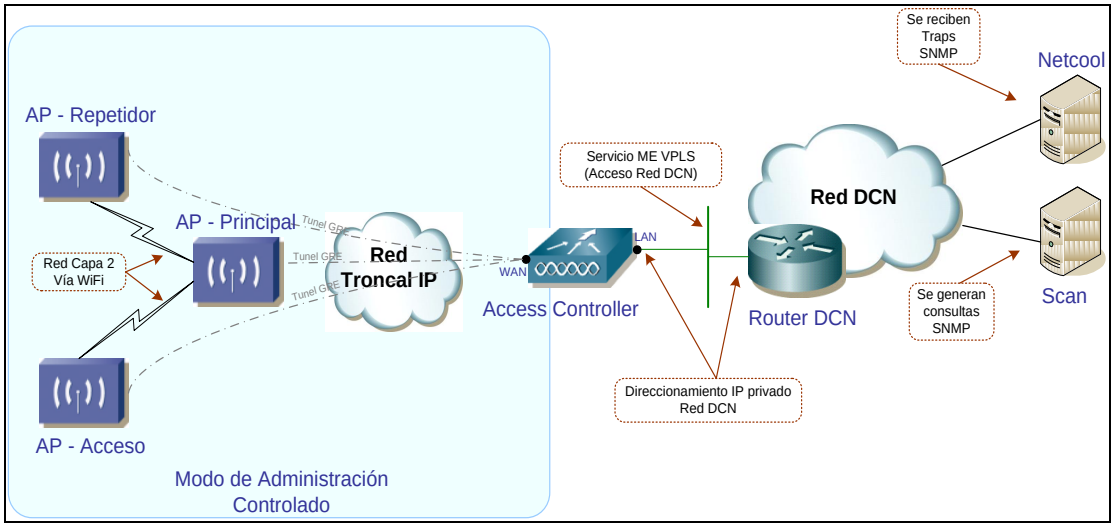

Figura 13. Diagrama lógico de la gestión del servicio.[13]

- Los "*Access Point*" serán administrados desde el "*Access Controller*", utilizando el modo de administración controlado (propietario del proveedor).
- El "*Access Controller*" será gestionado a través de la Red DCN vía Red ME.

El "*Access Controller*" se gestionará remotamente, utilizando los protocolos:

- HTPPS, para la administración vía *Web* mediante autenticación *Radius* (PAP) de Tacacs
- SNMP, para la recolección de variables de monitoreo desde SCAN y envío de alertas a NETCOOL.

Luego de conocer la topología de redes WIFI de CANTV y el funcionamiento de esta red pudimos notar la importancia del protocolo DHCP por ello haremos referencia de su funcionalidad para así poder tener de manera más clara su función.

DHCP se deriva de del protocolo *Bootstrap (BootP). BootP* fue de los primeros métodos para asignar de forma dinámica, direcciones IP a otros equipos (ordenadores, impresoras, etc.). Al ser las redes cada vez más grandes, *BootP* ya no era tan adecuado y DHCP fue creado para cubrir las nuevas demandas.

Como se ha comentado, se puede incluir información adicional en el protocolo DHCP. La configuración básica que puede ser enviada junto con la dirección IP es:

- Dirección IP y la máscara.
- Pasarela o Gateway para la máquina que quiere acceder a la red.
- Servidor DNS para que la estación de trabajo pueda resolver nombres a direcciones IP.

DHCP (*Dynamic Host Configuration Protocol*) es un conjunto de reglas para dar direcciones IP y opciones de configuración a ordenadores y estaciones de trabajo

en una red. Una dirección IP es un número que identifica de forma única a un ordenador en la red, ya sea en una red corporativa o en Internet. Una dirección IP es análoga a un número de teléfono.

La dirección IP puede ser asignada estáticamente (manualmente) por el administrador o asignada dinámicamente por un servidor central.

Funcionamiento de DHCP

DHCP funciona sobre un servidor central (servidor, estación de trabajo o incluso un PC) el cual asigna direcciones IP a otras máquinas de la red. Este protocolo puede entregar información IP en una LAN o entre varias VLAN. Esta tecnología reduce el trabajo de un administrador, que de otra manera tendría que visitar todos los ordenadores o estaciones de trabajo uno por uno. Para introducir la configuración IP consistente en IP, máscara, *Gateway*, DNS, etc.

Existen otros parámetros como servidores de registro o de sincronización.

Modos en DHCP

Existen 3 modos en DHCP para poder asignar direcciones IP a otros equipos:

- **Asignación manual:** El administrador configura manualmente las direcciones IP del cliente en el servidor DCHP. Cuando la estación de trabajo del cliente pide una dirección IP, el servidor mira la dirección MAC y procede a asignar la que configuró el administrador.

- **Asignación automática:** Al cliente DHCP (ordenador, impresora, etc.) se le asigna una dirección IP cuando contacta por primera vez con el DHCP Server. En este método la IP es asignada de forma aleatoria y no es configurada de antemano.

- **Asignación dinámica:** El servidor DHCP asigna una dirección IP a un cliente de forma temporal. Digamos que es entregada al cliente -Servidor que hace la petición por un espacio de tiempo. Cuando este tiempo acaba, la IP es revocada y la estación de trabajo ya no puede funcionar en la red hasta que no pida otra.

DHCP es un protocolo diseñado principalmente para ahorrar tiempo gestionando direcciones IP en una red grande. El servicio DHCP está activo en un servidor donde se centraliza la gestión de la direcciones IP de la red. Hoy en día, muchos sistemas operativos incluyen este servicio dada su importancia.

Luego de conocer las redes WIFI de CANTV nos podemos dar cuenta de la importancia de los protocolos y estándares utilizados en estas redes, ya que por medio de ellos nos vamos a regir para el monitoreo del tráfico de datos, tomando en cuenta algunas especificaciones técnicas de los equipos utilizados en la red inalámbrica de esta importante empresa de telecomunicaciones.

CAPITULO IV

4 SELECCIÓN DEL SISTEMA BASE PARA EL PROTOTIPO A DISEÑAR

Luego de conocer detalladamente el sistema de monitoreo que la empresa CANTV utiliza actualmente para sus redes WIFI, se pudo observar que solo se basa en alarmas que el sistema envía para avisar a sus operadores que algunos de los puntos de acceso no están operando. Sin embargo, se necesita mejorar la administración y monitoreo del tráfico de datos con la finalidad de permitir a la empresa tener un mayor alcance acerca de la información existente de sus redes.

Por otro lado, en la actualidad la empresa se encuentra en un tiempo de transformación, donde se destaca la migración hacia Software Libre, lo que tiene como objeto permitir la integración tecnológica debido a las bondades y ventajas que tiene un sistema operativo abierto como Linux para el desarrollo de cualquier sistema que la empresa CANTV necesite, y a su vez se pueda mejorar y amoldar a las necesidades de la compañía en el momento que sea necesario.

Por lo antes expuesto, surge la necesidad de desarrollar un sistema de administración y monitoreo de redes WIFI bajo el sistema operativo Linux, el cual pueda generar una o varias herramientas que permitan obtener la información a través de interfaces analíticas y gráficas que le permitan al administrador poseer varias vías de gestión de redes.

Luego tener claro el requerimiento de la Gerencia de Planificación con respecto a este trabajo de grado, el cual es desarrollar un sistema de administración y monitoreo de redes WIFI bajo el código abierto, se procedió a indagar e investigar

diferentes sistemas existentes en la red, los cuales pueden cumplir con los parámetros expresados por la empresa y que sean compatibles con los equipos a ser gestionados.

Después de investigar diferentes sistemas, se tomaron en cuenta principalmente tres sistemas para su estudio y evaluación al detalle para luego tomar una decisión y elegir el que sea más versátil y se ajuste mejor a nuestras necesidades. Entre los sistemas estudiados tenemos:

JFFNMS

JFFNMS (*Just For Fun Network Management System*), es un sistema de gestión y monitorización de red, diseñado para gestionar una red IP basado en el lenguaje de programación PHP, que se encuentra en constante desarrollo. Es desarrollado en software libre y esta bajo licencia GPL. Permite monitorear mediante distintos protocolos tales como SNMP, Syslog y Tacacs+, cuyo uso responde a características de manejo de dispositivos Cisco. La consola de eventos se puede abrir desde cualquier Navegador Web de Windows Xp, 2000 o Linux y muestra todos los tipos de eventos de manera ordenada.

NAGIOS.

Es un sistema de código abierto (*open source*) popular para monitorear una red. Monitorea los *hosts* y servicios que se especifiquen, alertando cuando algo sale mal y nuevamente cuando vuelve al estado correcto. Originalmente tuvo el nombre de Netsaint, fue creado y es mantenido actualmente por **Ethan Galstad**, junto con un grupo de desarrolladores de software que mantienen también varios *plugins*. Nagios fue diseñado originalmente para ser ejecutado en ambiente Linux, pero también se ejecuta bien en variantes de Unix. Nagios está licenciado bajo la GNU (*General Public License*) Version 2, publicada por la *Free Software Fundation*.

CACTI

Es una solución completa de graficado en red, diseñada para aprovechar el poder de almacenamiento y la funcionalidad de graficar que poseen las RRDtool. Esta herramienta desarrollada en PHP, provee un poder ágil, plantillas de gráficos avanzadas, múltiples métodos para la recopilación de datos, y manejo de usuarios. Tiene una interfaz de usuario fácil de usar, que resulta conveniente para las instalaciones del tamaño de una LAN, así también como para las redes complejas que poseen cientos de dispositivos.

Tiene además una herramienta para sondear, almacenar y presentar estadísticas de red y sistemas, está diseñada al rededor de *RRDTool*, con especial énfasis en la interfaz gráfica y casi todas las funcionalidades pueden configurarse a través de la web.

4.1 COMPARACIÓN DE SISTEMAS DE GESTIÓN DE REDES

Luego de haberse evaluado y comparado entre los diferentes sistemas de distintos fabricantes y las diferentes filosofías de cada uno, lo cual fue una labor bastante subjetiva, ahora bien, decidir cuál es el más idóneo, cuál es que mejor se adapta a los requerimientos de CANTV o cual es tecnológicamente más adecuado, puede tener muchos matices y muchas opiniones. Por esta razón para realizar este análisis, se ha decidido utilizar una metodología que permita evaluar dentro de unos parámetros bien definidos y de una manera objetiva, cuáles son las debilidades y fortalezas de los productos que participaran en este proceso.

Para este estudio se ha tomado como referencia un estudio realizado en un trabajo de grado desarrollado en el Centro Nacional de Tecnologías de Información (CNTI), el cual consta de una matriz de comparación donde se le coloca una puntuación estimada de cada producto [11]. En dicha matriz se colocan los aspectos

funcionales evaluados y se les asigna un peso sobre la totalidad de la puntuación. Cada una de estas áreas se representará en un renglón que tendrá una calificación entre 1 y 5 (véase Tabla 3).

Tabla 3: Comparación de los sistemas

	JFFNMS	**NAGIOS**	**CACTI**
Control de Fallas	5	4	4
Desempeño	5	5	4
Reportes	5	4	4
Configuración	3	3	3
Plataforma	5	4	3
Documentación	2	3	4
Instalación	3	2	3

Escala de puntuación:

5: Excelente en esta categoría, define el estándar de excelencia.
4: Muy bueno, este producto esta sobre la media en esta categoría.
3: Promedio, cumple con las especificaciones pero no muestra cualidades excepcionales ni es un mal producto en esta categoría.
2: Bajo el promedio, no cumple con las expectativas o de manera insuficiente con respecto a la media.
1: No soportado, el producto no cumple con la categoría.

Los administradores de red mediante su experiencia, desempeño y conocimiento en la administración y monitoreo de redes, evaluaron el desempeño de cada sistema

En lo que se refiere a las plataformas soportadas y los costos por licencias, se ha diseñado un esquema bastante práctico y sencillo de resumirlo (véase Tabla 4).

Tabla 4: Plataformas Soportadas Por Las Herramientas

Herramientas	Sistemas Operativos	Método de Acceso	Factor de Puntuación	URL
JFFNMS	(OpenBSD/Apple Mac OS X,) ALL POSIX(LinuxBSD/Independiente(Escrito en un lenguaje interpretado), FreeBSD,Linux;Solaris;Wn 2K, Windows XP	WEB	A	http://jffnms.org
NAGIOS	LINUX	WEB	A	http://www.nagios.org
CACTI	LINUX	WEB	A	

Los productos de código abierto JFFNMS, NAGIOS y CACTI no poseen costo alguno por licenciamiento además de poseer muchas herramientas para la administración y monitoreo de redes IP pero si para el adiestramiento del personal capacitado.

Para poder elegir el sistema sobre el cual se va desarrollar el prototipo de administración y monitoreo de redes WIFI, se tienen que tomar en cuenta muchos factores a evaluar: en función de lo que realmente necesitamos, lo esperado por la herramienta y cuáles son los recursos que se disponen tanto en el aspecto de tiempo como en el económico.

Una vez ya elegido el sistema a utilizar, se deben definir las características y funciones para poder compararlas y establecerlas según los requerimientos impuestos

por la empresa. Es primordial tener muy claro que es lo que necesitamos monitorear y por qué causa ha surgido la necesidad de desarrollar un nuevo sistema de administración y monitoreo del tráfico de datos.

Muchas veces se piensa que un sistema nos resolvería todos nuestros problemas, que estos se mantienen y funcionan solos, pero todos sabemos que la realidad es muy diferente: un sistema requiere de personal especializado que se encargue de su mantenimiento, administración y actualización de los recursos utilizados e incluso una de las labores más difíciles puede ser el arranque o implementación inicial, ya que requiere de una experiencia que quizás no se tenga y de un número de horas hombre que estarán dedicadas a este proceso, debido que se trata de un sistema desarrollado en un sistema operativo abierto, por lo que se requiere de muchos conocimientos en el área de la programación e informática.

Otro aspecto que se debe tomar en cuenta son los recursos de los cuales se disponen, este es un factor determinante en nuestra decisión, ya que si una organización suficientemente sólida está dispuesta a invertir en un proyecto de desarrollar un sistema de gestión de redes, ella puede optar por las plataformas comerciales más conocidas y probadas; sin embargo, a la hora de estimar costos, debemos incluir adicionalmente a los de licencias, las horas de consultoría para poner en marcha el producto, el entrenamiento al personal e incluso la contratación de personal especializado en esta área.

Es lógico que surjan dudas en desarrollar un software de monitoreo de redes en manos de un proyecto de código abierto que recientemente se está implantando en la corporación y para muchos es una modalidad ajena a sus conocimientos, pero hay que tomar en cuenta que el sistema seleccionado tiene flexibilidad de manejo ya que cuenta con un respaldo teórico que los administradores y operadores obtendrán una vez instalado y configurado el sistema.

Es bueno recordar que no todo software de código abierto es realmente gratuito, ya que es libre más no necesariamente gratis, y tampoco todo lo que este bajo esta filosofía es necesariamente bueno o funcional. Aquí es donde debemos ir un poco más allá y donde se deben investigar los siguientes puntos:

- ¿Quienes manejan y desarrollan el software libre?
- ¿Cuáles han sido los resultados y además de cual soporte disponemos a la hora de presentarse los problemas?

Debido a lo comentado anteriormente, para la elección de un software de administración y monitoreo de redes de estándar abierto, éste se debe de presentar como una propuesta seria, de bases sólidas, que tenga continuidad, que su visión sea siempre a mejorar y adaptar el software a las nuevas tecnologías, que tenga una comunidad dedicada a solucionar los problemas que se presenten a los usuario de dicho programa, que disponga de una buena documentación, entre otras. JFFNMS cumple con todas y cada una de las características antes mencionadas además de ser un software robusto de trayectoria y continuidad.

En definitiva, el software sobre el cual se desarrolló el prototipo de administración y monitoreo de redes WIFI de este proyecto fue el JFFNMS, por cumplir este con la mayoría de las exigencias de esta institución y por ser uno de los software de monitoreo menos engorroso a la hora de operarlo. Es importante hacer notar que JFFNMS permite el monitoreo y administración del tráfico de datos en tablas de texto, por lo cual se debe desarrollar módulos gráficos para que el administrador tenga acceso detallado de la red de manera grafica y de modo de texto. Estas características las tienen por separado los sistemas NAGIOS y CACTI, es decir, se tendrían que utilizar ambos para lograr esto que el JFFNMS tiene integrado de manera general, por ello sigue siendo más factible y versátil la utilización de un sistema que cuente con las características más resaltantes de estos dos, por ello se

decide finalmente que por requerimientos de la empresa el JFFNMS es el más apto para nuestro desarrollo.

Una vez elegido el sistema a desarrollar, especificamos las funciones a desempeñar por dicho sistema, es decir, se realiza el diseño de un prototipo de administración y monitoreo partiendo del JFFNMS como herramienta principal para cumplir con las necesidades expuesta por CANTV, a continuación se enumera las funciones generales a desarrollar:

1. Envío de alarmas.
2. Conexiones Establecidas.
3. Información gráfica de las redes a monitorear.
4. El prototipo se encuentre bajo el idioma español y pueda cambiar al idioma que se necesite.
5. Monitoreo del tráfico de las redes WIFI.
6. Mejora del rendimiento del tráfico de datos.

Es decir, luego de tener claro los requerimientos que necesita la Gerencia de Planificación de CANTV, debemos desarrollar y configurar módulos para la realización de estas funciones debido a que el sistema como tal tiene funciones básicas que nos permite desarrollarlas y modificarlas ya que es un sistema bajo código abierto.

