UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y COMUNICACIONES

Tema:

"SISTEMA DE MONITOREO Y CONTROL DE REDES INALÁMBRICAS PARA OPTIMIZACIÓN DEL SERVICIO DE INTERNET EN LA EMPRESA INTERCOMPU"

Trabajo de Graduación. Modalidad: TEMI. Trabajo Estructurado de Manera Independiente, presentado previo la obtención del título de Ingeniero en Electrónica y Comunicaciones.

AUTOR: Carlos Vinicio Ailaca Ramírez

TUTOR: Ing. M.Sc. Marco Jurado

Ambato - Ecuador

Noviembre 2011

APROBACIÓN DEL TUTOR

En mi calidad de tutor del trabajo de investigación sobre el tema: "Sistema de Monitoreo y Control de Redes Inalámbricas para Optimización del Servicio de Internet en la Empresa INTERCOMPU", del señor Carlos Vinicio Ailaca Ramírez, estudiante de la Carrera de Ingeniería en Electrónica y Comunicaciones, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el Art. 16 del Capítulo II Trabajo Estructurado de Manera Independiente, del Reglamento de Graduación para obtener el título terminal de tercer nivel de la Universidad Técnica de Ambato.

Ambato Noviembre, 2011

EL TUTOR

Ing. M.Sc. Marco Jurado

AUTORÍA

El presente trabajo de investigación titulado: "Sistema de Monitoreo y Control de Redes Inalámbricas para Optimización del Servicio de Internet en la Empresa INTERCOMPU". Es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato Noviembre, 2011

Carlos Vinicio Ailaca Ramírez
CC: 180381799-6

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La Comisión Calificadora del presente trabajo conformada por los señores docentes Ing. M.Sc. Geovanni Brito e Ing. M.Sc. Juan Pablo Pallo, revisó y aprobó el Informe Final del trabajo de graduación titulado "Sistema de Monitoreo y Control de Redes Inalámbricas para Optimización del Servicio de Internet en la Empresa INTERCOMPU", presentado por el señor Carlos Vinicio Ailaca Ramírez de acuerdo al Art. 17 del Reglamento de Graduación para obtener el título Terminal de tercer nivel de la Universidad Técnica de Ambato.

Ing. M.Sc. Oswaldo Paredes
PRESIDENTE DEL TRIBUNAL

Ing. M.Sc. Geovanni Brito
DOCENTE CALIFICADOR

Ing. M.Sc. Juan Pablo Pallo
DOCENTE CALIFICADOR

DEDICATORIA:

Dedico éste trabajo a mi familia, en especial a mis padres Yolanda y Carlos que gracias a su infinito amor, esfuerzo y dedicación hoy comparten conmigo este logro. A mis hermanos y hermanas David, Daniel, Verónica y Lissette que motivaron la inspiración para seguir adelante.

Carlos Vinicio Ailaca Ramírez

AGRADECIMIENTO:

Agradezco a mi querida facultad; en particular a sus docentes, por la dedicación en su labor y formación académica impartida; por sus mejores consejos que de seguro me ayudaran a lo largo de mi vida profesional.

A todos quienes confiaron en mí; que en todo momento con su incentivo y aliento, motivaron y brindaron siempre muestras de interés por ver alcanzada la meta que me perfile durante este periodo en mi vida. Gracias por su presencia y apoyo.

A todos muchas gracias.

Carlos Vinicio Ailaca Ramírez

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

Pág.

ÍNDICE DE TABLAS

RESUMEN EJECUTIVO

El proyecto que se detalla en este informe de TEMI tiene como finalidad el realizar un sistema de monitoreo y control para la red tomando en cuenta la seguridad de los enlaces inalámbricos que tiene la empresa Intercompu y cuya información fue desarrollada de la manera siguiente:

PRIMER CAPÍTULO.- Indica la descripción de la situación por la cual ha surgido el problema, buscando los generadores e influencias de sus causas y futuras consecuencias, sus beneficios e involucrados, delimitando además su contenido en espacio y tiempo para luego justificarlo y plantear objetivos que expresen el resultado que se espera alcanzar.

SEGUNDO CAPÍTULO.- El marco teórico nos indica los referentes conceptuales que fundamentan el trabajo desarrollado, dando el soporte teórico-científico orientando a su ejecución.

TERCER CAPÍTULO.- Contiene la metodología mediante la cual se realizó la investigación, describiendo de esta manera todas sus técnicas e instrumentos.

CUARTO CAPÍTULO.- Indica las respuestas de la entrevista realizada al gerente de la empresa sobre la implementación de un sistema de monitoreo y control de redes inalámbricas; así también los resultados de la encuesta realizada a los usuarios de la red.

SEXTO CAPÍTULO.- Señala las conclusiones y recomendaciones que conduce a la búsqueda de una propuesta.

QUINTO CAPÍTULO.- Describe el desarrollo de la propuesta cada una de las etapas necesarias para implementar el sistema de control y monitoreo de red inalámbrica, acoplándose a los requerimientos de la empresa, y buscando la mejora del servicio de Internet en la red de la empresa.

INTRODUCCIÓN

El desarrollo de las tecnologías inalámbricas en el mundo de las comunicaciones ha logrado la optimización de los recursos en una empresa, proporcionando soluciones a varios inconvenientes ya sea por dificultad del entorno en el que se encuentre la empresa o por la ubicación de los equipos terminales.

Las comunicaciones inalámbricas han tenido un logro significativo en la movilidad de los usuarios con el aumento y la popularidad de la Internet, esta tecnología cada vez es más aprovechada a nivel mundial. Sin embargo los problemas de seguridad también se han incrementado, la monitorización y control en redes inalámbricas es un tema que se necesita tener en cuenta en una empresa.

En el Ecuador y particularmente en la ciudad de Ambato, sin lugar a duda la tecnología en las comunicaciones inalámbricas ha ido evolucionando con sus bondades y limitaciones, pero hay que tener en cuenta que debido a la gran acogida por parte de los usuarios, a los nuevos servicios que la Internet ofrece, estos llegarán a saturar la capacidad que tienen los equipos, por lo que es necesario tener un control y monitoreo de las redes inalámbricas en una empresa.

El presente trabajo nos da a conocer el desarrollo del monitoreo y control aplicada a la tecnología inalámbrica su funcionamiento, arquitectura y estándares; así como los sistemas que se deberían incorporar para obtener un óptimo rendimiento en el servicio de Internet. También se llegará a conocer los beneficios que puede brindar el monitoreo y control en lograr la optimización del servicio de Internet en la empresa Intercompu.

CAPÍTULO I

EL PROBLEMA

1.1 Tema

Sistema de monitoreo y control de redes inalámbricas para optimizar el servicio de Internet de la empresa Intercompu.

1.2 Planteamiento del problema

1.2.1 Contextualización

Las comunicaciones inalámbricas cumplen un papel importante en la actualidad, realizando comunicaciones de manera eficiente entre dos puntos; las tecnologías inalámbricas empleadas, la optimización y el control de las transmisiones han proporcionado desde sus inicios soluciones a varios inconvenientes en las redes de comunicación en los mercados internacionales, procurando promover la comunicación en ambientes en donde es difícil el acceso por medio de redes cableadas; pero, durante los últimos 10 años las innovaciones en las nuevas técnicas de transmisión inalámbrica originaron la creación de nuevas tecnologías, cambiando de esta manera los estándares de comunicación; la gran acogida resultante entre los usuarios y empresas que utilizan este servicio inalámbrico, es debido a los excelentes resultados obtenidos en los últimos años; facilitando a las empresas incrementar terminales y equipos de comunicación de última generación sin la necesidad de tener una red cableada, permitiendo una mayor movilidad; sin embargo por el gran avance de la tecnología inalámbrica, aparecieron nuevos retos en materia de monitoreo y control de este tipo de redes. El aumento de redes

inalámbricas integro nuevos problemas como: redes superpuestas opacas, cuellos de botella de rendimiento, puntos únicos de fallo, latencia aumentada; por mencionar algunos de los problemas a los ya existentes propios de la tecnología inalámbrica.