Este sistema está instalado bajo la distribución de Debian Lenny 5.0 el cual es unas de las distribuciones más actualizadas del mercado debido a los numerosos paquetes que lo conforman, los cuales son los requeridos para un sistema de gestión.

Una vez seleccionada la distribución del sistema base a utilizar, debemos de utilizar los repositorios de la empresa para que la descarga de los paquetes sea más rápido y contar con los paquetes más actualizados.

Para realizar la instalación del JFFNMS, se tuvo que instalar numerosos paquetes a través de muchos comandos escritos bajo el lenguaje PHP. Para poder ejecutar las funciones ya expuestas, el sistema requiere de una base de datos robusta para almacenarlos (PostgreSQL ó MySQL), un Servidor Web para presentarlos (Apache), el intérprete PHP bajo el cual se ejecutará JFFNMS y utilidades y programas para generar gráficos (RRDtool, Graphviz, etc).

Una vez instalado y configurado el sistema base, se procede al desarrollo de los módulos en lenguaje de programación PHP para la activación del diseño, con el objetivo principal de obtener como resultado un prototipo de un sistema de administración y monitoreo para redes WIFI que sea suficientemente potente. Primeramente una de las modificaciones realizadas fue la construcción de una nueva red interna bajo la dirección IP 127.0.0.2 para poder capturar el tráfico de datos entre 2 computadores.

CAPITULO V

5 DESARROLLO DE UN PROTOTIPO DE ADMINISTARCIÓN Y MONITOREO DEL TRÁFICO DE DATOS DE LAS REDES WIFI.

5.1 DESCRIPCIÓN DE LOS COMANDOS DE LINUX PARA LA ADMINISTRACIÓN Y MONITOREO DE REDES.

5.1.1. ESTRUCTURA DE LOS COMANDOS

Un comando es una instrucción o conjunto de instrucciones que se le dan a un programa para que realice una acción determinada. Los comandos en esencia son funciones que, cuando se les añaden ciertos argumentos y opciones, pueden desencadenar en una acción en el sistema. Es decir, luego de incluir numerosos comandos en el sistema base (JFFNMS) utilizado, éste se convirtió en una nueva aplicación para la administración y monitoreo de las redes WIFI.

Un comando tiene la siguiente estructura:
<nombre del comando> [lista de opciones] [lista de argumentos] <retorno>

5.1.2. LISTADO DE LOS COMANDOS UTILIZADOS EN EL PROGRAMA

Un programa es un conjunto de comandos o instrucciones que se ejecutan en un orden específico para realizar una determinada tarea o trabajo.

La clasificación de los comandos que se utilizan para desarrollar programas en LINUX son:

- Generales.
- Conectividad.
- Administración y Monitoreo.

a) Comandos Generales

A continuación se tiene un listado de los comandos generales que se utilizaron en el desarrollo del prototipo, los cuales son herramientas para la administración de redes de datos:

UNAME

Permite obtener información sobre el tipo de sistema UNIX en el que se está trabajando, permite también determinar la versión del *kernel*.

PS

Muestra la información sobre los procesos que se encuentran en ejecución.

KILL

Es utilizado para enviar señales a los procesos en LINUX, tales como terminar un proceso instantáneamente o dándole tiempo a un proceso para que pueda terminar.

HOSTNAME

Permite obtener el nombre que tiene configurado el *host* local o el que se le pueda asignar.

En el campo de la administración de redes de datos, también se pueden tomar en cuenta algunas herramientas, como las pensadas de forma genérica para la administración de dichas redes:

LINUXCONF: Esta es una herramienta genérica de administración de redes de datos, donde se agrupan los diferentes aspectos de administración en una interfaz de menús textuales. Ésta interfaz se puede utilizar en casi cualquier distribución GNU/Linux y soporta diversos detalles propios de cada distribución.

WEBMIN: esta es otra herramienta de administración de redes pensada para una interfaz Web. Funciona con una serie de *plugins* que pueden ser añadidos para cada servicio que se desee administrar. Normalmente cuenta con formularios donde se especifican los parámetros de configuración de los servicios; además ofrece la posibilidad, si se activa, de permitir la administración remota desde cualquier máquina con navegador.

Los entornos de escritorio de Gnome y KDE se sirven del concepto de "Panel de control", el cual permite la gestión, tanto del aspecto visual de las interfaces gráficas, como de tratar algunos parámetros de los dispositivos del sistema.

b) Comandos de Administración y Monitoreo

A continuación se indica un listado de los comandos para la Administración y Monitoreo de red utilizados en el desarrollo de la aplicación:

ADDUSER

Este comando es utilizado para añadir un usuario al sistema.

USERDEL

El comando USERDEL permite eliminar un usuario del sistema.

IFCONFIG

Permite configurar y ver el estado de las interfaces de red en el *host* local. Es ayudado por los comandos *ifup***,** que habilita la interfaz especificada e *ifdown*, que deshabilita la interfaz especificada.

Este comando junto con otras opciones y argumentos muestra y manipula la tabla de ruteo. Ayuda en la gestión de paquetes, tráfico IP y muestra información relacionada con las interfaces del *host* local.

TCPDUMP

Es un comando al que añadiéndole determinadas opciones, puede capturar paquetes que cursan a través de una determinada interfaz de un *host* en la red, para luego interpretarlos y generar resultados. Comprende o entiende todos los protocolos básicos de Internet, y puede ser usado para salvar o guardar información de los paquetes para su posterior inspección.

SNMPWALK

El comando SNMPWALK sirve para recorrer un árbol MIB del agente, usando la petición *getnext-request* del protocolo SNMP. Con este comando se puede obtener determinada información de la MIB a través del nombre de la rama o mediante número OID.

SAMBA

Es una aplicación, que brinda a los usuarios LINUX un gran número de posibilidades a la hora de interactuar con equipos Windows, ya que trabaja con el protocolo SMB(*Server Message Block*), el cual le permite a LINUX actuar como servidor y ofrecer servicios tales como:

- Compartir uno o más sistemas de archivos.
- Compartir impresoras, instaladas tanto en el servidor como en los clientes.

SAMBA incluye varias herramientas de las cuales, para el desarrollo de la Aplicación, se utilizó: **nmblookup,** que es un comando que se usa para consultar nombres NetBIOS sobre TCP/IP a partir de direcciones IP o viceversa.

NMAP

NMAP es un comando que se utiliza para permitir el escaneo de redes y determinar los dispositivos que se encuentran activos, además de los servicios que estos ofrecen. Este comando proporciona también, la opción de detección remota del sistema operativo.

XGETTEXT

XGETTEXT es un comando que se utiliza para la creación de un archivo con formato.po, para luego tener el formato de archivo con formato.mo, conocido como archivo binario. De esta manera se puede realizar el cambio de idioma de una cadena de caracteres, según el idioma requerido por la aplicación, se puede tener la traducción de varios idiomas, este comando funciona con el lenguaje PHP.

TC

El comando TC permite mostrar y manipular las opciones de control de tráfico en determinada interfaz, además se puede implementar control de tráfico de datos.

HTB (*Hierarchical Token Bucket*)

El comando HTB permite simular un enlace físico en varios enlaces de menor velocidad, además permite enviar diferentes tipos de tráfico hacia los distintos enlaces simulados, para lo cual, utiliza un algoritmo que divide el ancho de banda de manera que se puede especificar un ancho de banda mínimo y un máximo, tanto para el enlace físico como para los enlaces simulados.

5.2. DISEÑO DEL PROTOTIPO DE ADMINISTRACIÓN Y MONITOREO DEL TRÁFICO DE DATOS DE LAS REDES WIFI

Este prototipo se creó en el ambiente de programación PHP, este nos permite desarrollar aplicaciones en las cuales podemos llamar a ejecutar comandos internos de LINUX y los resultados enviarlos a archivos, en donde se les pueda modificar para su posterior presentación a través de una interfaz adecuada. Para el desarrollo del programa se han definido los siguientes componentes, los cuales se indican en la figura 14.

- Entrada de datos
- Procesamiento de datos
- Salida de datos.

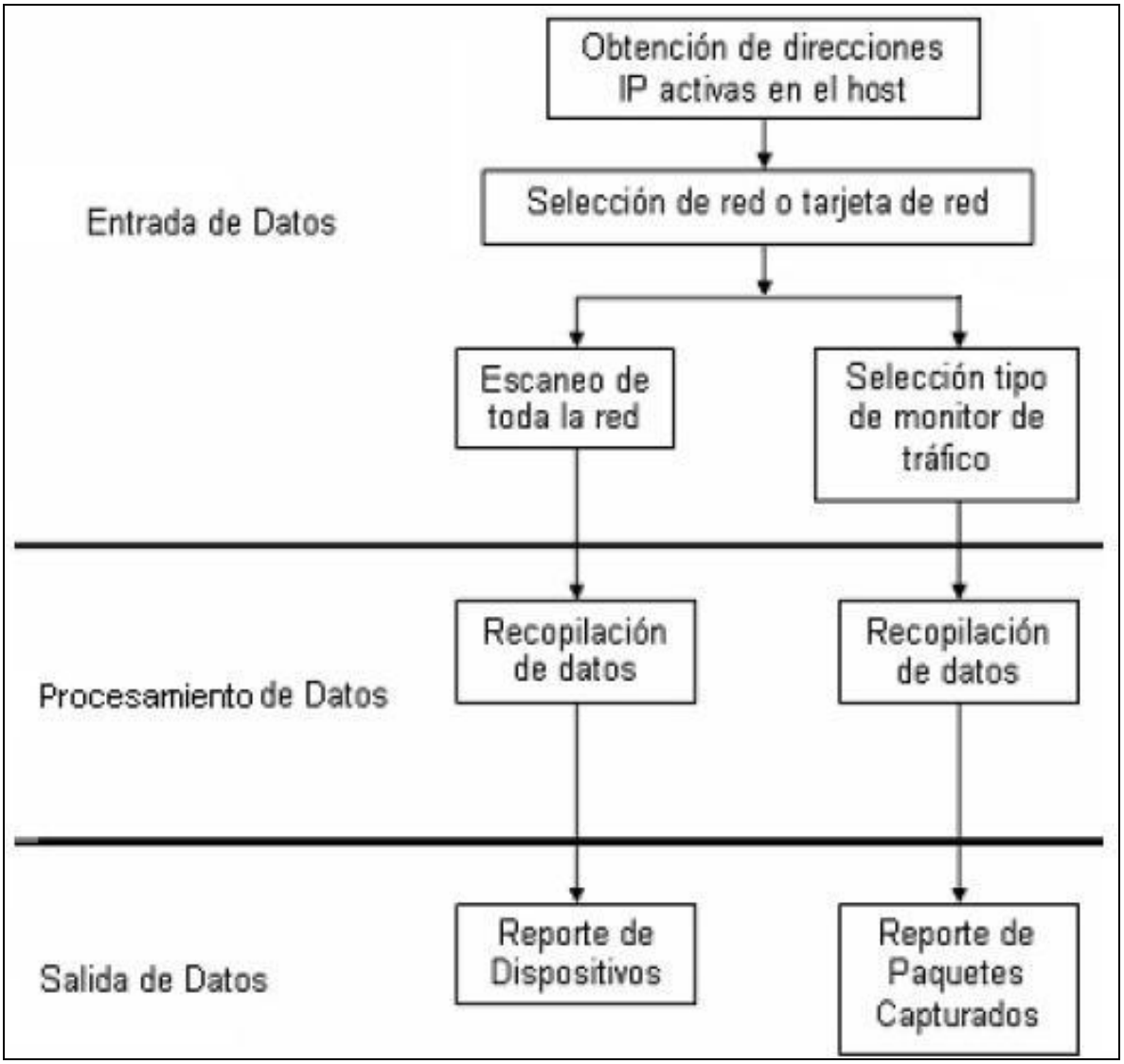

Figura 14: Componentes para el desarrollo del prototipo.

5.3. DISEÑO DEL PROTOTIPO PARA EL MONITOREO DE DISPOSITIVOS DE RED

Para el funcionamiento adecuado del programa para el Monitoreo de dispositivos, es necesario que el *host* donde se ejecuta la aplicación cumpla con los siguientes requisitos:

- En el archivo */etc/snmp/snmpd.conf* se debe incluir la red o redes a las que pertenece el *host*

- El servicio *snmpd* debe estar iniciado

- Los comandos *nmap, nmblookup* deben estar instalados y funcionando correctamente.

- Cabe destacar que para que se ejecute el sistema de monitoreo para las redes WIFI se debe editar el */etc/snmp/snmpd.conf* para agregarle información que permita la captura del tráfico al igual debemos crear una nueva configuración a nivel de la tarjeta de red, ya que la que viene por defecto trabaja con redes alámbricas y en este caso se agregó una eth1, para que el *kernel* levante el sistema y reconozca la red, y así el servidor tenga acceso a las IP generadas por los equipos a monitorear.

Para el monitoreo de los dispositivos de red, primeramente se sondean las tarjetas de red, es decir, se revisa las direcciones ip activas en los equipos para luego poder seleccionar la IP que se quiere monitorear. Seguidamente mediante el comando ya aplicado e instalado NMAP y utilizando el sistema operativo Linux, directamente se obtiene el nombre de la red, en otras palabras mediante los datos almacenados en la base de datos se obtiene la información requerida y luego ésta despliega los datos de manera ordenada al administrador de red.

En caso de no trabajar con el sistema operativo Linux se obtiene el dominio y nombre IOS con SNMP.

En la figura 15 se muestra en forma de diagrama de flujo, los pasos que se deben llevar a cabo para el monitoreo de dispositivos de red en el prototipo a desarrollar.

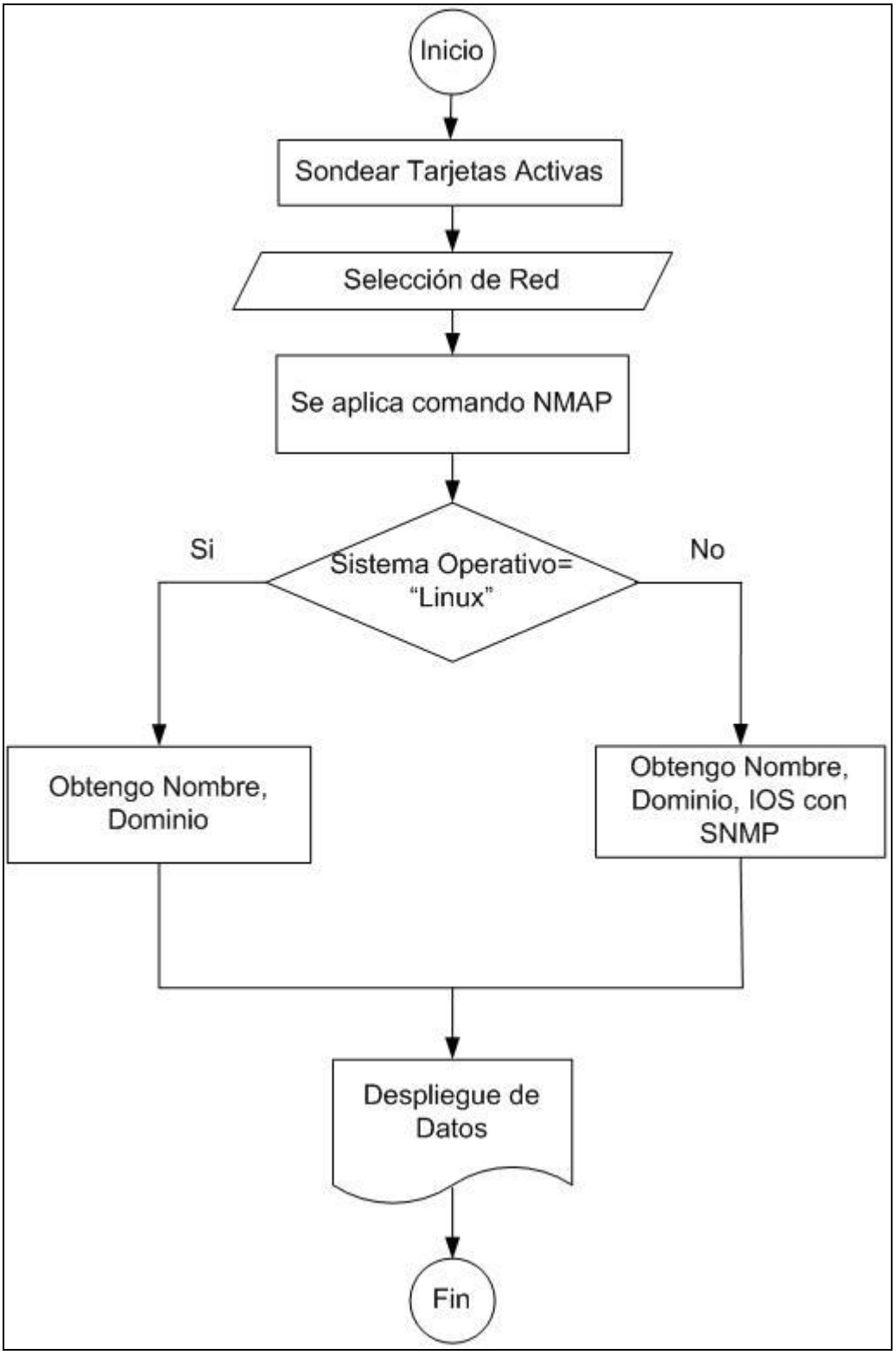

Figura 15: Diagrama de flujo del monitor de dispositivos de red

5.3.1. ENTRADA DE DATOS PARA EL MONITOREO DE DISPOSITIVOS DE RED

El comando **ip route list** permite obtener la información de la red o redes activas configuradas en el equipo, es decir, muestra las interfaces de red con su respectivo nombre, dirección IP, dirección de red y máscara de red.

Otra opción que presenta, es la del ingreso manual de la dirección de red, máscara e interfaz, además del ingreso de la comunidad SNMP a la cual se va a acceder en los dispositivos administrables y equipos LINUX. En la figura 16 se aprecia el diagrama de flujo el procedimiento para la entrada de datos en el monitoreo de dispositivos de red.

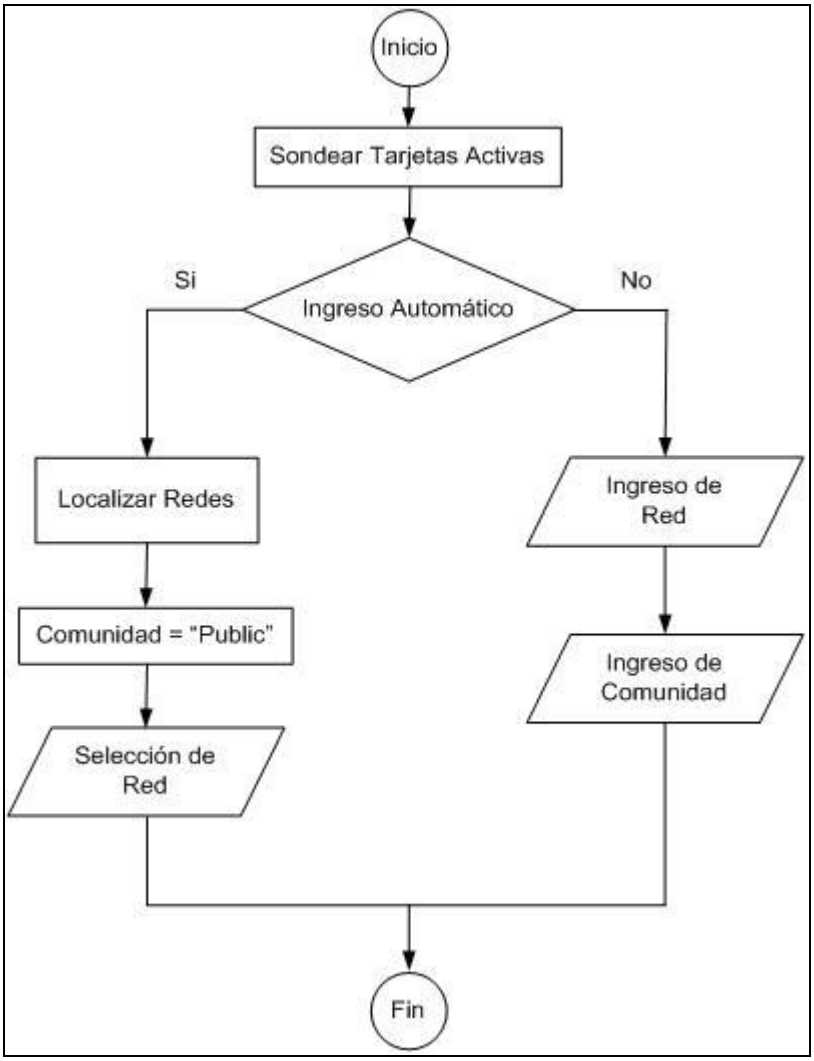

Figura: 16 Diagrama de flujo de la entrada de datos para el monitoreo de dispositivos.

5.3.2. PROCESAMIENTO DE DATOS PARA EL MONITOREO DE DISPOSITIVOS DE RED

Una vez ingresados los datos, el programa de exploración de dispositivos se inicia con la ejecución del comando **nmap –O <dirección de red/máscara>,** donde –O es la opción que le indica a *nmap* que debe realizar la exploración con la obtención del sistema operativo, direcciones IP activas, direcciones MAC con su respectivo fabricante y tipo de dispositivo.

Para los dispositivos clasificados como *host* con sistema operativo LINUX, se extrae el nombre y dominio de red a través del comando **snmpwalk –v1 –c <comunidad> <dirección ip> system.sysName.0** (donde –v es la opción de versión de SNMP, -c es la opción de comunidad SNMP). Si el dispositivo se encuentra clasificado como administrable, entonces, se procede a obtener su nombre (si lo tiene), tipo de sistema operativo IOS (*Input Ouput System*) para poder distinguir entre conmutador (*switch*) o enrutador (*router*), esto se lo hace mediante el comando **snmpwalk –v1 –c <comunidad> <dirección ip>.**

Para los archivos con resultados obtenidos del comando *nmblookup*, se realiza el tratamiento de texto necesario para generar un documento que contenga información del nombre del *host* y su respectivo dominio.

Los archivos que contienen información de nombre, dominio y tipo, para los dispositivos administrables, son generados de la misma manera que los anteriores, pero la fuente de ésta información son los resultados del comando *snmpwalk*.

Los archivos que contienen la información organizada de acuerdo a los requerimiento de salida de datos para el monitoreo de dispositivos, son guardados en un directorio de reportes con la fecha y hora en la que se inició el monitoreo. En la figura 17 se muestra el procesamiento de los datos en el monitoreo de dispositivos de red

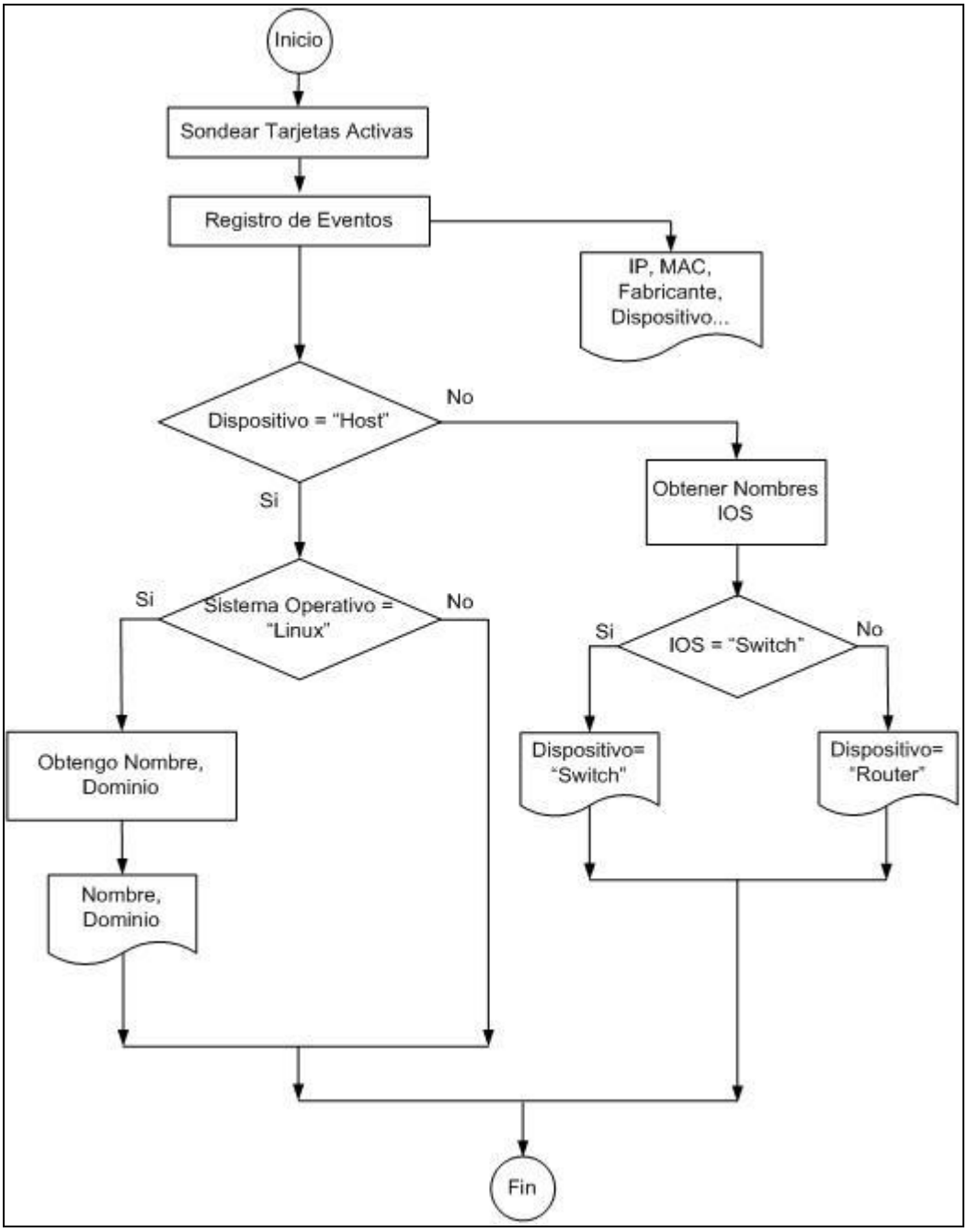

Figura. 17 Diagrama de Flujo del Procesamiento de datos del Monitor de Dispositivos de Red

5.3.3. SALIDA DE DATOS PARA EL MONITOREO DE DISPOSITIVOS DE RED

El despliegue de resultados, se realiza a través de la lectura de los archivos generados en cada uno de los procesos anteriores, ubicándolos en listas con diferentes columnas, donde se presenta la información recopilada durante el monitoreo.

Los resultados se muestran a manera de reporte por medio de alarmas clasificadas por tipo, es decir, *hosts* y dispositivos administrables, cada uno con sus respectivos detalles.

Dentro del proceso de actualización de monitoreo de dispositivos, a través del comando *ping* se verifica si las direcciones IP que estuvieron en el monitoreo anterior siguen activas, de lo cual, se genera un documento que muestra un listado con las direcciones IP que no respondieron a este comando.

Existe además la posibilidad de acceder a reportes de monitoreo anteriores, a través de la opción “archivos” en la barra del menú, la cual desplegará el reporte en forma de texto plano en la pantalla.

6.4. DISEÑO DEL PROGRAMA PARA EL MONITOREO DE TRÁFICO

Para el correcto funcionamiento del Monitor de Tráfico es necesario tener instalado el comando *tcpdump*.

Dentro del monitoreo de tráfico, se pueden realizar las siguientes tareas:

- Monitoreo de Tráfico por puertos, y además
- Dentro de cada uno de los monitoreo, la opción de monitorear sólo el tráfico del *host* local. Ver figura 18.

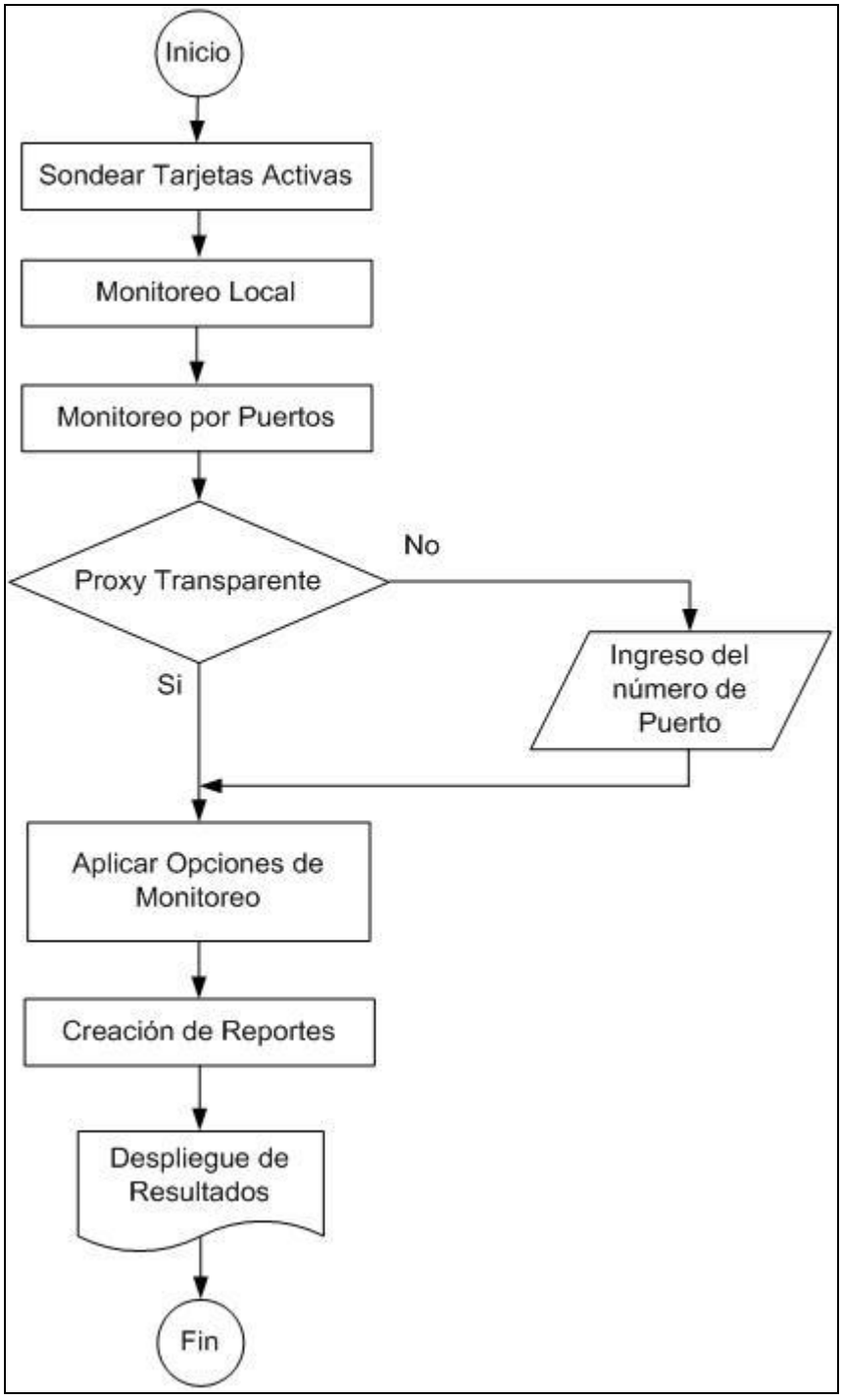

Figura 18. Diagrama del procedimiento utilizado para realizar el monitoreo de Tráfico.

5.4.1. ENTRADA DE DATOS PARA EL MONITOREO DE TRÁFICO

Para obtener la información de las interfaces de red activas configuradas en el *host*, se hace uso del comando **ip –o -4 addr show**, el mismo que despliega información de las interfaces de red con su respectiva dirección IP, máscara y nombre.

Para el Monitor de Tráfico se debe seleccionar el tipo de monitoreo que se desea realizar, si el monitoreo de tráfico es por puertos; y se debe además elegir si se utiliza o no proxy transparente, es decir, si no se eligió proxy transparente, se deberá ingresar el número de puerto proxy.

5.4.2. PROCESAMIENTO DE DATOS PARA EL MONITOREO DE TRÁFICO

Con los datos de información de interfaz de red, se procede con la ejecución del comando **tcpdump**, en el cual, tratándose del monitor de tráfico por puertos, la forma del comando será así: **tcpdump –i <interfaz> port <puerto>,** donde, en la opción puerto se puede ingresar cualquiera de los números de puerto disponibles en el archivo /etc/services para su monitoreo.

La recopilación de los paquetes capturados por el comando *tcpdump* son enviados a un archivo de registro mediante la opción **–w**, la cual, una vez terminado el proceso de captura, crea un archivo con la información necesaria para obtener los resultados totales a partir de la opción **-r** del mismo comando *tcpdump*. Este procedimiento se realiza para el monitoreo de cada uno de los de puertos, para luego realizar el cálculo de los promedios generales mediante el uso de comandos para tratamiento de texto.

Los archivos que se crean a partir del tratamiento de texto, son guardados en un directorio de reportes con la fecha y hora en que inició el monitoreo.

5.4.3. SALIDA DE DATOS DEL MONITOREO DE TRÁFICO

La presentación de los resultados se realiza a través de la lectura de los archivos generados en cada uno de los procesos anteriores, ubicándolos en listas donde se presenta la información detallada y promedio de lo recopilado durante el monitoreo, está información se presenta mediante gráficos, los cuales contienen los datos del tráfico, es decir, mediante el escaneo de la base de datos, esta información se expresará a través de herramientas gráficas que contiene la aplicación.

Existe además la posibilidad de observar reportes de monitoreo anteriores a través del menú y opción archivos de monitor de tráfico, la cual desplegará el reporte en forma de texto plano y gráfica en pantalla.

5.5 PROCEDIMIENTO QUE REALIZA EL PROTOTIPO DE ADMINISTRACIÓN Y MONITOREO DEL TRÁFICO DE DATOS DE LAS REDES WIFI

Una vez instalado y configurado cada módulo del prototipo de administración y monitoreo del tráfico de datos de las redes WIFI, se procede a guardar la información a monitorear, es decir, nombres, *host*, direcciones, interfaces, etc; el sistema se asocia con el medio de transmisión y partes semejantes, tal como transmisores y receptores, conectores, niveles de voltaje, entre otros.

En esta fase básicamente se realiza la transmisión de los *bits* de información a lo largo del canal de comunicación, donde se decide la representación de los *bits* (la

forma de modulación, señales eléctricas u ópticas) y se establece la duración de un *bit.* En otras palabras, cubre lo que es la ingeniería de transmisión.