En América del Sur y específicamente en Ecuador la tecnología inalámbrica tiene un uso importante, la disminución de costos en los equipos inalámbricos promueve el cambio de los dispositivos destinados a las redes de comunicación inalámbrica. Las empresas privadas que brindan servicios inalámbricos en el Ecuador llegaron moderadamente mientras que en otros países del mundo donde se encuentra más avanzada la tecnología inalámbrica, los sistemas de comunicación están en una continua evolución. En estos últimos años, la SENATEL[1] ha registrado un incremento de empresas de servicios de valor agregado de Internet, con datos al 31 de diciembre de 2007 existieron 130 empresas que brindaron el servicio en distintas partes del país; hasta la fecha del último registro estadístico en la SENATEL, realizado el 30 de Abril de 2009 se registró 185 empresas. El incremento de empresas que brindan servicios de Internet es notorio, sea esta de manera alámbrica o inalámbrica; la necesidad de ofrecer un servicio de calidad, ha puesto en evidencia los problemas que tiene que ver con la seguridad y controles de las redes, con mayor complejidad en redes de tipo inalámbrico.

En la empresa INTERCOMPU de la ciudad de Ambato, el servicio de los sistemas de comunicación inalámbricos aún son deficientes, a pesar que en el último año se ha tenido un incremento importante en la calidad del servicio, pero sigue aún limitada por la carencia de un adecuado sistema que regule toda la red y específicamente las conexiones inalámbricas; también la inadecuada arquitectura de la red ha causado que los accesos a internet sean aún congestionadas en ciertas horas, consecuentemente bajando la calidad del servicio, la necesidad de una solución a los problemas de red interna y externa de la empresa es evidente; el incremento de los usuarios que utilizan la red inalámbrica y la vulnerabilidad que se presenta en la red ha generado la necesidad de realizar una investigación que se

[1] SENATEL: Secretaria Nacional de Telecomunicaciones

base en encontrar una solución de bajo coste y aceptable rendimiento para la empresa y usuarios de la red.

1.2.2 Análisis critico

La utilización de los sistemas inalámbricos basados en el estándar 802.11 en el país es conocida y en diversas aplicaciones es notoria sus ventajas, y en efecto, el avance tecnológico que ha experimentado el mundo de las comunicaciones inalámbricas ponen al país en un reto tecnológico significativo, comprometiéndonos en la mejora de la calidad de servicios de acceso a Internet para las empresas y los usuarios.

En la ciudad de Ambato, la implementación de las tecnologías inalámbricas por parte de las empresas privadas distribuidoras de servicios de Internet, ha experimentado diversos problemas en el servicio prestado, debido a la naturaleza de las señales inalámbricas; el interés por buscar mejoras en los sistemas de comunicaciones ha sido medianamente tratada, el aumento de la demanda de los usuarios de Internet vía inalámbrica encamina nuevos retos; la preocupación por resolver los problemas como los cuellos de botella debido a la saturación del ancho de banda, bajas en el rendimiento en enlaces inalámbricos, puntos únicos de fallo en la red, latencia aumentada en la transmisión, enfoca la atención al estudio de los controles y el monitoreo de redes inalámbricas.

Un limitante que la empresa tiene presente, por el cual se realiza el estudio de un sistema de control y monitoreo para su implementación en red inalámbrica es el factor económico. La compra de equipos que internamente poseen mecanismos para realizar estas actividades representa un costo considerable; teniendo en cuenta que el avance de la ciencia y tecnología ha hecho que en poco tiempo se requiera actualizar los equipos de comunicación; enfrentando de esta manera la empresa una costosa inversión en equipos con tecnología actual. Considerando los factores expuestos, se hace necesario esta investigación en el campo del monitoreo y control de redes de tipo inalámbrico, encaminado a solucionar los problemas presentes en la red interna y externa de la empresa Intercompu;

mejorando la asignación de anchos de banda y protocolos de Internet en el sistema de comunicación de la red.

1.2.3 Prognosis

En los próximos meses, al no realizarse una investigación que brinde a la empresa Intercompu soluciones novedosas; para la innovación e implementación de un sistema de monitoreo y control de su red interna y externa, teniendo presente el problema que causa la inadecuada asignación de anchos de banda y de protocolos de Internet, en su red inalámbrica, podrían agravarse debido al aumento de la demanda y al inadecuado dimensionamiento de la red; produciendo fugas de información, ingresos no autorizados en su red, pérdida de usuarios que utilizan el servicio de Internet de su red inalámbrica externa; y eventualmente el perjuicio económico que esto conlleva.

1.2.4 Formulación del problema

¿Cómo determinaría un sistema de monitoreo y control de redes inalámbricas para la optimización del servicio de Internet de la empresa Intercompu?

1.2.5 Interrogantes

- ¿Análisis de los sistemas de monitoreo y control en redes inalámbricas?
- ¿Los equipos existentes en la empresa soportarían la mejora en las asignaciones de ancho de banda y protocolos de Internet, utilizando el monitoreo y el control de red interna y externa?
- ¿Qué variaciones se efectuaría en la arquitectura de la red inalámbrica existente para el soporte de banda ancha, con el monitoreo y control de su red?

1.2.6 Delimitación del objeto de investigación

Objeto de estudio: Redes

Este proyecto está enfocado en la investigación de nuevas aplicaciones en el control y monitoreo de la tecnología de redes de comunicación inalámbrica, para

brindar un orden a un mundo congestionado presente en la internet y la transferencia de información; con el fin de mejorar las asignaciones de anchos de banda y protocolos de transmisión, relacionado los inconvenientes que soporta al manipular la naturaleza de las señales y la red, se desarrollará en la empresa Intercompu ubicada en la Avenida Bolivariana 2-13 y Pastaza de la ciudad de Ambato con una duración de seis meses, a partir de la aprobación por parte del Honorable Consejo Directivo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

1.3 Justificación

La investigación del tema se encaminará a la obtención de nueva información respecto de cómo se encuentre la tecnología en monitoreo y control en redes inalámbricas y cuáles son los beneficios que brinda la nueva tecnología inalámbrica para los proveedores y usuarios.

También se podrá estudiar las formas de cómo evitar la inadecuada asignación de anchos de banda y protocolos de Internet, las diferentes formas que los terminales pueden acceder a las conexiones, así como los diferentes dispositivos a emplearse con la tecnología inalámbrica.

Finalmente se podrá determinar los beneficios de la tecnología actual, su convergencia, escalabilidad y mejoras, posibilitándonos tener una amplia visión del alcance de las aplicaciones en las comunicaciones inalámbricas.

1.4 Objetivos de la investigación

1.4.1 Objetivo general

- Implementar un sistema de monitoreo y control de redes inalámbricas para optimizar el servicio de internet de la empresa Intercompu.

1.4.2 Objetivos específicos

- Realizar un estudio sobre la calidad del servicio de Internet entregado por la empresa Intercompu.

- Analizar los distintos sistemas de monitoreo y control para redes inalámbricas seguras.

- Plantear una propuesta que permita optimizar el servicio de internet de la empresa Intercompu mediante la implementación de un sistema de monitoreo y control para redes inalámbricas.