Luego se asegura la transferencia de datos libres de error entre nodos adyacentes (sincronización a nivel de datos). Esta información está encapsulada por tramas (típicamente constituidas por algunos cientos de octetos) y las transmite en forma secuencial, recibiendo tramas de confirmación (ACK: confirmación positiva, NACK: confirmación negativa) por el receptor.

Ejemplo de algunos protocolos que permiten la transferencia de datos son: HDLC, LAPB, LAPD, SLIP y PPP.

Las tramas acceden a dos medios existentes; al control de acceso los medios existentes y al control de enlace lógico, es decir, enlazan al control de acceso al medio (MAC) con el control de enlace lógico (LLC).

Seguidamente se determinan las rutas adecuadas para llevar la información de un lado a otro (proporciona el enrutamiento), es decir, se proporciona una interfaz para que la transferencia de datos sea idéntica a la de la tecnología del enlace de datos. Cabe destacar que los paquetes de datos, son la unidad de información, lógicamente agrupada, que se desplaza entre los sistemas de computación. Estos paquetes incluyen la información origen junto con otros elementos necesarios para hacer que la comunicación sea factible y confiable en relación con los distintos dispositivos, y son semejantes en su estructura a las tramas, pudiendo ser también de longitud variable.

Estos paquetes ocupan el campo de datos en las tramas y son gestionados por el protocolo IP; este protocolo permite la entrega de paquetes (llamados datagramas IP), cuya característica principal es la de un protocolo no orientado a la conexión,

debido a que cada uno de los paquetes puede seguir rutas distintas entre el origen y el destino, no es fiable porque los paquetes pueden perderse, dañarse o llegar retrasados.

Ya recorridas las sub redes, los datos o bloques de información son transportados, aceptados y a su vez son fraccionados cuando es necesario, en unidades más pequeñas para que puedan ser fácilmente manejados por la capa de red y asegurarse de que todos los bloques de información lleguen correctamente al otro extremo, esta función es generada por el TCP/IP que permite la comunicación entre *hosts*. Este es un protocolo orientado a la conexión, es decir, la comunicación se trata como un flujo de datos (*stream*).

Para la operación de TCP, es necesaria la sincronización del intercambio de señales de tres vías, y significa que antes de establecerse la comunicación entre dos dispositivos, deben llevar a cabo el proceso de sincronización para establecer una conexión virtual para cada sesión. Este proceso siempre lo inicia el cliente y para lo cual usa un puerto conocido del servicio que se desea contactar.

El proceso ocurre así: primero el cliente inicia la sincronización enviando un paquete SYN para iniciar la conexión, en el siguiente paso, el otro dispositivo recibe el paquete y responde con un acuse de recibo ACK, como último paso el dispositivo que inició la conversación responde con un ACK indicando que recibió el ACK enviado por el otro dispositivo y finaliza el proceso de conexión para esta sesión.

Luego se procede a gestionar y finalizar las conexiones entre usuarios (procesos o aplicaciones), que dos comunicaciones a la misma operación crítica no se efectúen al mismo tiempo, es decir, que dada una sesión establecida entre dos máquinas, la misma se pueda efectuar para las operaciones definidas de principio a fin, reanudándolas en caso de interrupción. En otras palabras, se trata de mantener el enlace entre los dos computadores que estén transmitiendo datos de cualquier índole.

Ya teniendo la transmisión de datos de manera segura se procede a la compresión y encriptación de la información, debido a que los diferentes equipos pueden tener diferentes representaciones internas de caracteres, números, sonido o imágenes; Por ello, permite que los datos lleguen de manera reconocible, y así poder leer la información de manera satisfactoria. En esta fase se trata la semántica y la sintaxis de los datos transmitidos, ya que distintas computadoras pueden tener diferentes formas de manejarlas. En pocas palabras es un traductor.

Una vez que se tiene la información en un solo formato, podemos proporcionar diferentes aplicaciones según el usuario lo pida, en este caso vamos a administrar y monitorear el tráfico de datos mediante el protocolo SNMP (Protocolo simple de gestión de red) que es un protocolo de nivel de aplicación, es decir, es la capa que interactúa con el sistema operativo o aplicación cuando el usuario decide transferir archivos, leer mensajes, o realizar otras actividades de red. Por ello, en esta capa se incluyen tecnologías tales como http, DNS, SMTP, SSH, Telnet, entre otras. Este protocolo pertenece a la familia TCP/IP y ofrece servicios de gestión de red. Permite a los administradores supervisar el desempeño de la red, buscar y resolver sus problemas, y planear su crecimiento. Una vez el dispositivo administrado se refiere a un nodo de red que contiene un agente SNMP y reside en una red administrada, éstos recogen y almacenan información de administración, la cual es puesta a disposición de los NMS's usando SNMP. Los dispositivos administrados, a veces llamados elementos de red, pueden ser *routers,* servidores de acceso, *switches*, *hubs,* y computadores que se utilizaron para las pruebas del prototipo. Esto se muestra en la figura 19.

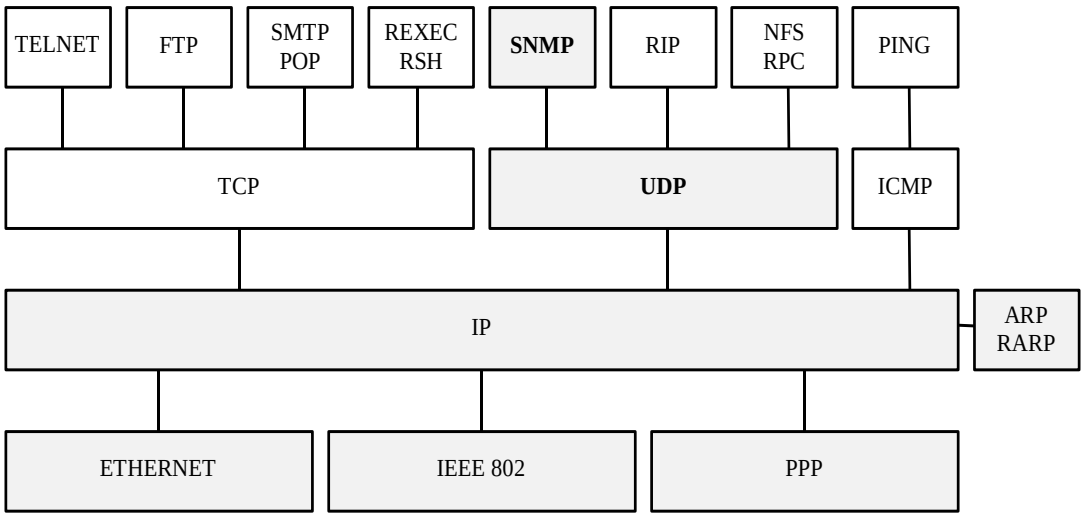

Figura 19: Principales Protocolos utilizados en la administración de red.

El agente posee un conocimiento local de la información de administración (memoria libre, número de paquetes IP recibidos, rutas, etc), la cual es traducida a un formato compatible con SNMP y se crean las siguientes herramientas o acciones:

- Informar del funcionamiento de la red o subred
- Detectar averías y funcionamientos incorrectos
- Permitir actuar sobre los elementos de la red: modificando su configuración, equipos desconectados, etc.

SNMP define una relación cliente/servidor entre el gestor de red (que actúa de cliente) y los elementos gestionados (que son los servidores y reciben el nombre de "agentes SNMP").

Típicamente el gestor de red se ejecutará en una estación de trabajo (en nuestro proyecto va a ser una máquina de CANTV que proporcione la información requerida) controlada manualmente por el administrador de red o automáticamente por un plan de trabajo definido previamente.

Las operaciones básicas de administración a través del protocolo SNMP utiliza un servicio no orientado a la conexión (UDP) para enviar un pequeño grupo de mensajes (PDUs) entre los administradores y agentes, para asegurar que las tareas de administración de red no afectarán al rendimiento global de la misma.. Ver Figura 20.

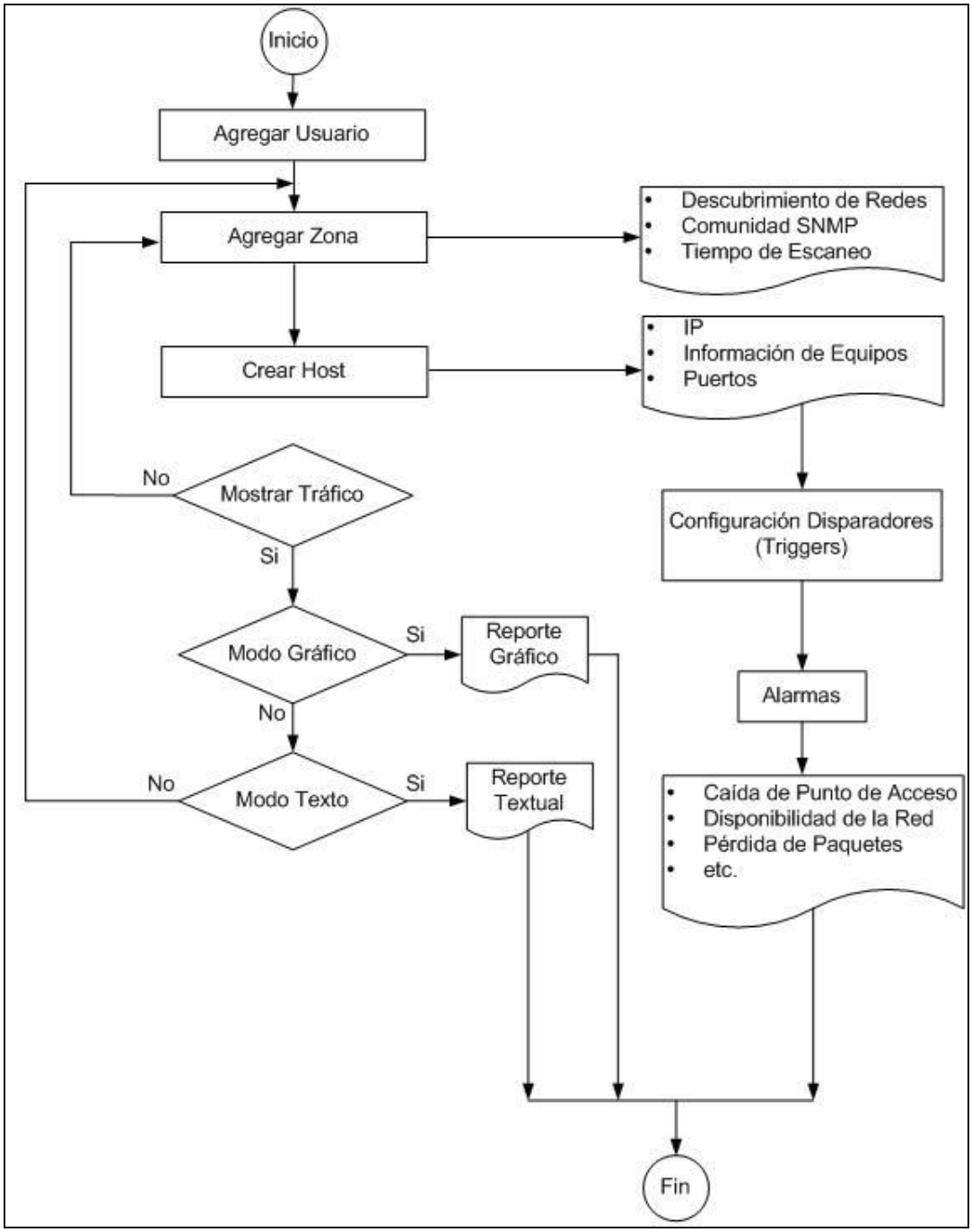

Figura 20. Diagrama del funcionamiento general del Prototipo

6.6 REQUERIMIENTOS DEL DESARROLLO DEL PROTOTIPO DE ADMINISTRACIÓN Y MONITOREO DE RED

6.6.1 REQUERIMIENTOS GENERALES

El objetivo de diseñar un prototipo, es utilizar los comandos y utilidades del sistema operativo LINUX para obtener una aplicación gráfica que permita monitorear y administrar el tráfico de datos en redes WIFI, se utilizó un ambiente de ventanas (ver figura 21); en el cual la ejecución del programa requiere que el equipo donde se instale la aplicación esté conectado a una red y tenga la configuración de red básica para su funcionamiento, además deben haber sido ejecutados los comandos necesarios para el funcionamiento de la aplicación. En el caso de la administración del tráfico de datos, el programa debe ser ejecutado en el *host* que esté actuando como servidor de la red, es decir, éste debe proveer las aplicaciones que el software de administración de tráfico va a controlar, como se observa en la figura 22.

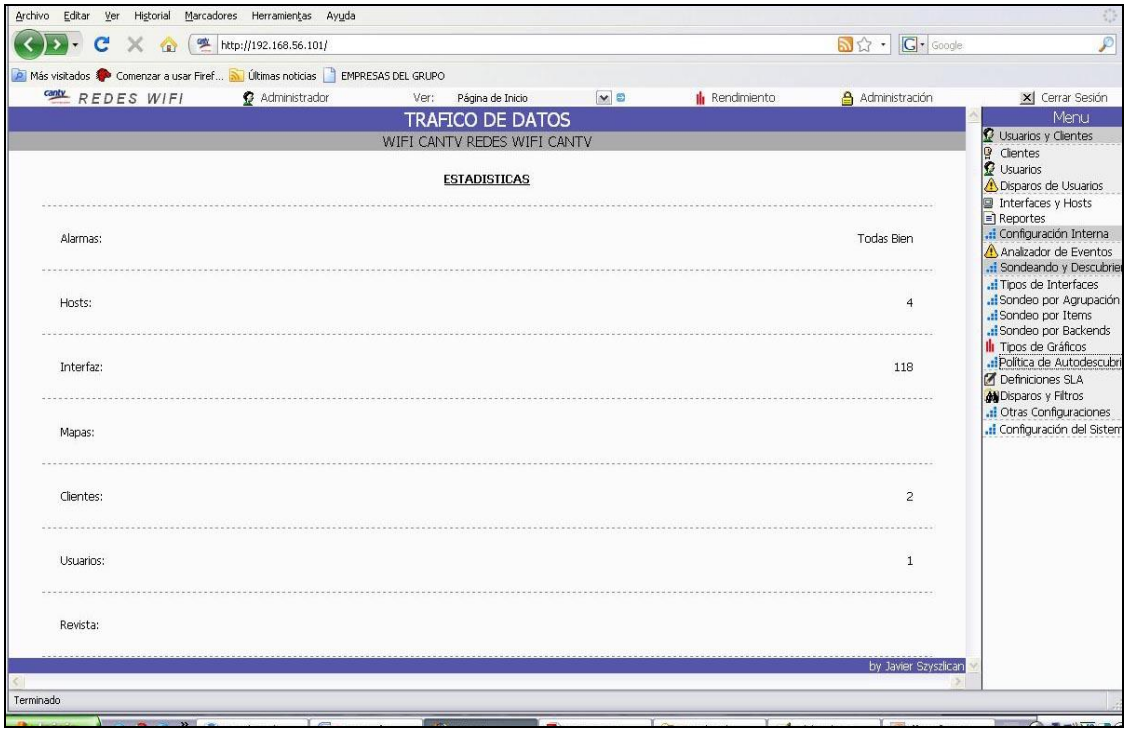

Figura 21. Ambiente tipo ventanas

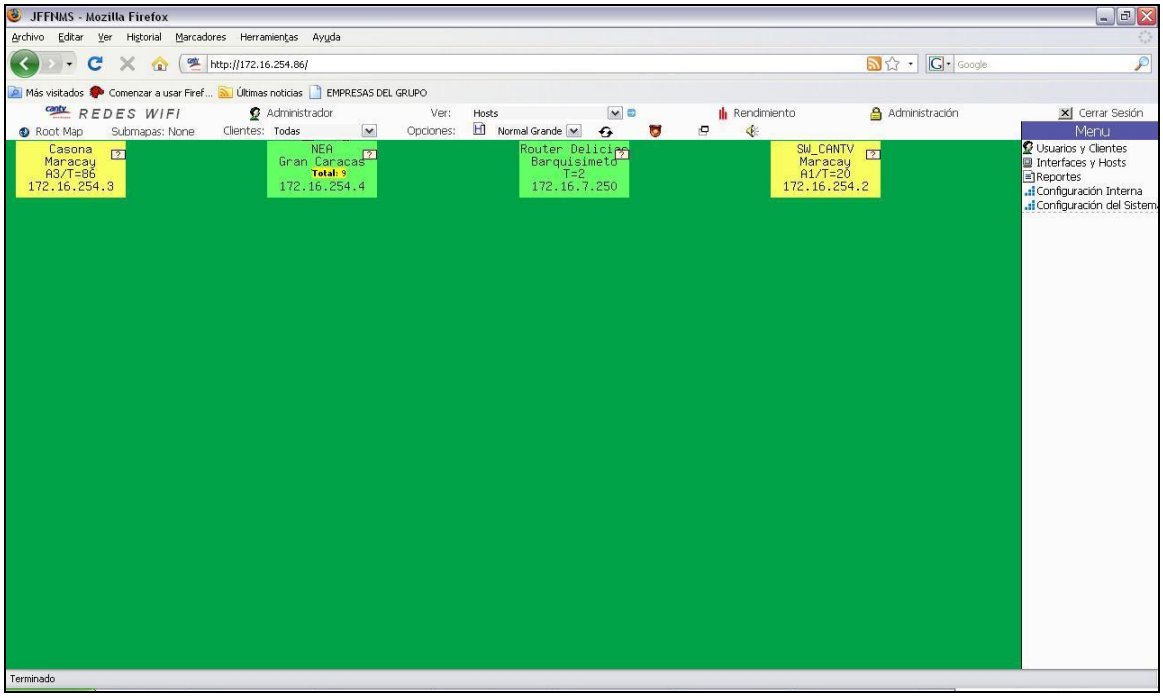

Figura 22. Muestra de host configurados

5.6.1. REQUERIMIENTOS DE INGRESO DE DATOS

Inicialmente el programa debe recoger la información de red, además debe determinar las redes activas, luego comienza la exploración de dispositivos, monitoreo y administración de tráfico dentro de la red. Ver figura 23.