CAPÍTULO II

MARCO TEÓRICO

2.1 Antecedentes investigativos

Previo a la revisión de archivos realizada en la biblioteca de la Facultad de Ingeniería en Sistemas Electrónica e Industrial se encuentra el trabajo de grado modalidad seminario "DISEÑO DE UN PROGRAMA DE MONITOREO Y CONTROL DE CARTERA Y CREDITOS CON PROTOCOLO TCP/IP PARA LA SINCRONIZACIÓN DE LA INFORMACIÓN ENTRE LA FILIAL AMBATO Y LA MATRIZ QUITO DE FUNDACIÓN ECUATORIANA DE DESARROLLO" elaborada por Mario Daniel Vaca Salcedo en septiembre del 2010, una conclusión textualmente indica:

"La evolución de las redes de banda ancha depende de la dinámica competitiva y del desarrollo del mercado en nuestro país, la políticas públicas en las comunicaciones son factores adicionales que influenciaron dicha evolución."

2.2 Fundamentación

2.2.1 Fundamentación legal

En la ciudad de Ambato el 20 de Febrero de 2000 se crea la empresa INTERCOMPU; ubicada en la Avenida Bolivariana 2-13 y Provincia de Pastaza, empresa que durante diez años fue dirigida por el Lic. Pablo Tapia, que después vende todos los derechos a su actual gerente y dueño Lic. Darwin Dávila, realizados todos los trámites pertinentes obtiene el siguiente RUC:

1802393197001 para realizar su actividad económica. Los objetivos de la empresa consisten en:

- Venta y asesoramiento en la adquisición de todas las marcas de equipos de cómputo.
- Instalación de redes estructuradas de datos.
- Soporte técnico en sistemas de impresión de tinta continua.
- Reparación y mantenimiento de equipos de cómputo.
- Prestación y comercialización de servicios de Internet.

Para el cumplimiento de su objetivo social, la empresa podrá realizar toda clase de actos y contratos civiles, mercantiles de cualquier otra índole permitidos por las leyes nacionales, y se rige por la Ley de Fomento de la Pequeña Industria.

2.3 Categorías fundamentales

En la figura 2.1 se puede observar la inclusión entre las variables y su relación:

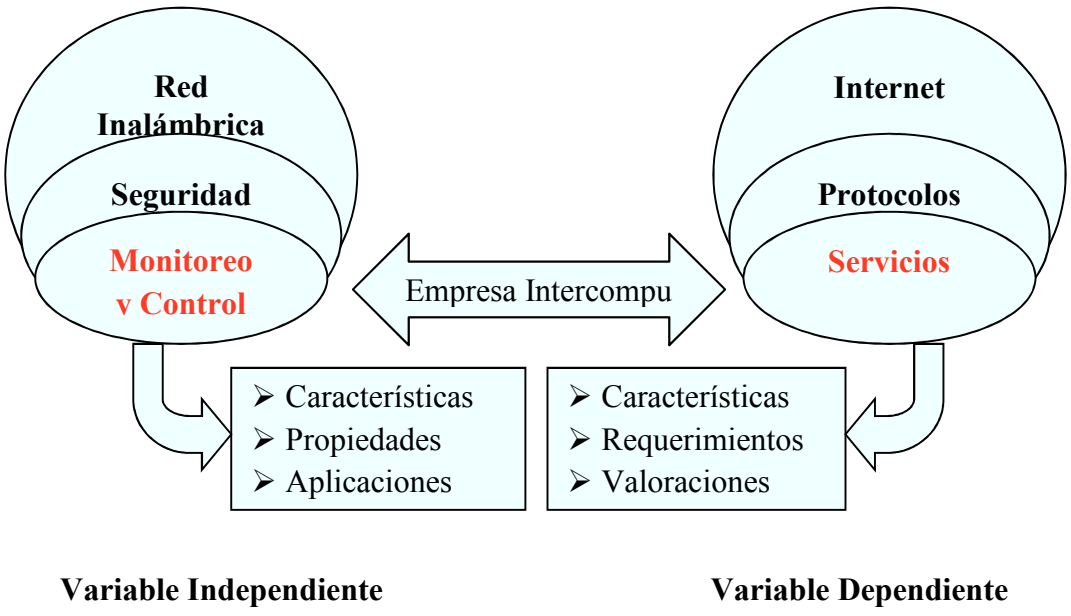


Figura 2.1 Inclusión de variables.
Realizado: Carlos Ailaca

2.3.1 Redes de equipos

En lo elemental, una red de equipos consiste en un conjunto de equipos interconectados entre sí, ya sea por medio de cables o de ondas de radio (Wireless).

El principal propósito de armar una red consiste en que todos los equipos que forman parte de ella se encuentran en condiciones de compartir su información y sus recursos con las demás. De esta manera, se estaría ahorrando dinero, debido a que si se colocara un dispositivo, por ejemplo, una impresora, todas las computadoras de la red podrían utilizarlo.

Los recursos que se pueden compartir en una red son:

- Procesador y memoria RAM, al ejecutar aplicaciones de otras PC.
- Unidades de disco duro.
- Unidades de disco flexible.
- Unidades de CD-ROM/DVD-ROM.
- Impresoras.
- Fax.
- Módem.
- Conexión a Internet.

También es posible compartir la información almacenada en las computadoras conectadas a la red, por ejemplo:

- Ejecución remota de programas de aplicación.
- Bases de datos.
- Documentos en general (archivos de texto, imagen, sonido, video, etc.).
- Directorios (carpetas).

Como ventaja adicional, la instalación de una red ofrece una interfaz de comunicación a todos sus usuarios. Esto se logra por medio de la utilización del correo electrónico, el chat y la videoconferencia.

2.3.1.1 Principales tipos de redes

Las redes de equipos se clasifican en dos grupos, dependiendo de su tamaño y función tenemos.

Red de área local (LAN, Local Area Network)

La Red de área local es el bloque básico de cualquier red de equipos. Una LAN puede ser muy simple (dos equipos conectados con un cable) o compleja (cientos de equipos y periféricos conectados dentro de una gran empresa). La característica que distingue a una LAN es que está confinada a un área geográfica limitada, ya sea en la misma habitación, en diferentes pisos de un edificio como se muestra en la figura 2.2 o en edificios muy cercanos, lográndose extender 200 metros, o con repetidores podría llegar hasta la distancia de un 1 kilómetro. Las LAN proveen una excelente velocidad de transferencia, que va desde los 10 Mbps hasta los 1000 Mbps. Esto se debe a la corta distancia existente entre sus terminales evitando así las interferencias.

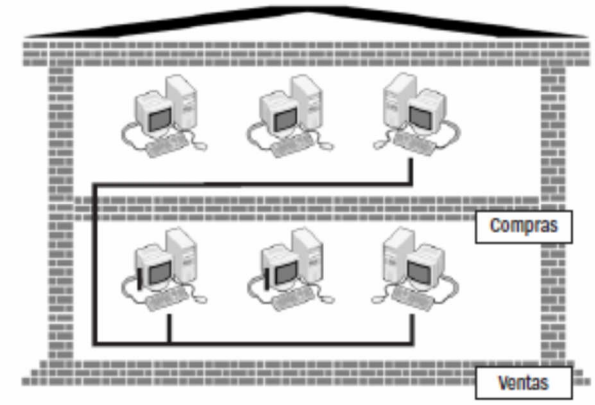


Figura 2.2 Esquema de una red LAN.
Fuente: http://www.redsinfronteras.org/pdf/redes_wireless.pdf

Red de área extensa (WAN, Wide Area Network)

Red de área extensa no tiene limitaciones geográficas. Puede conectar equipos y otros dispositivos situados en extremos opuestos del planeta. Esta peculiaridad las hace más proclives a las interferencias, lo cual disminuye su velocidad de transferencia a 30 Mbps. Una WAN consta de varias LAN interconectadas; por lo general, utilizando la línea telefónica para conectarse entre sí. Podemos ver a Internet como la WAN suprema. No obstante, las empresas de mayor envergadura

unen las computadoras que forman parte de la red mediante una conexión satelital para conectar como se observa en la figura 2.3, por ejemplo, a sucursales situadas en diferentes países.

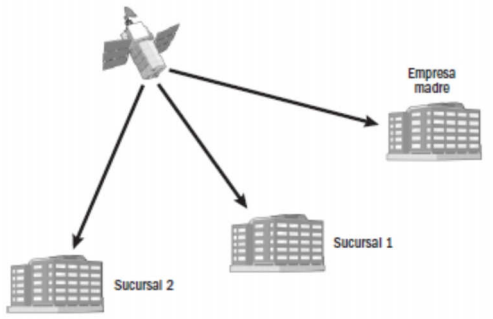


Figura 2.3 Esquema de una red WAN.
Fuente: http://www.redsinfronteras.org/pdf/redes_wireless.pdf

2.3.1.2 Configuración de redes

Por lo general, todas las redes tienen ciertos funciones y componentes comunes en las que pueden estar inmersos; equipos servidores, equipos clientes, el medio de comunicación, datos compartidos, impresoras y otros periféricos compartidos y en definitiva, cualquier recurso; pero, a pesar de tener estas similitudes las redes se dividen en dos categorías principales:

Redes Trabajo en Grupo

En una red Trabajo en Grupo, no hay servidores dedicados, y no existe una jerarquía entre los equipos. Todos los equipos son iguales, y por tanto son pares (peer). Cada equipo actúa como cliente y servidor, y no hay un administrador responsable de la red completa. El usuario de cada equipo determina los datos de dicho equipo que van a ser compartidos en la red.

- **Tamaño.** Las redes Trabajo en Grupo (peer-to-peer) se llaman también grupos de trabajo (workgroups). El término "grupo de trabajo" implica un pequeño grupo de personas. Generalmente, una red Trabajo en Grupo abarca un máximo de diez equipos.
- **Coste.** Las redes Trabajo en Grupo son relativamente simples. Como cada equipo funciona como cliente y servidor, no hay necesidad de un potente servidor central o de los restantes componentes de una red de alta capacidad.

Las redes Trabajo en Grupo pueden ser más económicas que las redes basadas en servidor.

- **Sistemas operativos.** En una red punto a punto, el software de red no requiere el mismo tipo de rendimiento y nivel de seguridad que el software de red diseñado para servidores dedicados. Los servidores dedicados sólo funcionan como servidores, y no como clientes o estaciones. Las redes Trabajo en Grupo están incorporadas en muchos sistemas operativos. En estos casos, no es necesario software adicional para configurar una red Trabajo en Grupo.
- **Implementación.** En entornos típicos de red, una implementación Trabajo en Grupo ofrece las siguientes ventajas: Los equipos están en las mesas de los usuarios, los usuarios actúan como sus propios administradores, y planifican su propia seguridad y los equipos de la red están conectados por un sistema de cableado simple, fácilmente visible.

Redes basadas en servidor

En un entorno con más de 10 usuarios, una red Trabajo en Grupo (con equipos que actúen a la vez como servidores y clientes) puede que no resulte adecuado. Por tanto, la mayoría de las redes tienen servidores dedicados. Un servidor dedicado es aquel que funciona sólo como servidor, y no se utiliza como cliente o estación, Los servidores se llaman *dedicados* porque no son a su vez clientes, y porque están optimizados para dar servicio con rapidez a peticiones de clientes de la red, y garantizar la seguridad de los archivos y directorios. Las redes basadas en servidor se han convertido en el modelo estándar para la definición de redes.

A medida que las redes incrementan su tamaño (y el número de equipos conectados y la distancia física y el tráfico entre ellas crece), generalmente se necesita más de un servidor. La división de las tareas de la red entre varios servidores asegura que cada tarea será realizada de la forma más eficiente posible.

Los servidores para grandes redes se han especializado para adaptarse a las necesidades de los usuarios. A continuación se dan ejemplos de los diferentes tipos de servidores incluidos en muchas redes de gran tamaño.

- Servidores de archivos e impresión.
- Servidores de aplicaciones.
- Servidores de correo.
- Servidores de fax.
- Servidores de comunicaciones.
- Servidores de servicios de directorio.

Ventajas de redes basadas en servidor

Aunque resulta más compleja de instalar, gestionar y configurar, una red basada en servidor tiene muchas ventajas sobre una red simple Trabajo en Grupo.

- **Compartir recursos.** Un servidor está diseñado para ofrecer acceso a muchos archivos e impresoras manteniendo el rendimiento y la seguridad de cara al usuario. La compartición de datos basada en servidor puede ser administrada y controlada de forma centralizada. Como estos recursos compartidos están localizados de forma central, son más fáciles de localizar y mantener que los recursos situados en equipos individuales.
- **Seguridad.** La seguridad es a menudo la razón primaria para seleccionar un enfoque basado en servidor en las redes. En un entorno basado en servidor, hay un administrador que define la política y la aplica a todos los usuarios de la red, pudiendo gestionar la seguridad.
- **Copia de seguridad.** Las copias de seguridad pueden ser programadas varias veces al día o una vez a la semana, dependiendo de la importancia y el valor de los datos. Las copias de seguridad del servidor pueden programarse para que se produzcan automáticamente, de acuerdo con una programación determinada, incluso si los servidores están localizados en sitios distintos de la red.
- **Redundancia.** Mediante el uso de métodos de copia de seguridad llamados sistemas de redundancia, los datos de cualquier servidor pueden ser duplicados y mantenidos en línea. Aun en el caso de que ocurran daños en el área primaria de almacenamiento de datos, se puede usar una copia de seguridad de los datos para restaurarlos.

- **Número de usuarios.** Una red basada en servidor puede soportar miles de usuarios. Este tipo de red sería, imposible de gestionar como red Trabajo en Grupo, pero las utilidades actuales de monitorización y gestión de la red hacen posible disponer de una red basada en servidor para grandes cifras de usuarios.
- **Hardware.** El hardware de los equipos cliente puede estar limitado a las necesidades del usuario, ya que los clientes no necesitan la memoria adicional (RAM) y el almacenamiento en disco necesarios para los servicios de servidor.

2.3.1.3 Topologías de Redes

La topología en una red es definida por la estructura de distribución y la forma de interconexión que tienen las redes. Existen dos tipos de topologías:

Topología Física

La topología física consiste en la configuración o disposición del cableado, dispositivos y equipos de comunicación.

La forma en que se distribuye los elementos de una red, pueden ser utilizado para categorizarlas. De acuerdo a la configuración dispuesta por el cableado se puede conseguir diferentes clases de redes según su topología física. Las cuales se describe a continuación:

- **Bus.** En esta tipología, los elementos que constituyen la red se disponen linealmente, es decir, en serie y conectados por medio de un cable; el bus. Las tramas de información emitidas por un nodo (terminal o servidor) se propagan por todo el bus(en ambas direcciones), alcanzado a todos los demás nodos. Cada nodo de la red se debe encargar de reconocer la información que recorre el bus, para así determinar cual es la que le corresponde, la destinada a él.
- **Anillo.** En la topología tipo anillo los nodos de la red se disponen en un anillo cerrado conectado a él mediante enlaces punto a punto. La información describe una trayectoria circular en una única dirección y el

nodo principal es quien gestiona los conflictos entre nodos al evitar la colisión de tramas de información. En este tipo de topología, un fallo en un nodo afecta a toda la red.