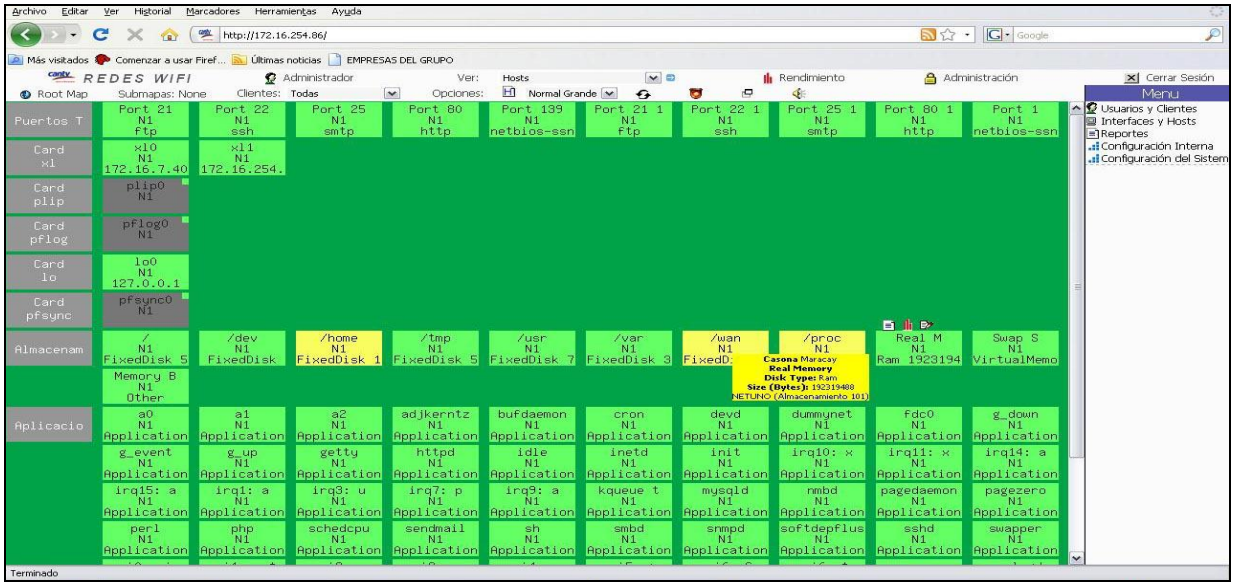

Figura 23. Exploración de los dispositivos en la red

Todo esto se realiza mediante el uso de cuadros de diálogo con campos específicos, representados por pestañas para los diferentes tipos de datos a ingresar. Como se muestra al lado izquierdo de la figura 24.

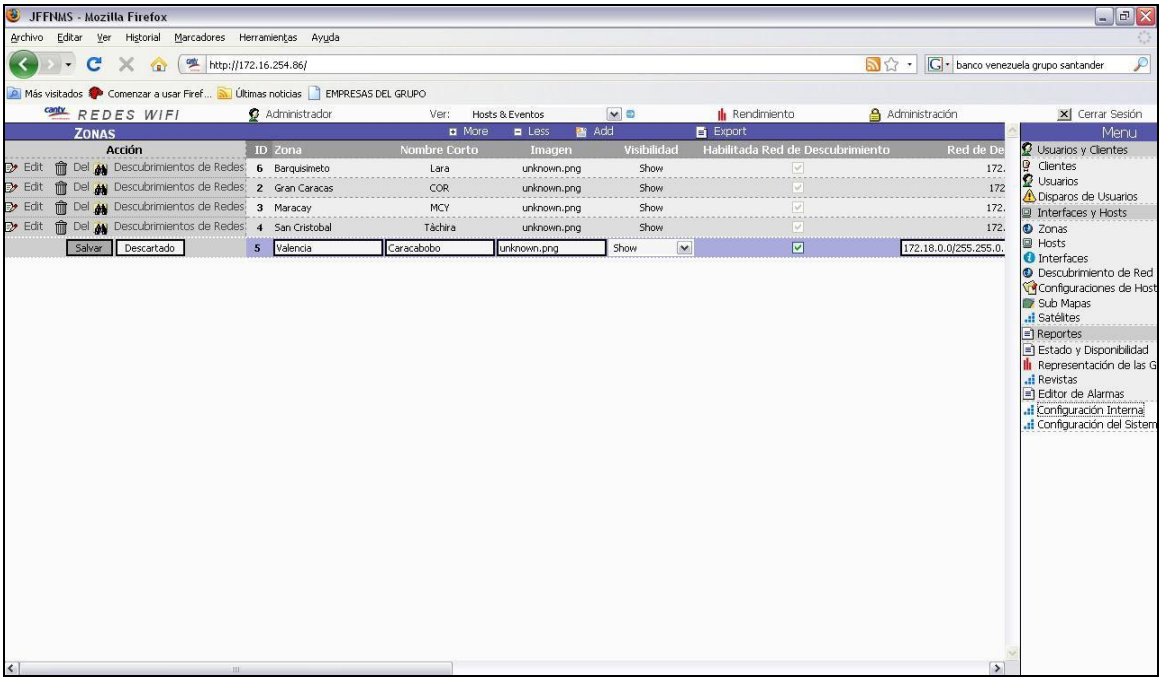

Figura 24. Muestra de menú por pestañas y datos a ingresar

5.6.2. REQUERIMIENTOS DE SALIDA DE DATOS

Una vez terminado con el monitoreo y exploración, se necesita mostrar los resultados obtenidos, en forma de lista, de los componentes o dispositivos encontrados y en una tabla con los resultados obtenidos del monitoreo de tráfico.

Para un mejor entendimiento de los resultados, la lista de dispositivos encontrados en entorno LINUX y dispositivos administrables; por el lado de la tabla de paquetes capturados por el monitor de tráfico, se presentan estos resultados mediante gráficas, ver figura 5.

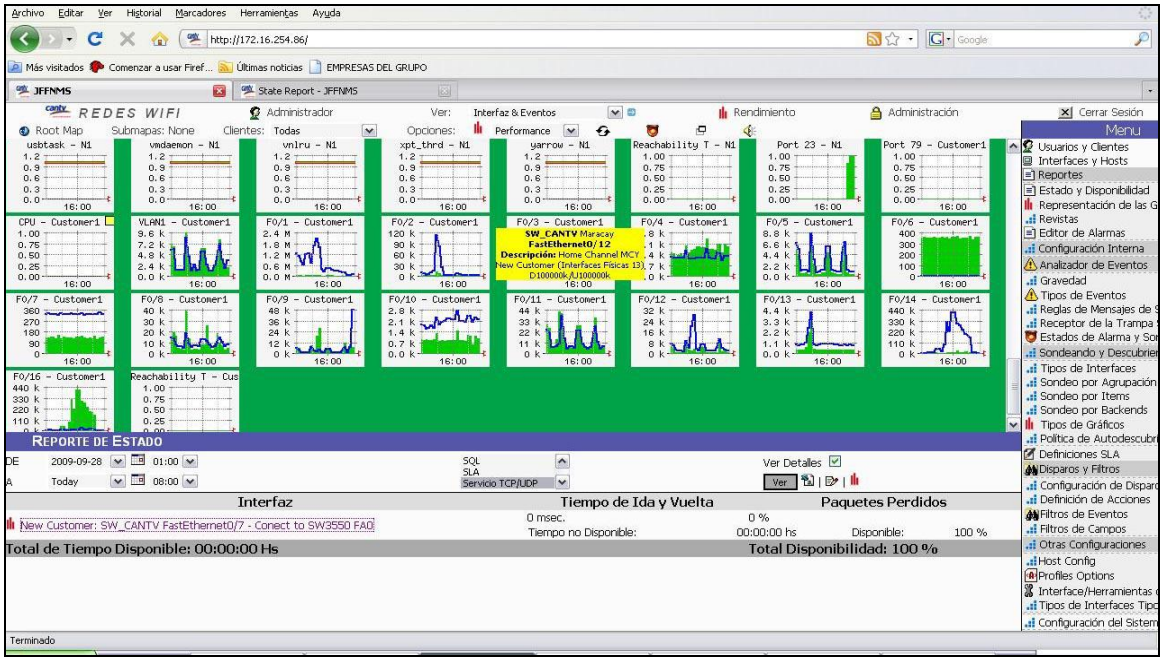

Figura 25. Muestra de resultados por grafica y modo texto

CAPITULO VI

6 PRUEBAS Y EVALUACIONES DEL PROTOTIPO DESARROLLADO.

6.1. PRUEBAS DEL MONITOREO Y ADMINISTRACIÓN

Las pruebas se efectuaron en una maqueta WIFI establecida en CANTV.

6.2 LIMITACIONES DEL PROTOTIPO

A continuación se describen algunas limitaciones que tiene la aplicación de Monitoreo:

- No se puede determinar el nombre del dispositivo o *hos*t, cuando éste se encuentre en los siguientes casos:

1. Dispositivos administrables sin configuración SNMP, y
2. *Hosts* LINUX con servicio SNMP apagado.

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

- Para el Monitor de Tráfico, si el usuario no sabe de la utilización de un proxy y si éste es o no transparente, el análisis de tráfico HTTP se realiza a través del puerto 80, además si los números de puerto asignados originalmente a las aplicaciones HTTP, FTP, SMTP y SNMP fueron cambiados en el *host* donde

se ejecuta la aplicación, el Monitoreo de Tráfico por puertos no entregará los resultados adecuados.

- Para la Administración del tráfico de datos, la ejecución del programa se debe realizar en un *host* que esté sirviendo alguna aplicación tal como, HTTP, FTP, SMTP o ICMP a la red, caso contrario, no se observará ningún efecto. Además el usuario debe tomar en cuenta el ingreso o no del número de puerto proxy, ya que caso contrario, el control para el tráfico HTTP se realizará a través del puerto 80.

El desarrollo del prototipo de administración y monitoreo del tráfico de datos de las redes WIFI fue evaluado a través de las pruebas realizadas en CANTV, cumpliendo con los requerimientos exigidos por la Gerencia de Planificación de dicha empresa, es decir, se obtuvieron los resultados que dieron credibilidad del funcionamiento esperado por los administradores de red. A continuación se describe las funciones del prototipo diseñado:

a) **Monitoreo de dispositivos**: Se realiza una búsqueda de los dispositivos que se encuentran activos en la red mediante el comando *nmap*. Luego, con el comando *nmblookup*, se obtiene el nombre de los *hosts* pertenecientes de la red, la cual corresponde a información del protocolo NetBIOS. Para obtener el nombre de los *hosts* dentro del entorno LINUX y para el nombre y sistema operativo de los dispositivos administrables, se utiliza el comando snmpwalk. Ver figura 26.

.

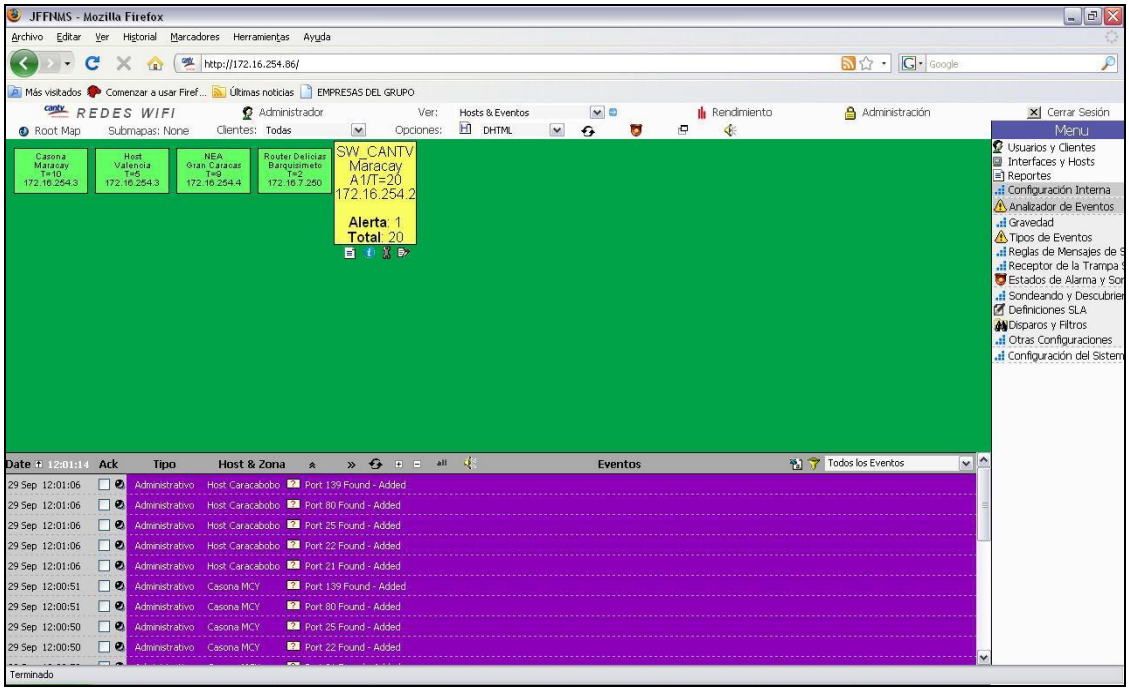

Figura 26. Nombres de los *host* y alarmas.

b) **Monitoreo de tráfico**: Se realiza la captura de paquetes por puertos, por medio de las opciones que ofrece el comando tcpdump. A través de una serie de eventos que son expresados por medio de alarmas, luego de utilizar el comando snmptrap y configurar los disparadores (*triggers*) y *host* existentes en los equipos a monitorear, permiten mostrar la información existente en dichos puertos como lo muestra la figura 27.

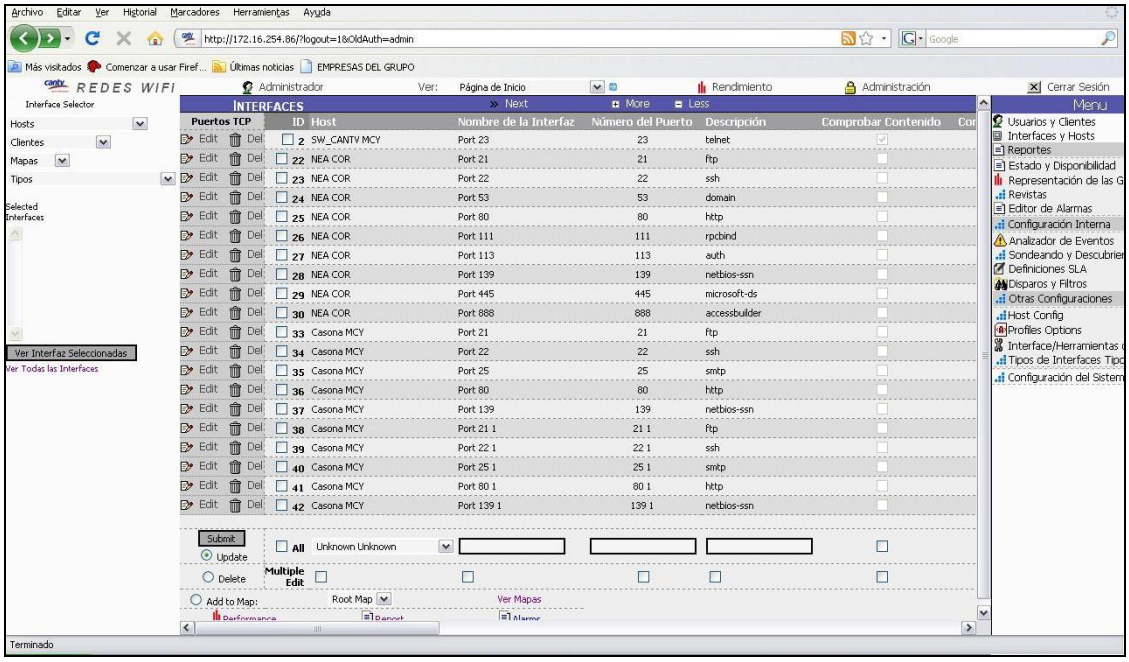

Figura 27. Puertos existentes en el *host* la casona.

c) **Administración de tráfico**: En base a los comandos *tc y htb*, se crean clases y filtros de acuerdo a direcciones IP y protocolos. Luego, en base a la aplicación gráfica del prototipo llamado "Redes WIFI de CANTV", se muestra en pantalla de modo gráfico y de texto la información almacenada en la base de datos de cada unos de los equipos configurados en la red, según la opción que se haya seleccionado, ver figura 28.