- **Estrella.** Para la topología tipo estrella todos los nodos se conectan a un punto central común, usualmente se usa equipos como un hub o switch para la conexión.
- **Estrella extendida.** En este tipo de topología estrella extendida se enlazan las estrellas conectando los switches de estas a un switch central.
- **Topología Jerárquica.** Mientras la topología jerárquica es muy similar a la estrella extendida pero en lugar de interconectar switches se hace a través de hubs.
- **Mallas.** Se configura una malla cuando cada host es conectado a todos los otros, existiendo de esta manera múltiples caminos de un nodo a otro. Este tipo de configuración se utiliza por lo general donde es indispensable que no exista interrupciones en la comunicación de un nodo y otro.

Topología Lógica

La topología lógica especifica cómo los datos fluyen a través de la red. Para la topología lógica de las redes, es importante la manera en cómo los hosts se comunican a través de medio físico. Las dos topologías lógicas más utilizadas son:

- **Topología broadcast (difusión).** Para la topología broadcast el host envía sus datos a todos los otros hosts conectados al medio físico de la red. No existe un orden en la transmisión de datos. El primero en acceder al medio es el primero en transmitir. Por ejemplo: Ethernet.
- **Topología token passing (pase de testigo).** En la topología token passing se controla el acceso al medio utilizando un testigo electrónico que se pasa a cada host. Cuando un host recibe el testigo puede transmitir datos si los tiene. Si no, entonces pasa el testigo al siguiente host.

2.3.1.4 Modos de transmisión en redes

Según la direccionalidad de los datos en la transmisión un canal de comunicaciones se puede tener tres clases de transmisiones, que son las siguientes:

- **Simplex.** Es aquella transmisión unidireccional, entre un nodo que transmite y otro recibe. Una estación siempre actúa como fuente y la otra siempre como colector, este método permite la transmisión de información en un único sentido.
- **Half-duplex.** Es la transmisión que en determinado tiempo, una estación A actúa como fuente y otra estación B actúa como colector, y en el momento siguiente, la estación B actuará como fuente y la estación A como colector. Permitiendo la transmisión en ambas direcciones, aunque en momentos diferentes. Teniendo comunicaciones bidireccionales, en donde sólo un nodo transmite a la vez.
- **Duplex.** Es la transmisión entre dos estaciones A y B; que actúan como fuente y colector, transmitiendo y recibiendo información simultáneamente, y donde los nodos pueden transmitir datos bidireccionales al mismo tiempo. Este tipo de comunicación se lo puede observar en las redes telefónicas.

2.3.2 ¿Qué son las redes inalámbricas?

Las redes inalámbricas son aquéllas que carecen de cables. Gracias a las ondas de radio, se lograron redes de computadoras de este tipo, aunque para su creación se requirió varios años de búsqueda.

Esta tecnología facilita en primer lugar el acceso a recursos en lugares donde se imposibilita la utilización de cables, como zonas rurales poco accesibles. Además, estas redes pueden ampliar una red ya existente y facilitar el acceso a usuarios que se encuentren en un lugar remoto, sin la necesidad de conectar sus computadoras a un hub o a un switch por intermedio de cables. Estos usuarios podrían acceder a la red de su empresa o a la computadora de su casa en forma inalámbrica, sin configuraciones adicionales.

2.3.2.1 Infraestructura de la red inalámbrica

La siguiente lista presenta los requerimientos mínimos para la implementación de una red inalámbrica WiFi:

- Un router wifi o un punto de acceso (necesarios únicamente en el modo infraestructura).
- Una o más tarjetas WiFi (por lo general se conectan a un puerto USB, PCI o PCMCIA). También existen adaptadores Ethernet / WiFi que son utilizados especialmente para las consolas de videojuegos que solo disponen de un puerto Ethernet.

Estos dispositivos corresponden a una norma. Actualmente, la más común es la 802.11g pero las tarjetas o routers 802.11b son compatibles con hardware más reciente. La norma 802.11b permite una velocidad teórica máxima de 11 Mbps y la 802.11g de 54 Mbps. También existe la norma 802.11g+, que funciona a una velocidad de 108 Mbps.

Si utilizamos diferentes normas, entonces la velocidad máxima será la más baja, o sea la de la norma 802.11b. También existe la norma 802.11a que no es compatible con las otras dos pero que se supone maneja mejor las zonas densas en conexiones inalámbricas WiFi.

2.3.2.2 Topologías y configuraciones en redes inalámbricas

La versatilidad y flexibilidad de las redes inalámbricas es el motivo por el cual la complejidad de una LAN implementada con ésta tecnología sea tremendamente variable. Esta gran variedad de configuraciones ayuda a que este tipo de redes se adapte a casi cualquier necesidad.

Una red inalámbrica puede funcionar de dos modos:

- Modo Ad-Hoc.
- Modo Infraestructura

A continuación se detalla estos modos de funcionamiento.

El modo Ad-Hoc

También conocidas como redes peer to peer (punto a punto), es la configuración más sencilla, ya que en ella los únicos elementos necesarios son terminales móviles equipados con los correspondientes adaptadores para comunicaciones inalámbricas.

En este tipo de redes, el único requisito deriva del rango de cobertura de la señal, ya que es necesario que los terminales móviles estén dentro de este rango para que la comunicación sea posible. Por otro lado, estas configuraciones son muy sencillas de implementar y no es necesario ningún tipo de gestión administrativa de la red.

Un ejemplo sencillo de esta configuración se muestra en la figura 2.4.

Figura 2.4 Conexión peer to peer.
Fuente: http://multingles.net/docs/Manual%20-%20Redes%20WiFi%20inalambricas.pdf

El modo Infraestructura

Con este modo, la gestión está centralizada en un *Punto de Acceso*, esta configuración utiliza el concepto de celda, ya utilizado en otras comunicaciones inalámbricas, como la telefonía móvil. Así los datos que un equipo emite llegan al punto de acceso y éste los transfiere a los otros miembros de la red; de este modo se economiza el ancho de banda.

Una celda podría entenderse como el área en el que una señal radioeléctrica es efectiva. A pesar de que en el caso de las redes inalámbricas esta celda suele tener un tamaño reducido, mediante el uso de varias fuentes de emisión es posible combinar las celdas de estas señales para cubrir de forma casi total un área más extensa.

La estrategia empleada para aumentar el número de celdas, y por lo tanto el área cubierta por la red, es la utilización de los llamados puntos de acceso, que funcionan como repetidores, y por tanto son capaces de doblar el alcance de una red inalámbrica, ya que ahora la distancia máxima permitida no es entre estaciones, sino entre una estación y un punto de acceso.

Los puntos de acceso mostrado en la figura 2.5 son colocados normalmente en alto, pero solo es necesario que estén situados estratégicamente para que dispongan de la cobertura necesaria para dar servicio a los terminales que soportan.

Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos de metros.

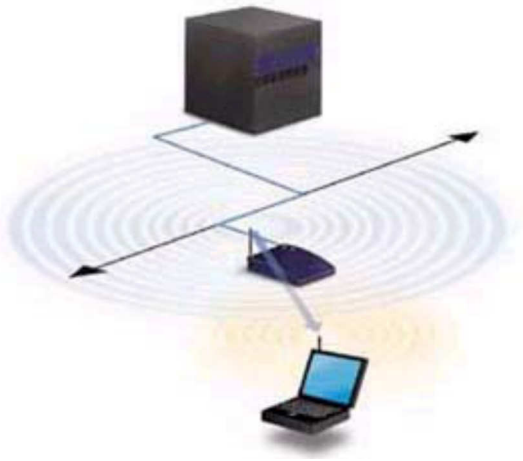


Figura 2.5 Utilización de un punto de acceso.
Fuente: http://multingles.net/docs/Manual%20-%20Redes%20WiFi%20inalambricas.pdf

La técnica de punto de acceso es capaz de dotar a una red inalámbrica de muchas más posibilidades. Además del evidente aumento del alcance de la red, ya que la utilización de varios puntos de acceso como se muestra en la figura 2.6, y por lo tanto del empleo de varias celdas que colapsen el lugar donde se encuentre la red, permite lo que se conoce como *roaming*, es decir que los terminales puedan moverse sin perder la cobertura y sin sufrir cortes en la comunicación. Esto representa una de las características más interesantes de las redes inalámbricas.