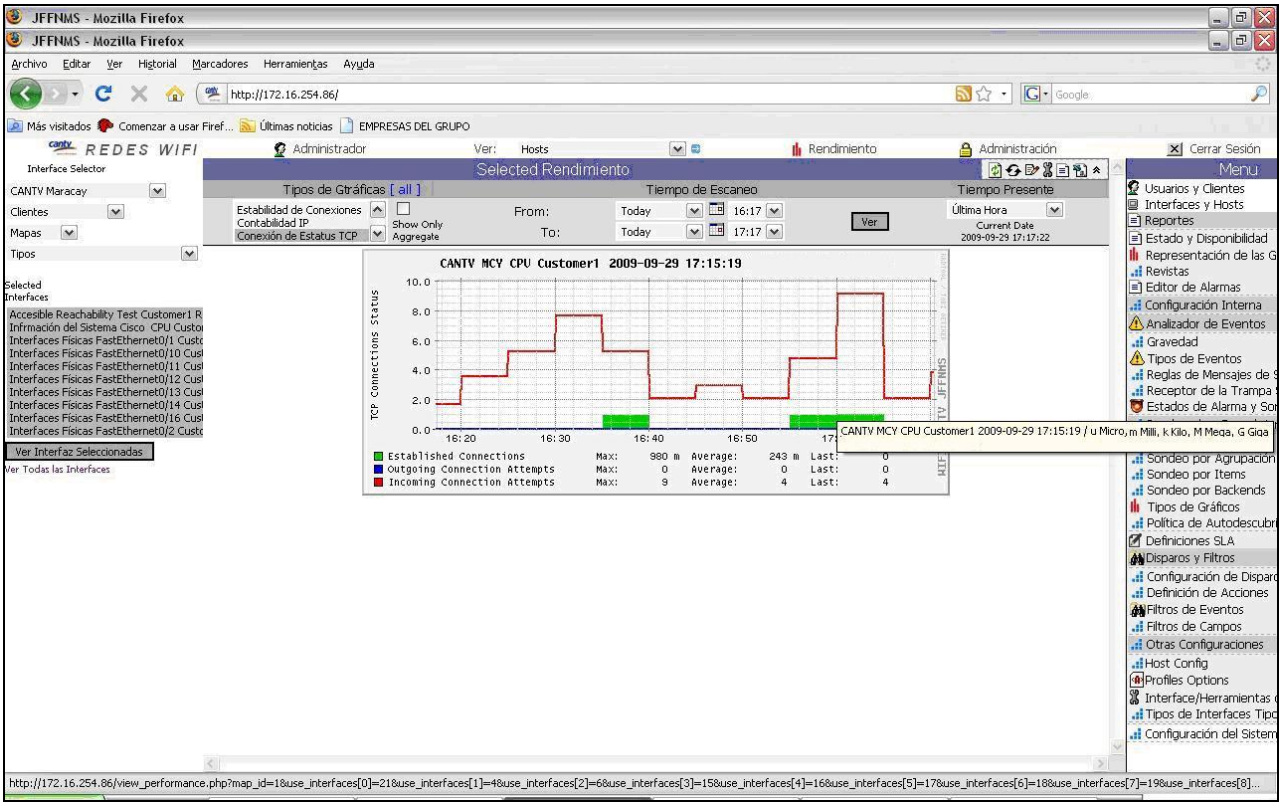

Figura 28. Muestra información mediante gráficas.

d) **Internacionalización**: Luego de instalar los paquetes xgettex, gettext y msgfmt junto con el comando **xgettext --default--domain = messages traduce.php,** crea un tipo de archivo .po y luego con la inserción de la siguiente función:

<?

putenv ("LC_MESSAGES=es"); // Specify location of translation tables

bindtextdomain ("messages", "./locale"); // Choose domain

textdomain ("messages");

?>.

Luego se guarda con el formato de PHP, que también permite al sistema contar con diferentes idiomas, según sea el requerimiento, solo se debe de cambiar las iniciales de cada idioma (en, es, entre otros); Es decir, luego de ingresar la función a la que se hace referencia, se crea un archivo .mo el cual es de formato binario y

trabaja bajo el lenguaje PHP, este muestra la cadena de caracteres del lenguaje utilizado, y de manera ordenada te va cambiando el idioma, cabe destacar, que hay que estudiar y editar el código del programa ya que se debe tener claro que variables, funciones y caracteres del mismo.

Esta función tiene la ventaja de poder realizarse varias veces y cambiar el idioma del sistema a varios idiomas, según lo requerido, solo se tiene que cambiar las iníciales según el idioma. De esta manera minuciosa y segura se obtuvo un prototipo en español para mayor facilidad de los nuevos operadores y administradores de red, como se muestra en la figuras 29 y 30.

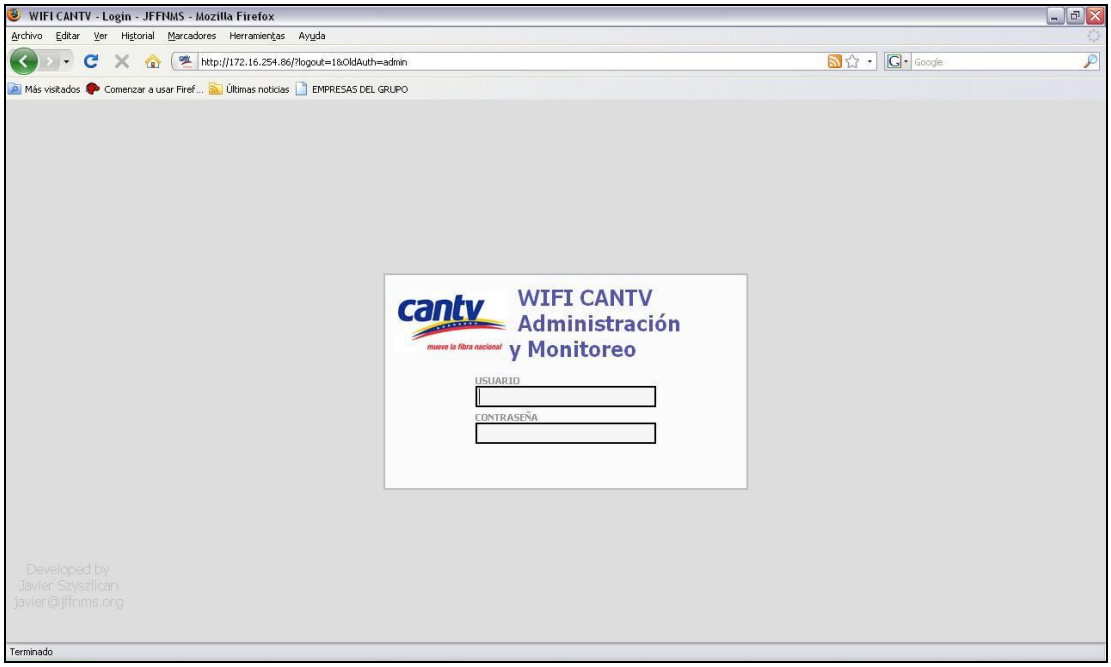

Figura 29: Presentación del prototipo en español

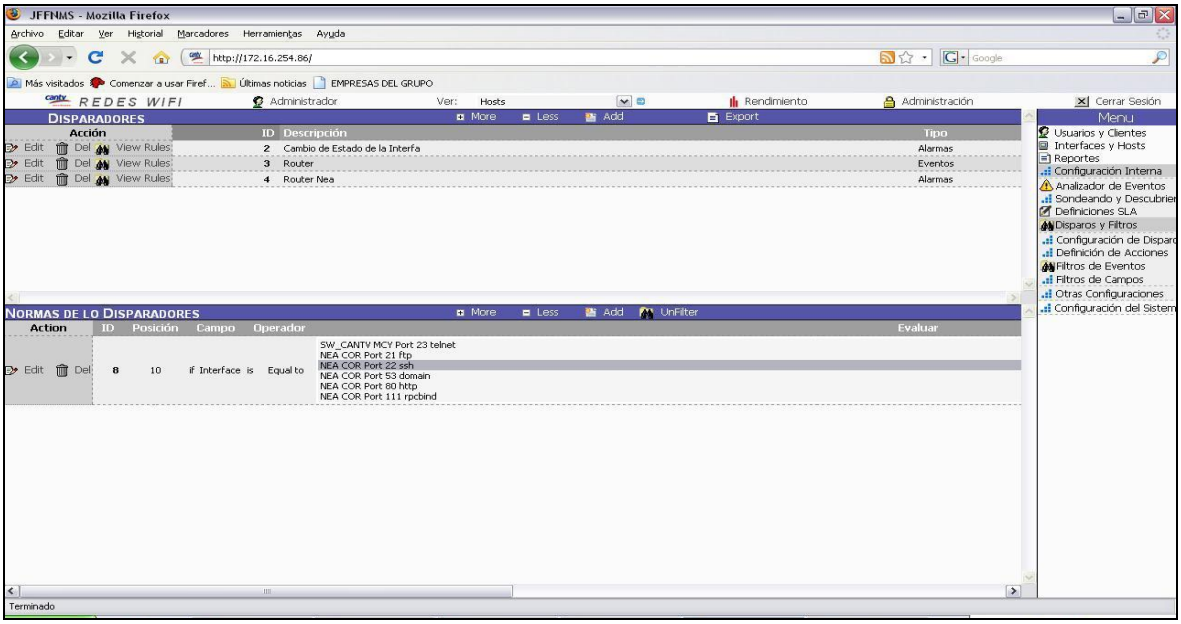

Figura 30: Prototipo en español

d) **Mejoras del Rendimiento del Tráfico de Datos**: Este prototipo ofrece mejoras del tráfico de datos mediante la activación de alarmas con un nivel de gravedad identificado con el color rojo (ver figura 31), que se activa y envía al administrador de red a través de un mensaje vía consola, una vez configurado y agregado la información de un equipo de la red al prototipo da a conocer los eventos encontrados como: capacidad de memoria, retardo de conexión, conexiones establecidas paquetes perdidos y ancho de banda consumido ver en figuras 32 y 33. En el caso del monitoreo de un *router* se procede a cambiar el canal de comunicación ya que por defecto del equipos los datos se transmiten por el canal 2 lo que tuve como consecuencia retardo de conexión en horas donde el trafico es más alto, por ello se habilitó y configuró un nuevo canal de comunicación, lo cual hace se mejore el tráfico de datos.

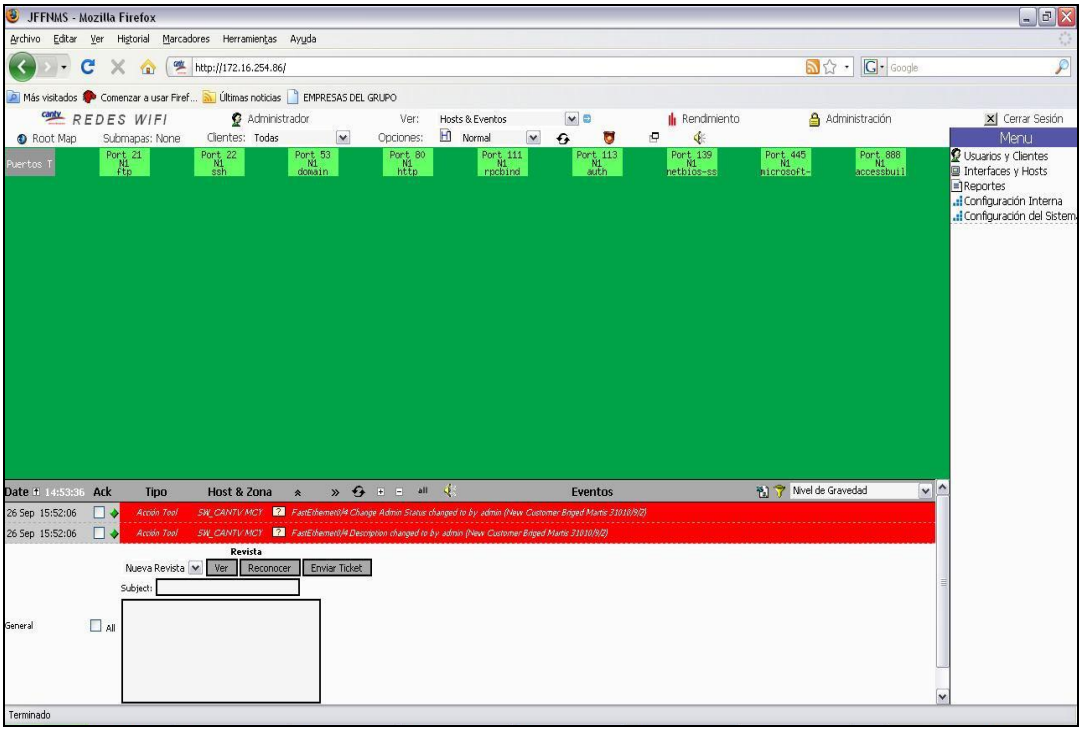

Figura 31. Alarma crítica

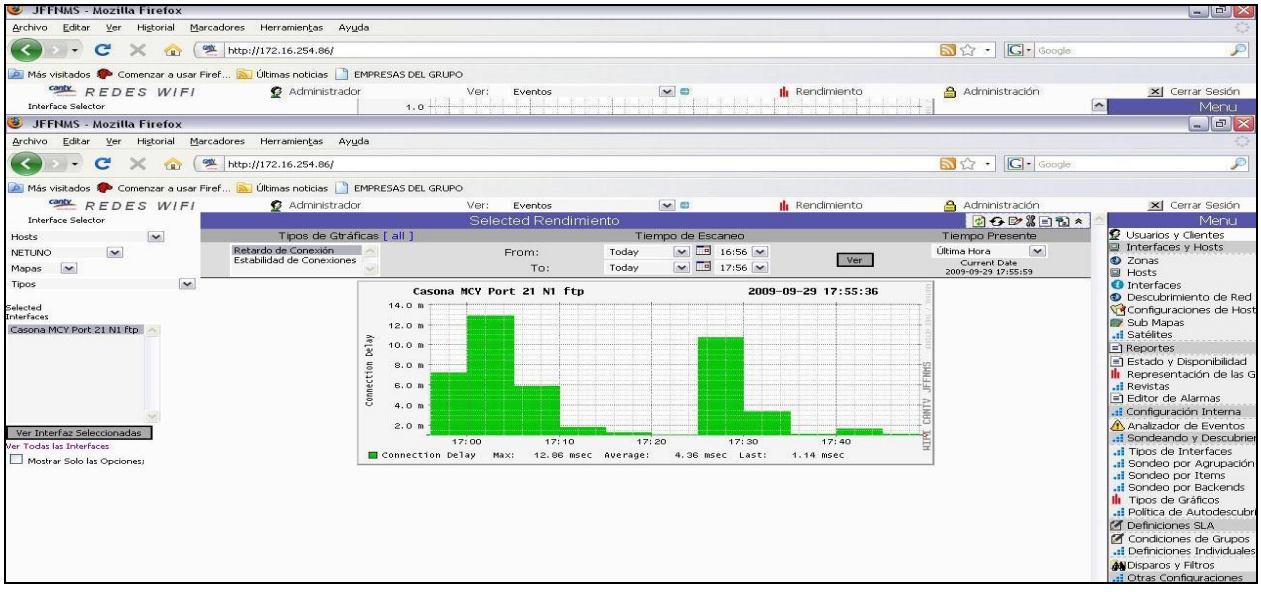

Figura 32. Retardo de conexiones

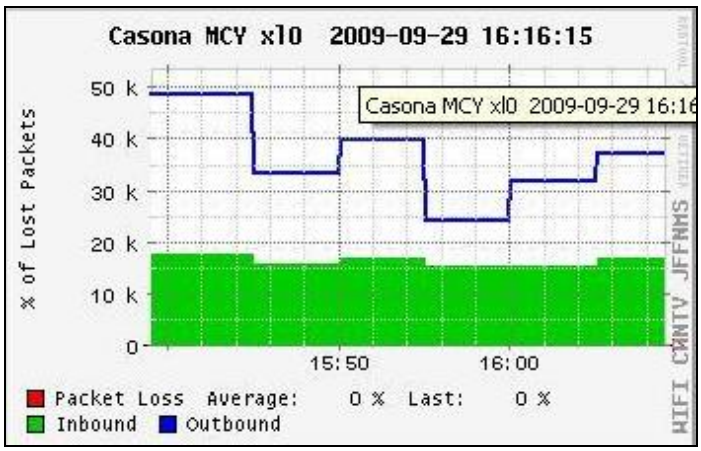

Figura 33. Pérdidas de paquetes.

Cabe destacar que en el momento de realizar dichas pruebas, las interfaces y puertos trabajaron sin ningún problema lo que no generó pérdidas de paquetes.

El sistema de alarmas informa a los administradores el rendimiento de la transmisión de datos, por ello se configuraron los disparadores (*triggers*) los cuales poseen la información necesaria de los *host* y se programan con un tiempo de cada 10 minutos para realizar el monitoreo del trafico y así arrojar la información requerida mediante gráficas, el cual hace más visible y didáctico para los administradores el estudio del tráfico de datos. Así como lo muestran las figuras 34 y figura 35.

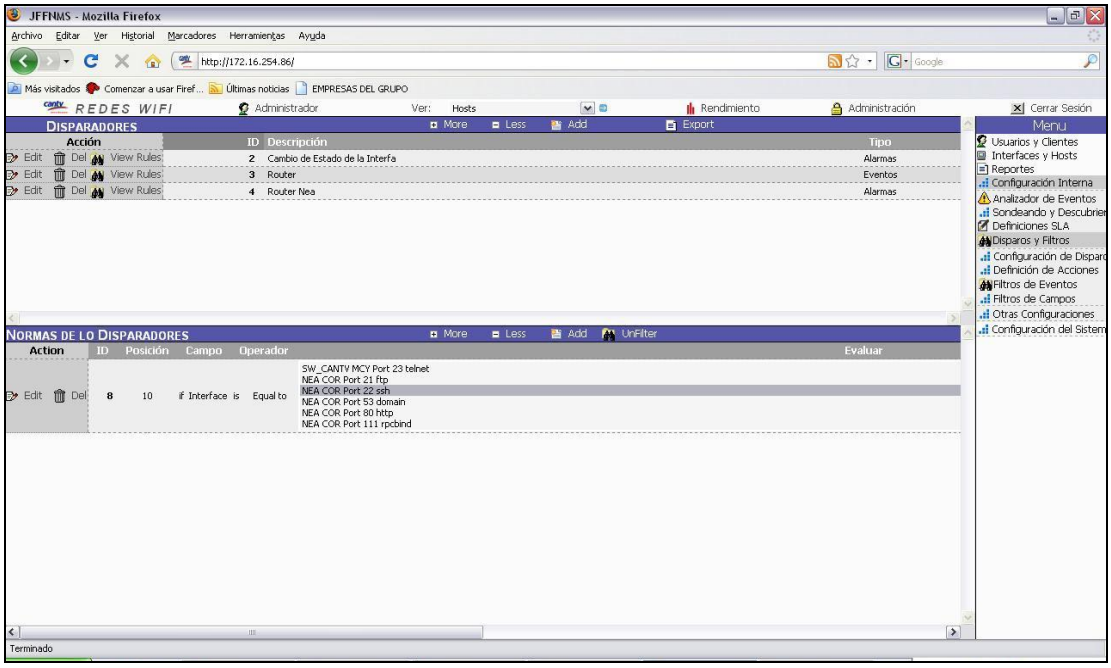

Figura 34: Configuración de disparadores (*triggers*).

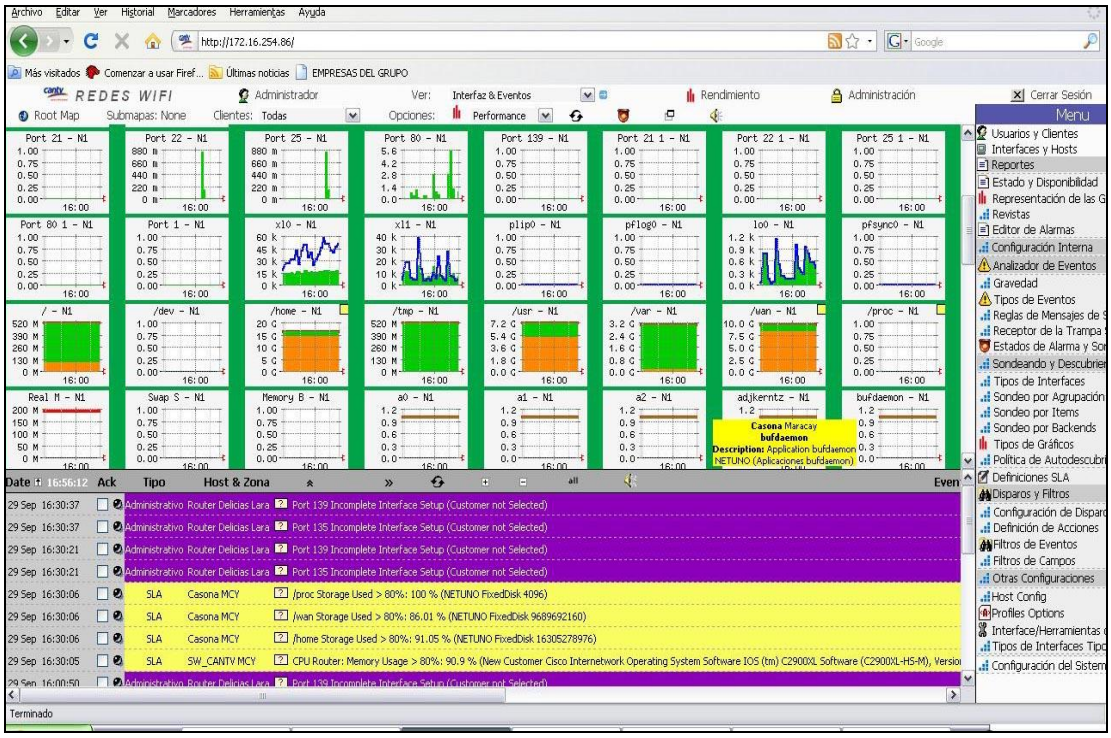

Figura 35. Información de los *host* de manera gráfica y alarmas enviadas.

Para mayor confiabilidad el prototipo de administración y monitoreo realiza el cálculo del promedio de la disponibilidad de las conexiones establecidas en la red, es decir, calcula la disponibilidad total de la conexiones establecidas, ver figuras 36 y 37.

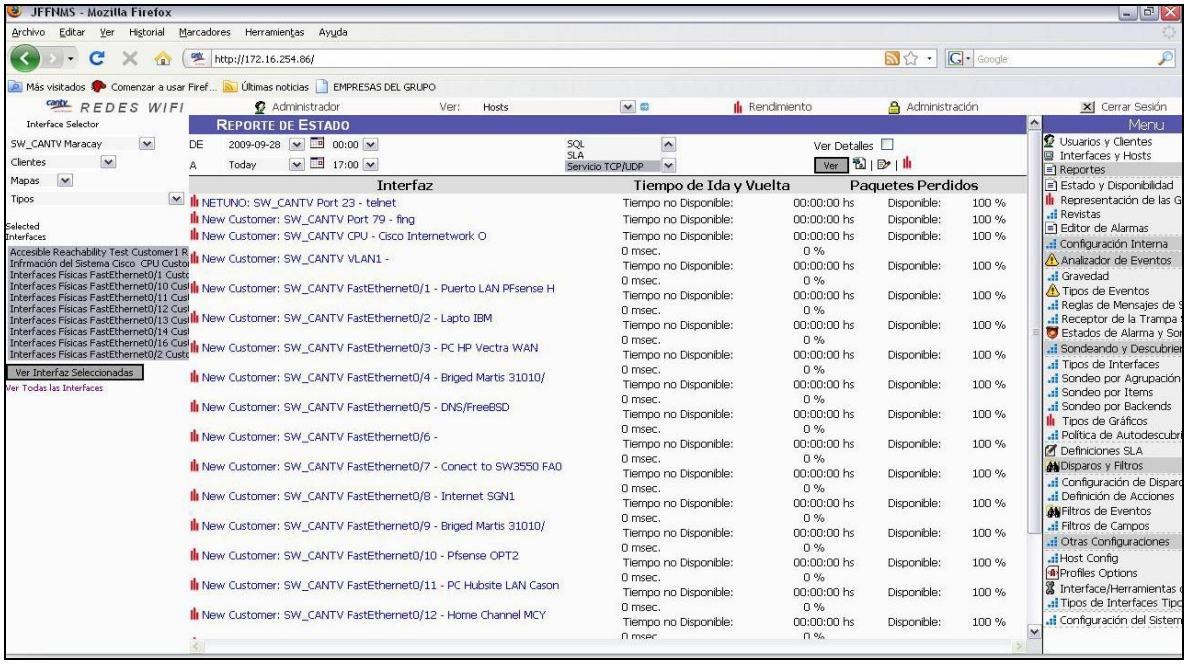

Figura 36. Disponibilidad de la red

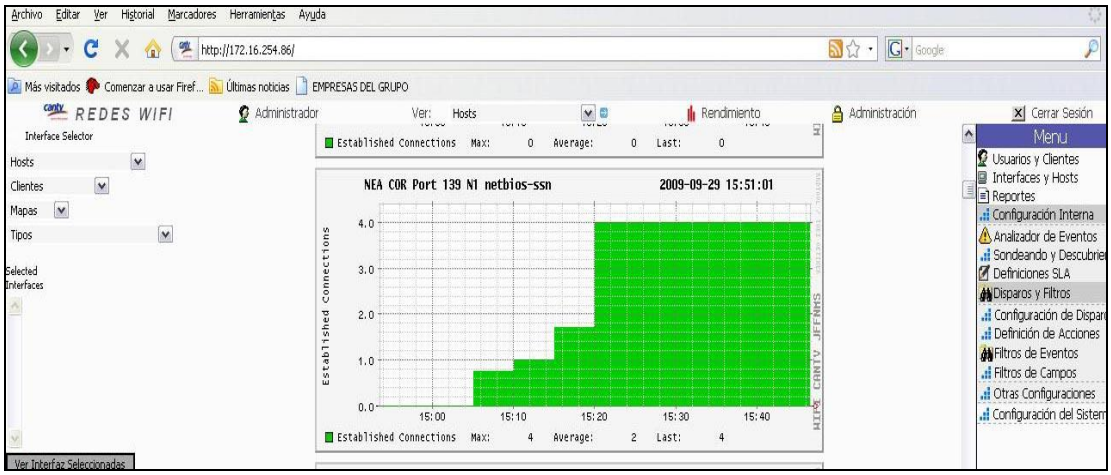

Figura 37: Conexiones establecidas

Para realizar el cálculo del tiempo total disponible, se escanea la base de datos de todas las interfaces existentes en la red o las ya seleccionadas por el administrador para el intervalo de tiempo solicitado. A continuación, se explica de manera detallada la forma de cómo a partir de eventos existentes en la red, el administrador adquiere la información de los equipos y en cual momento se realizaron los eventos y también saber la disponibilidad que tuvo con respecto a las conexiones establecidas. La lista ordenada es escaneada y luego se expresa los resultados de "Interfaces Caídas", el contador se establece inicialmente en 0 y se incrementa cuando al escanear nuevamente la alarma se encuentra abajo y disminuye cuando se encuentra arriba.

Por ejemplo, si hay una serie de eventos para el período de tiempo seleccionado las 10:00 a las 15:00 (normalmente este ciclo se realiza durante todo el día yo tome un margen de 7 horas para explicar el estudio).

En la tabla 5, el contador procesará los acontecimientos en una serie de alarmas que se parecerá a la tabla.

Tabla 5: Ejemplo de lista de eventos de la interfaz

*T*iempo	Interfaz	Estado
10:00hs	A	Abajo
11:00hs	B	Abajo
12:00hs	B	Arriba
13:00hs	C	Abajo
14:00hs	A	Arriba
15:00hs	C	Arriba

Tabla 6: Alarmas transformados a base de ejemplo los acontecimientos

Iniciar	Parar	Duración (horas)	Interfaz
10:00	14:00	4	A
11:00	12:00	1	B
13:00	15:00	2	C

Cuando el informe tiene que trabajar con el tiempo total disponible, no se tiene en cuenta la interfaz particular, sino la afectada por la *Up* o evento de *Down (*ver tabla 6*)*, entonces se utiliza un contador de las interfaces de abajo. Un conteo de 0 significa que el sistema está disponible. El Cuadro muestra el cómo se calcula los tiempos de la disponibilidad de la interfaz. Ver tabla 7.

Tabla 7: Interfaz de Cálculo Estado

Tiempo	Estado	Contador	Notas
00:00hs	Abajo	0	Contador fue de 0 para un tiempo récord como inicio
10:00hs	Abajo	1	
11:00hs	Abajo	2	
12:00hs	Arriba	1	
13:00hs	Abajo	2	
14:00hs	Arriba	1	
15:00hs	Abajo Arriba	0	Ahora es 0 para un tiempo récord como parada de esta interrupción

La disponibilidad no se calculara de alarmas que desde un principio no estén programadas por el administrador, por ello solo se realizara el estudio de aquellas interfaces y puertos ya seleccionados.

La tabla 7, muestra un corte del sistema de 5 horas, comenzando a las 10:00, cuando bajó una interfaz y acabado a las 15:00 cuando C interfaz empiece a funcionar. Usando un método como éste, implica obtener un tiempo total disponible de 5 horas en lugar de 7, ya que 5 horas es el tiempo que las interfaces se estaba caída (*down*).

El tiempo total disponible ahora es fácil de trabajar utilizando el tiempo total disponible y el tiempo total, es decir, el tiempo total se refiere a las 24 horas que la red esta monitoreada por ejemplo:

(24h - 5h) * 100 / 24h = 19 * 100 / 24 = 79.17% (24h - 5h) * 100 / 24 = 19 * 100 / 24 = 79,17%

Así que el tiempo total disponible para nuestro informe es de 5 horas y la disponibilidad total es de 79,19%.

En este caso, los disparadores se ejecutan siempre y cuando el prototipo realice el cálculo de disponibilidad total ya explicado, el cual se compara con el umbral mínima utilizado en CANTV es del 75%, este se compara con el ya calculado, una vez hecho la comparación y resulte éste último menor, se activa la alarma con nivel de gravedad, lo que permite al operador analizar la alarma y así procede a resolver este evento de manera inmediata según lo requiera la falla.

Cabe destacar que se programaron 4 tipos de alarmas según el nivel de gravedad, que son diferenciadas por el color, las programadas son las primeras 4, ver figura 38.

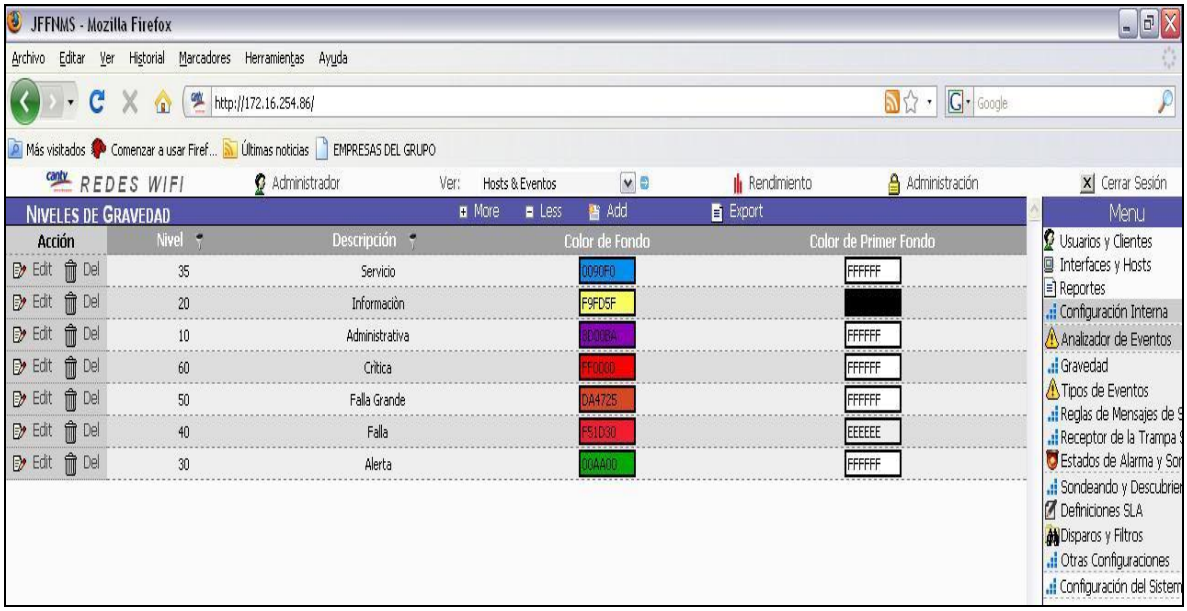

Figura 38: Color de las alarmas según el nivel de gravedad

g) **Desarrollo de Módulos**: Cabe resaltar que este prototipo fue desarrollado bajo el sistema base llamado JFFNMS, que realiza una gestión de rede IP, éste sistema base envía un tipo de alarmas que da la información de no funcionamiento de la interfaz, al JFFNMS se le pudo desarrollar bajo el lenguaje PHP, módulos que generan información detallada de las interfaces y puertos existentes en la red. Los detalles se visualizan mediante gráficas y tablas generados por la bases de datos, y mediante la selección de botones agregados muestra el escaneo de interfaces y eventos alarmados como se muestra en el figura 39. Todo este trabajo fue realizado gracias al estudio de lenguajes de programación y la utilización de protocolos que capturan el tráfico de datos.

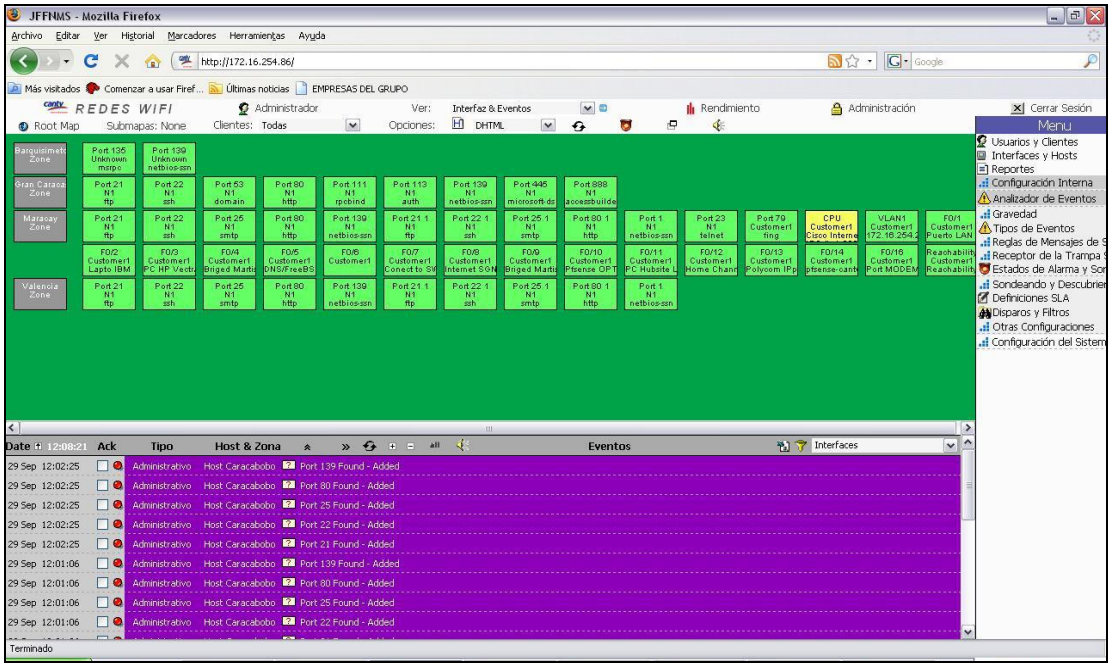

Figura 39: Puertos escaneados y menú con sus principales botones.