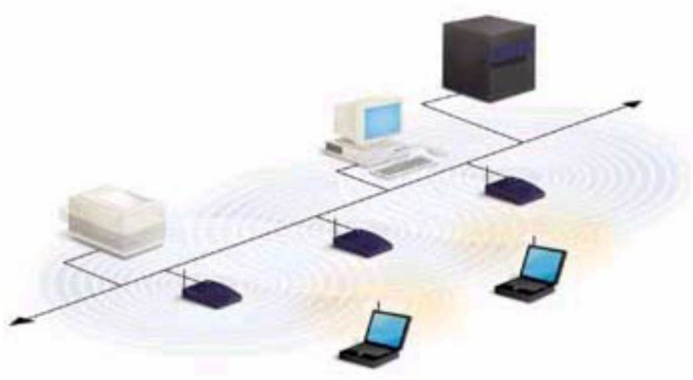


Figura 2.6 Utilización de varios Puntos de acceso. Terminales con capacidad de roaming.
Fuente: http://multingles.net/docs/Manual%20-%20Redes%20WiFi%20inalambricas.pdf

Las posibilidades de las redes inalámbricas pueden verse ampliadas gracias a la interconexión con otras redes, sobre todo con redes alámbricas. De esta forma los recursos disponibles en ambas redes se amplían.

Interconexión de redes

La interconexión de redes se la realiza mediante el uso de antenas (direccionales u omnidireccionales) es posible conectar dos redes separadas por varios cientos de metros como se observa en la figura 2.7, como por ejemplo dos redes locales situadas en dos edificios distintos. De esta forma, una LAN no inalámbrica se beneficia de la tecnología inalámbrica para realizar interconexiones con otras redes, que de otra forma serían más costosas, o simplemente imposibles

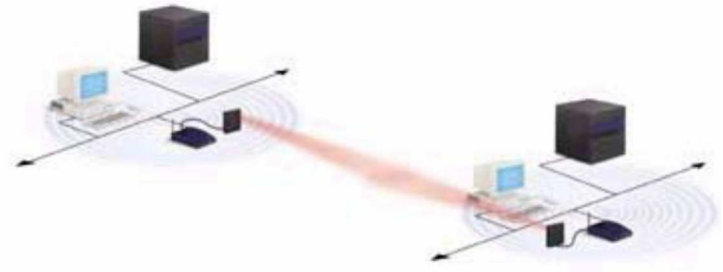


Figura 2.7 Interconexión de LAN mediante antenas direccionales.
Fuente: http://multingles.net/docs/Manual%20-%20Redes%20WiFi%20inalambricas.pdf

2.3.3 Seguridad de red inalámbrica

2.3.3.1 Infraestructura adaptada

Durante la instalación de una red inalámbrica lo primero que se hace es ubicar el punto de acceso en un lugar razonable dependiendo del área de cobertura que se desee. Sin embargo, es común que el área cubierta sea más grande que lo deseado. En este caso es posible reducir la señal de la terminal de acceso para que su rango de transmisión concuerde con el área de cobertura.

La capacidad de adaptiva a las áreas que se desea que sean cubiertas; aumentando o disminuyendo la potencia de la señal, sería lo más adecuado; sin embargo, no muchos dispositivos disponen de esta propiedad de controlar la potencia de la señal.

2.3.3.2 ¿Cómo evitar el uso de valores predeterminados?

Cuando se instala un punto de acceso por primera vez, se configura con ciertos valores predeterminados, en la que está incluida la contraseña del administrador. Muchos administradores principiantes suponen que como la red ya está funcionando, no tiene sentido cambiar la configuración del punto de acceso. Sin embargo, las configuraciones predeterminadas brindan sólo un nivel de seguridad mínimo. Por esta razón, es vital registrarse en la interfaz de administración (casi siempre a través de una interfaz Web o al usar un puerto en particular en el terminal de acceso) para establecer especialmente una contraseña administrativa.

Además, para conectarse a un punto de acceso es necesario conocer el identificador de red (SSID). Por ello se recomienda cambiar el nombre predeterminado de la red y desactivar la transmisión del nombre en la red. Cambiar el identificador de red predeterminado es muy importante, ya que de lo contrario puede brindarles a los hackers información sobre la marca o el modelo del punto de acceso que se está usando.

2.3.3.3 Filtrado de direcciones MAC (Media Access Control)

Todo adaptador de red (término genérico para la tarjeta de red) tiene su propia dirección física (denominada dirección MAC). Esta dirección está representada por 12 dígitos en formato hexadecimal divida en grupos de dos dígitos separados por guiones.

Las interfaces de configuración de los puntos de acceso les permiten, por lo general, mantener una lista de permisos de acceso (llamada ACL[2]; Lista de control de acceso) que se basa en las direcciones MAC de los dispositivos autorizados para conectarse a la red inalámbrica.

Esta precaución algo restrictiva le permite a la red limitar el acceso a un número dado de equipos. Sin embargo, esto no soluciona el problema de la seguridad en las transferencias de datos.

2.3.3.4 WEP (Wired Equivalent Privacy)

Para solucionar los problemas de seguridad de transferencia en redes inalámbricas, el estándar 802.11 incluye un sencillo mecanismo de cifrado llamado WEP (Privacidad Equivalente al Cableado).

WEP es un protocolo de cifrado de trama de datos 802.11 que utiliza el algoritmo simétrico RC4[3] con claves de 64 bits o 128 bits. El concepto de WEP consiste en establecer una clave secreta de 40 ó 128 bits con antelación. Esta clave secreta se debe declarar tanto en el punto de acceso como en los equipos cliente. La clave se usa para crear un número que parece aleatorio y de la misma longitud que la trama de datos. Cada transmisión de datos se cifra de la siguiente manera. Al utilizar el número que parece aleatorio como una "máscara", se usa una operación "O excluyente" para combinar la trama y el número que parece aleatorio en un flujo de datos cifrado.

La clave de sesión que comparten todas las estaciones es estática, es decir que para poner en funcionamiento un número elevado de estaciones inalámbricas,

[2] ACL: Siglas en inglés, Access Control List es un concepto de seguridad informática usado para fomentar la separación de privilegios.
[3] RC4: Sistema de cifrado de flujo (Stream cipher)

éstas deben configurarse con la misma clave de sesión. Por lo tanto, con sólo saber la clave se pueden descifrar las señales.

Además, para la inicialización se usan sólo 24 bits de la clave, lo que implica que sólo 40 de 64 bits o 104 de 128 bits de la clave se utilizan realmente para el cifrado.

En el caso de una clave de 40 bits, con un ataque de fuerza bruta (que prueba todas las claves posibles) una persona dedicada a filtrase en las redes puede encontrar la clave de sesión con rapidez. Asimismo, una falla detectada por Fluhrer, Mantin y Shamir en la generación del flujo que parece aleatorio permite que se descubra la clave de sesión al almacenar y analizar de 100 MB a 1 GB de tráfico.

Por lo tanto, el WEP no garantiza verdaderamente la privacidad de los datos. Sin embargo, se recomienda utilizar al menos una clave WEP de 128 bits para garantizar un nivel de privacidad mínimo. Esto puede reducir el riesgo de una intrusión en un 90 por ciento.