6.2 VENTAJAS Y DESVENTAJAS DE SU DESARROLLO EN SOFTWARE LIBRE.

6.2.1 VENTAJAS

1. Una de las ventajas importantes de desarrollar el prototipo en Linux es que a diferencia de otros sistemas operativos, es multitarea real, y multiusuario; posee un esquema de seguridad basado en usuarios y permisos de lectura, escritura y ejecución establecidos sobre los archivos y directorios. Esto significa que cada usuario es propietario de sus archivos, y otro usuario no puede acceder a estos archivos.

2. Esta propiedad no permite el contagio de virus entre archivos de diferentes usuarios y por ende le ofrece a la red la mayor estabilidad por intrusos existentes en la red.

3. Por el hecho de estar desarrollado bajo Linux, el prototipo puede ser modificado para agregarle módulos que requiera el administrador en un determinado momento, sin tener que implementar otro, es decir, evita invertir tiempo en conocer otro tipo de sistema ya que programadores y desarrolladores día a día prestan su colaboración y hace esto posible.

4. Además, cualquier sistema, prototipo o aplicación programada bajo LINUX, permite incorporar una gama de interfaces que le aporta al prototipo desarrollado vistosidad por un lado y facilidad de manejo por otro. Al igual que los entornos gráficos de otros sistemas (Solaris, Apple Mac) X-Windows ofrece un entorno multiventana, pero a diferencia de aquellos, X-Windows supone el núcleo sobre el cual se pueden ejecutar distintos gestores de ventanas.

5. El prototipo diseñado bajo LINUX, utiliza varios formatos de archivo que son compatibles con casi todos los sistemas operativos utilizados en la actualidad.

6. La seguridad de saber qué hace un programa tan sólo viendo el código fuente, o en su defecto, tener la seguridad que está el código disponible.

7. El hecho de que el sistema sea mantenido por una gran comunidad de programadores y usuarios alrededor del mundo, provee una gran velocidad de respuesta ante errores de programas que se van descubriendo, que ninguna compañía comercial de software puede igualar.

6.2.2 DESVENTAJAS

El prototipo por ser desarrollado bajo Linux tiene los siguientes puntos débiles que se enumeran a continuación:

- No es tan fácil administrar para los principiantes, debido al modo de como instalar programas, lo cual se hace a través de la consola donde se ejecutan los diferentes comandos, según la distribución de LINUX que utilices, por ello, es de suma importancia tomar cursos de administración de Linux y así optimizar el tiempo en desarrollar más y no desperdiciarlo en soporte técnico por falta de los conocimientos previos al utilizar este sistema.

- Debido a que todavía algunos fabricantes se muestran reservados para entregar la información de sus dispositivos, el soporte a nuevos dispositivos es un poco más lento que el de otros sistemas operativos.

- Los programas son estructurados en forma monolítica, y las dependencia de uno al otro causa interdependencias a veces difíciles de manejar.

CONCLUSIONES

- La administración de red tiene por objetivo proporcionar herramientas automatizadas y manuales de administración al usuario de red, para que éste pueda detectar posibles fallas o degradaciones en el desempeño de la misma y así permitirle a los operadores obtener mayor cantidad de información de la red, para así realizar el mantenimiento pertinente a los equipos que conforman dicha red. En consecuencia, el presente prototipo desarrollado permite optimizar la infraestructura existente y mejorar el rendimiento de las aplicaciones y servicios.

- Luego de haber trabajado con los comandos que nos proporciona Linux en el ámbito de la administración y monitoreo, se puede decir que este sistema operativo es bastante robusto, estable y rápido, ideal para servidores y aplicaciones distribuidas. Adicionalmente es libre, lo que implica no sólo la gratuidad del software, sino también que es modificable y que tiene una gran cantidad de aplicaciones libres en distintas bibliografías y hasta en el mismo Internet. Y lo más importante aún, ya no está restringido a personas con grandes conocimientos de informática ya que sus desarrolladores han hecho un gran esfuerzo por dotar al sistema de asistentes de configuración con ayuda, además de sistemas gráficos muy potentes. Por ello, su integridad hace confiable la utilización de este sistema operativo en servidores, programas, sistemas entre otros.

- Después de conocer la topología de las redes WIFI de CANTV, nos pudimos dar cuenta de la gran necesidad que tiene la empresa de mantener comunicado a sus usuarios; por lo que requiere de una buena administración y monitoreo de red que permita un mejor manejo y control de los elementos que la conforman. Es decir, este prototipo de administración y monitoreo del tráfico de datos de las redes WIFI bajo el software libre, está desarrollado para brindarles a sus usuarios

servicios de calidad como lo ha hecho a través de los años y cumpliendo por la normativa de la empresa de desarrollar aplicaciones bajo ambiente LINUX.

- Luego de realizar estudios de diferentes sistemas que funcionan bajo Software Libre, para utilizarlo como base de nuestro prototipo a desarrollar, se verificaron las numerosas herramientas que ofrece el sistema operativo de código abierto, de esta manera se consideró la utilización del sistema surge de gestión IP "JFFNMS", debido a la ventaja que tiene de ser programado bajo el lenguaje de programación PHP, lenguaje conocido que permite conseguir sus documentación en múltiples bibliografías e Internet.

- Lo que permitió realizar el prototipo con éxito, fue entre las cosas más importantes, la utilización de comandos como NMAP y con ayuda de varios protocolos como SNMP, que facilitan de gran forma la detección de dispositivos activos presentes en la red. NMAP, además, presenta el listado de direcciones MAC, el tipo y sistema operativo del dispositivo, lo que hace posible el desarrollo de un prototipo de administración y monitoreo del tráfico de datos de las redes WIFI, mediante un modo gráfico y un modo texto que a su vez hace más sencillo captar las información requerida por los administradores de dicha red.

- El diseño del prototipo de administración y monitoreo realizado, facilita el trabajo a los administradores de red, mediante sus resultados gráficos, ya que permite conocer las fallas y el rendimiento de la red de manera ordenada, mediante botones y pestañas de fácil acceso, que permiten la ubicación de la falla a través de las alarmas

- Después de realizar las pruebas y ver el funcionamiento del prototipo se comprobó que cumple con las necesidades de la Gerencia de Planificación de CANTV y que la principal desventaja de LINUX, es que se requiere de un conocimiento medio de los conceptos básicos de este sistema operativo y de

lenguajes de programación. La principal ventaja de realizar el prototipo en LINUX es su integración, es decir, unir en un mismo paquete, múltiple funciones de administración.

RECOMENDACIONES

- Utilizar varios *host* como servidor para las diferentes aplicaciones (FTP, MAIL, DNS, WEB, etc). Esto, con el fin de evitar que todo el tráfico sea dirigido hacia un solo *host* y éste se vea congestionado por la cantidad de información que debe manejar.

- Implementar Calidad de Servicios (QoS) a este prototipo, para así hacer más confiable los resultados obtenidos, de esta manera poder cumplir con un riguroso funcionamiento de los equipos, lo que permite un mejor rendimiento.

- Ampliar la memoria RAM del servidor a 2GB ó 4GB preferiblemente a fin de maximizar su potencialidad.

- Se recomienda utilizar la versión 1 del SNMP, debido que a pesar de las versiones más recientes poseen seguridad, no son compatibles con muchos de los equipos existentes en CANTV, es decir, se sugiere realizar un estudio previo de los equipos

- Al desarrollar aplicaciones bajo software libre, se recomienda trabajar con las versiones de los programas y paqueterías más recientes debido a las actualizaciones que constantemente están sometidos dichos paquetes.

- Hacer un respaldo de la base de datos MySQL cada 3 meses a fin de evitar que se pierda información valiosa por falta de espacio en disco ya que por lo general los equipos poseen más información de lo debido.

REFERENCIAS BIBLIOGRAFICAS

[1] it.aut.uah.es. Gestión De Redes (2004/2005) http://it.aut.uah.es/mar/gestion/tema-2.pdf

[2] info-ab.uclm.es. Mantenimiento y monitorización de redes TCP/IP. www.info-ab.uclm.es/asignaturas/42524/teoria/ar2Tema7x2.pdf

[3] det.uvigo.es. Gestión Y Planificación De Redes Con Sistemas Inteligentes www.det.uvigo.es/~mramos/gprsi/gprsi2.pdf

[4] linuxdata.com.ar. Introducción a la Administración de una Red Local basada en Internet http://www.linuxdata.com.ar/index.php?idmanual=tutorialadmionredss.html-&manuale1

[5] it.aut.uah.es. Gestión y Administración de Redes http://it.aut.uah.es/alarcos/do-cente/garii/5monitorizacion&control.pdf

[6] php.net Lenguaje de programación PHP http://www.php.net/

[7] jffnms.org Gestión de Redes ip http://www.jffnms.org/docs/jffnms.pdf

[8] es.wikipedia.org Protocolos de redes Inalámbricas http://es.wikipedia.org-/wiki/IEEE_802.11

[9] ditec.um.es Gestión de red http://ditec.um.es/laso/docs/tut-tcpip/3376c414.html

[10] luxik.cdi.cz HTB LINUX queuing discipline manual user guide http://luxik.cdi.-cz/~devik/qos/htb/manual/userg.htm

[11] ORTIZ L., Daniel A. Trabajo de Grado Titulado "Evaluación E Implantación De Un Sistema De Monitoreo Para La Red Inalámbrica Del Centro Nacional De Tecnologías De Información Mediante El Uso De Software Libre.". UNEXPO. Caracas, Enero 2008.

[12] Wikipedia.org Protocolos de transmisión de bit http://es.wikipedia.org/wiki/-LAPB

[13] Topología de las redes WIFI de CANTV.

BIBLIOGRAFIA

ARIAS ODON, Fidias. “Tesis & Proyectos de Investigación” Editorial Episteme. Caracas – Venezuela. Mayo 1998

BRUCE, Alexander. "802.11 Wireless Network Site Surveying and Installation" Editoral Cisco System. Febrero 2008

HERNÁNDEZ SAMPIERI, R., Fernández Collado, C. y BAPTISTA LUCIO, P. " Metodología de la investigación**”.** Editorial McGraw-Hill. Segunda edición. México 1991

KRAFFT, Martín F. “Debian System Concepts and Techniques” Editorial No Starch Press, Inc. USA. Septiembre 2005

MAWBEW S, Gast. “802.11 Wireless Networks“. Editorial O'Reilly Media, Inc.; segunda edición. USA. Abril 2005.

MINISTERIO DE CIENCIA Y TECNOLOGIA. ""Libor Amarillo Del Software Libre". Editorial Impresos Caracas segunda edición. Septiembre 2004.

GLOSARIO

ARP: (Address Resolution Protocol). El protocolo de resolución de direcciones es responsable de convertir la dirección de protocolo de alto nivel (direcciones IP) a direcciones de red físicas. El protocolo IP debe conocer la dirección física del dispositivo destino para que la capa de enlace pueda proceder con la transmisión de paquetes IP.

ext2: Sistema de Ficheros Extendido 2. Permite hasta 256 caracteres en los nombres de los ficheros y tamaños de estos de hasta 4 Terabytes.

FTP: .Protocolo de Transferencia de Archivos *(File Transfer Protocol)***.** Es uno de los diversos protocolos de capa aplicación. Es el ideal para transferir grandes bloques de datos por la red.

GNU: Es un proyecto que ha desarrollado un sistema completo de software libre llamado "GNU" (GNU No es Unix) que es compatible con Unix. El proyecto GNU no está limitado a sistemas operativos, si no a proporcionar un amplio espectro de software esto incluye software de aplicación.

HTTP: Protocolo de transferencia de hipertexto (HTTP, HyperText Transfer Protocol) es el protocolo usado en cada transacción de la Web (WWW World Wide Web). El hipertexto es el contenido de las páginas web, y el protocolo de transferencia es el sistema mediante el cual se envían las peticiones de acceso a una página web, y su respuesta, remitiendo la información que se verá en pantalla.

HOST: Son los computadores conectados a la red, que proveen y/o utilizan servicios a/de ella. Los usuarios deben utilizar hosts para tener acceso a la red. En general, los hosts son computadores mono o multiusuario que ofrecen servicios de transferencia de archivos, conexión remota, servidores de base de datos, servidores WWW, etc. Los

usuarios que hacen uso de los hosts pueden a su vez pedir los mismos servicios a otras máquinas conectadas a la red.

ICMP: El Protocolo IP utiliza el protocolo de mensajes de control Internet "ICMP Internet Control Message Protocol" para informar de los errores que pueden ocurrir durante el enrutamiento de paquetes IP. ICMP es realmente una parte integral del protocol IP.

IOS: Sistema de Entrada y Salida (Input Output System). Es el sistema operativo de switches y ruteadores. Al igual que un host, un ruteador o switch no puede funcionar sin un sistema operativo, es decir, el hardware no puede realizar ninguna función.

NetBIOS: Protocolo de red originalmente creado para redes locales de computadoras IBM PC. NetBIOS engloba un conjunto de protocolos de nivel de sesión, que proveen 3 tipos de servicios: Servicio de nombres, Servicio de paquetes y Servicio de sesión.

Nodo: Punto final de la conexión de red o una unión que es común para dos o más líneas de una red. Los nodos pueden ser procesadores, controladores o hosts. Los nodos, que varían en cuanto al enrutamiento y a otras aptitudes funcionales; pueden estar interconectados mediante enlaces y sirven como puntos de control en la red. La palabra nodo a veces se utiliza de forma genérica para hacer referencia a cualquier entidad que tenga acceso a una red y frecuentemente se utiliza de modo indistinto con la palabra dispositivo.

NTP: (Protocolo de Tiempo de Red), Protocolo desarrollado sobre el TCP que garantiza la precisión de la hora local, con referencia a los relojes de radio y atómicos ubicados en la Internet. Este protocolo puede sincronizar los relojes distribuidos en milisegundos durante períodos de tiempo prolongados.

PDU: Es la unidad de datos de protocolo de las capas del modelo ISO/OSI.

PHP: Es un lenguaje de programación interpretado, diseñado originalmente para la creación de páginas web dinámicas.

PLUGINS: Es una aplicación que se relaciona con otra para aportarle una función nueva y generalmente muy específica.

POSIX: (Portable Operating System Interface). Estándar que describe una condición para la fuente del software, debe ser un sistema operativo compatible POSIX, es decir, que sea un sistema portable y ser recompilado con poca dificultad.

PPP: (Point-to-Point Protocol). El protocolo Punto A Punto es un protocolo más reciente y robusto que SLIP, pero cumplen funciones similares.

PROXY: El término *proxy* hace referencia a un programa o dispositivo que realiza una acción en representación de otro. La finalidad más habitual es la del servidor prox*y*, que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.

RRDTOOL: Es una herramienta que trabaja con una base de datos que maneja planificación según Round Robin.

RUTEADOR: Un ruteador es un tipo especial de computador. Cuenta con una CPU, memoria, bus de sistema y distintas interfaces de entrada/salida. Sin embargo, los ruteadores están diseñados para cumplir algunas funciones muy específicas como conectar y permitir la comunicación entre dos redes y determinan la mejor ruta para la transmisión de datos a través de las redes conectadas.

SLIP: (Serial Line Internet Protocol) permite la transmisión de paquetes IP sobre líneas seriales (líneas telefónicas). La información es empaquetada y transmitida en paquetes IP. Trabaja sobre TCP/IP.

SMTP. Simple Mail Transfer Protocol (SMTP), o protocolo simple de transferencia de correo electrónico. Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras y/o distintos dispositivos (PDA's, Celulares, etc).

SWITCH: Un switch (en castellano "interruptor" o "conmutador") es un dispositivo de interconexión de redes de hosts/computadoras que opera en la capa 2 (nivel de enlace de datos) del modelo OSI (Open Systems Interconection). Un switch interconecta dos o más segmentos de red, pasando datos de una red a otra, de acuerdo con la dirección MAC de destino de los datagramas en la red.

TELNET: Terminal de red. Aplicación que permite que un usuario se conecte a otro dispositivo en cualquier parte de la red y actúe como un terminal del mismo.

THROUGHPUT: Tasa de transferencia, rendimiento o throughput, se refiere a la tasa efectiva de bits.

UDP: (Protocolo de Datagrama de usuario). Es un protocolo no orientado a conexión. No proporciona fiabilidad ni mecanismos de control de flujo. No proporcionan procedimientos de recuperación de errores. Protocolos del nivel de aplicación, como el Protocolo de Transferencia de Datos Trivial (TFTP) y la Llamada de Procedimiento Remoto (RPC) utilizan UDP.

XML: Lenguaje Extensible basado en Marcas (Extensible Markup Language). Es un estándar abierto para describir datos. Permite al desarrollador de páginas web definir marcas especiales.