2.3.3.5 ¿Cómo mejorar la autenticación?

Para administrar la autenticación, autorización y contabilidad (AAA) de manera más eficaz, se puede usar un servidor RADIUS (Servicio de usuario de acceso telefónico de autenticación remota). El protocolo RADIUS (definido por la RFC 2865 y la 2866) es un sistema cliente/servidor que permite administrar de manera central cuentas de usuarios y permisos de acceso relacionados.

2.3.3.6 VPN (Virtual Private Network)

Para todas las comunicaciones que requieran un alto nivel de seguridad, es mejor utilizar un cifrado cerrado de datos al instalar una red privada virtual (VPN).

La VPN no es más que una estructura de red corporativa implantada sobre una red de recursos de carácter público (Internet), pero que utiliza el mismo sistema de gestión y las mismas políticas de acceso que se usan en las redes privadas; en sí, no es más que la creación en una red pública de un entorno de carácter

confidencial y privado que permitirá trabajar al usuario como si estuviera en su misma red local.

2.3.3.7 WPA (Wi-Fi Protected Access)

WPA (Acceso Inalámbrico Protegido) es una solución de seguridad inalámbrica (Wi-Fi[4]) ofrecida por WiFi Alliance para solucionar las carencias de WEP.

WPA es una versión "liviana" del protocolo 802.11i que depende de protocolos de autenticación y de un algoritmo de cifrado cerrado: TKIP (Protocolo de integridad de clave temporal) El TKIP genera claves aleatorias, para lograr mayor seguridad, puede alterar varias veces por segundo una clave de cifrado.

El funcionamiento de WPA se basa en la implementación de un servidor de autenticación (en general un servidor RADIUS) que identifica a los usuarios en una red y establece sus privilegios de acceso. No obstante, redes pequeñas pueden usar una versión más simple de WPA, llamada WPA-PSK, al implementar la misma clave de cifrado en todos los dispositivos, con lo cual ya no se necesita el servidor RADIUS.

El WPA (en su primera construcción) sólo admite redes en modo infraestructura, es decir que no se puede utilizar para asegurar redes punto a punto inalámbrico (modo "ad-hoc").

2.3.4 Gestión de red local inalámbrica

Gestionar redes Wi-Fi añade complejidad a la gestión de red para los administradores de redes. Por dos razones fundamentales:

- Se usan señales de radio en vez de cable para enlazar a los usuarios a la infraestructura de red, lo que significa que cualquiera con un adaptador 802.11 puede conectarse a ella.

[4] Wi-Fi: Es una marca de la Wi-Fi Alliance (anteriormente la WECA: Wireless Ethernet Compatibility Alliance), la organización comercial que adopta, prueba y certifica que los equipos cumplen los estándares 802.11 relacionados a redes inalámbricas de área local.

- Los usuarios al no estar ya ubicados a la red por ningún cable pueden moverse libremente dentro de la cobertura inalámbrica, cruzándose por múltiples puntos de acceso y subredes.

Esto exigen un enfoque más detallado que en la gestión de LAN convencionales, así como herramientas para monitorizar y administrar los dispositivos físicos que forman la infraestructura; sin embargo, la función básica de gestionar es la misma que en las redes cableadas; es decir, cuanta más información se disponga de la WLAN, en mejores condiciones se estará para garantizar la disponibilidad y conectividad, optimizar el rendimiento y soportar las distintas naturalezas de un número creciente de aplicaciones y servicios de voz, vídeo y localización.

2.3.4.1 ¿Qué se busca en una gestión WLAN?

La gestión de las redes Wi-Fi abarca desde la configuración y securización hasta la monitorización y administración, tanto de los puntos de acceso y los controladores; así como, de los dispositivos de acceso y los usuarios finales. Para cubrir estas áreas (en mayor o menor medida) están las soluciones por software o por una combinación de hardware y software que hoy se dispone en el mercado. Básicamente, una aplicación de gestión WLAN proporciona una interfaz gráfica con la que interactuar con distintos programas de software encargados de recoger, procesar y mostrar en tiempo real datos relativos al estado y comportamiento de una red Wi-Fi. Tales datos no sólo pueden proceder del hardware de red; sino también, de sensores instalados para escanear las bandas del espectro de radiofrecuencia utilizadas por los estándares 802.11; los programas de gestión permiten además, definir aplicar y reforzar políticas que controlen las autorizaciones y permisos de acceso de usuarios y grupos de usuarios. También es necesario conocer en qué modo y a qué nivel, la solución se conectará con los dispositivos de la infraestructura de red desplegada para la gestión, como son: directorios, autenticación, seguridad y monitorización del rendimiento. Siempre habrá que tener en cuenta que la gestión de WLAN abarca componentes separados y distintos.

2.3.4.2 Controlar el espectro

Está basado en la gestión de radiofrecuencia, en aspectos como la fortaleza de la señal, ruido, errores e interferencias. Como mínimo, la gestión de radiofrecuencia debe analizar las interferencias entre señales y el nivel de ruido en las bandas más relevantes, así como detectar dispositivos wireless no autorizados. Asimismo, es necesario controlar la utilización de los canales, el número de clientes por punto de acceso y estadísticas referentes a factores tales como caídas y errores de paquetes, jitter(fluctuación) y retardos del tráfico. Finalmente, para tener un control eficaz es esencial conocer la experiencia de los usuarios en términos de cobertura, fortaleza de la señal, nivel de ruido, capacidad de proceso, etc. Sin información sobre todos estos aspectos será imposible mantener y optimizar la comunicación inalámbrica, eliminar los problemas de cobertura y mejorar el sistema de alarmas ante la aparición de problemas potenciales, como los conflictos entre canales o la caída de conexiones. Y tratándose de redes wireless, el soporte de la seguridad y su gestión es clave.

2.3.5 Control de ancho de banda

En redes el ancho de banda es la cantidad de información o de datos que se puede enviar a través de una conexión de red en un período dado. El ancho de banda se indica generalmente en bits por segundo (bps), kilobits por segundo (Kbps), o megabits por segundo (Mbps).

El control del ancho de banda permite reservar cierta capacidad del ancho de banda de salida de un determinado interfaz para determinados tipos de tráfico. Esto puede ayudar igualmente a asegurar que el dispositivo (router) va a enviar siempre cierto tipo de tráfico (en especial aplicaciones de tiempo real) con un mínimo retardo. Dado el incremento en el uso de aplicaciones de tiempo real tales como la voz sobre IP (VoIP), los requerimientos de ancho de banda van también creciendo.

El control del ancho de banda tiene como objetivo responder a las siguientes preguntas:

- ¿Quién debería obtener un determinado nivel de servicio para ciertas aplicaciones?
- ¿Qué nivel de prioridad debería asignarse a cada tipo de tráfico?
- ¿Para qué tipo de tráfico debe garantizarse su entrega?
- ¿Qué cantidad de ancho de banda debe ser reservada para garantizar un correcto funcionamiento?

El control del ancho de banda también permite la configuración del ancho de banda de salida permitido en un interfaz para su coincidencia con el que puede manejar la red. Esto ayuda a reducir los retardos y las pérdidas de paquetes en el siguiente dispositivo de enrutamiento. Por ejemplo, es posible configurar el interfaz WAN con una velocidad de 1000Kbps si la conexión de ADSL dispone de una velocidad de subida de 1000Kbps.

2.3.5.1 Ancho de banda: Clases y filtros

Utilizando la definición de clases, en la gestión del ancho de banda se puede reservar cierto ancho de banda. La configuración de un filtro permite definir una clase en base a una aplicación específica y/o subred.

El total del ancho de banda reservado para las clases no puede exceder del ancho de banda configurado para la clase raíz.

2.3.5.2 Reserva del ancho de banda

La gestión del ancho de banda permite definir qué cantidad del ancho de banda puede obtener cada clase; sin embargo, el ancho de banda real para cada clase crece o decrece en proporción al ancho de banda real disponible.

Ejemplos Gestión de ancho de banda:

Gestión de Ancho de Banda basado en aplicación como se muestra en la figura 2.8. Indica de esta manera el ancho de banda asignado a cada clase que entre en uso.

Gestión de Ancho de Banda basado en Subred como se muestra en la figura 2.9. Asignando a cada subred un correspondiente ancho de banda disponible.

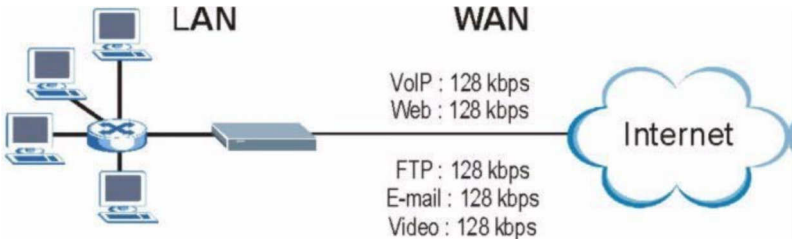


Figura 2.8 Gestión de ancho de banda basado en aplicación.
Fuente: http://www.zyxel.es/descargas/Manuales/P660HW-61/Funcionalidad%20Gesti%F3n%20Ancho%20de%20Banda.pdf

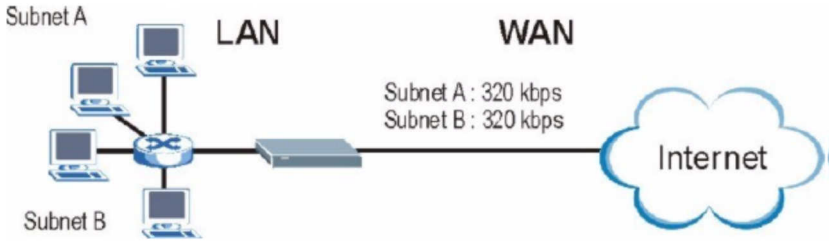


Figura 2.9 Gestión de ancho de banda basado en subred.
Fuente: http://www.zyxel.es/descargas/Manuales/P660HW-61/Funcionalidad%20Gesti%F3n%20Ancho%20de%20Banda.pdf

Gestión de Ancho de Banda basado en Aplicación y Subred como se muestra en la figura 2.10. Asignando una cierta cantidad de ancho de banda de la subred a cada clase que se utilice observado en la tabla 2.1.

Tabla 2.1 Gestión de ancho de banda basado en aplicación y subred.

TIPO DE TRAFICO	DESDE SUBRED A	DESDE SUBRED B
VoIP	64Kbps	64Kbps
Web	64Kbps	64Kbps
FTP	64Kbps	64Kbps
E-mail	64Kbps	64Kbps
Video	64Kbps	64Kbps

Fuente: http://www.zyxel.es/descargas/Manuales/P660HW-61/Funcionalidad%20Gesti%F3n%20Ancho%20de%20Banda.pdf

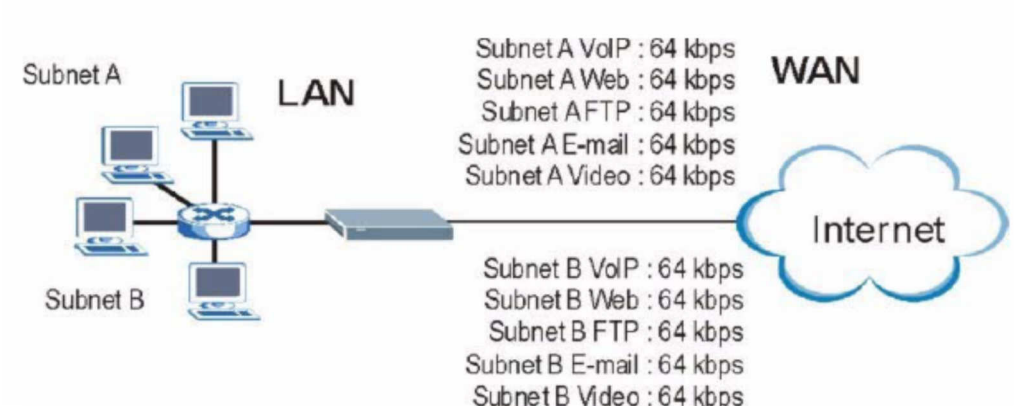


Figura 2.10 Gestión de ancho de banda basado en aplicación y subred.
Fuente: http://www.zyxel.es/descargas/Manuales/P660HW-61/Funcionalidad%20Gesti%F3n%20Ancho%20de%20Banda.pdf

2.3.6 Monitoreo de red

El término Monitoreo de red describe el uso de un sistema que constantemente monitoriza una red de computadoras en busca de componentes defectuosos o lentos, para luego informar a los administradores de redes mediante correo electrónico u otras alarmas. Es un subconjunto de funciones de la administración de redes.

Mientras que un sistema de detección de intrusos monitorea una red por amenazas del exterior (externas a la red), un sistema de monitoreo de red busca problemas causados por la sobrecarga y/o fallas en los servidores, como también problemas de la infraestructura de red (u otros dispositivos).

Por ejemplo, para determinar el estatus de un servidor web, software de monitoreo puede enviar, periódicamente, peticiones HTTP (Protocolo de Transferencia de Hipertexto) para obtener páginas; para un servidor de correo electrónico, enviar mensajes mediante SMTP (Protocolo de Transferencia de Correo Simple), para luego ser retirados mediante IMAP (Protocolo de Acceso a Mensajes de Internet) o POP3 (Protocolo Post Office).

Comúnmente, los datos evaluados son tiempo de respuesta y disponibilidad (o uptime), aunque estadísticas tales como consistencia y fiabilidad han ganado popularidad. La generalizada instalación de dispositivos de optimización para redes de área extensa tiene un efecto adverso en la mayoría del software de

monitoreo, especialmente al intentar medir el tiempo de respuesta de punto a punto de manera precisa, dado el límite de visibilidad de ida y vuelta.

Las fallas de peticiones de estado, tales como que la conexión no pudo ser establecida, tiempo de espera agotado, entre otros, usualmente produce una acción desde del sistema de monitoreo. Estas acciones pueden variar; una alarma puede ser enviada al administrador, en ejecución automática de mecanismos de controles de fallas, etc.

Monitorear la eficiencia del estado del enlace de subida se denomina Medición de tráfico de red.

2.3.6.1 Enfoques de monitoreo

Existen, al menos, dos puntos de vista para abordar el proceso de monitorear una red: el enfoque activo y el enfoque pasivo. Aunque son diferentes ambos se complementan.

Monitoreo Activo

El monitoreo activo se realiza inyectando paquetes de prueba en la red, o enviando paquetes a determinadas aplicaciones midiendo sus tiempos de respuesta. Este enfoque tiene la característica de agregar tráfico en la red. Es utilizado para medir el rendimiento en una red.

Técnicas de monitoreo activo:

Basado en ICMP (Protocolo de Mensajes de Control de Internet).

- Diagnosticar problemas en la red
- Detectar retardo, pérdida de paquetes.
- RTT (Round-Trip delay Time)
- Disponibilidad de host y redes.

Basado en TCP (Protocolo de Control de Transmisión)

- Tasa de transferencia
- Diagnosticar problemas a nivel aplicación

Basado en UDP (Protocolo de Datagrama de Usuario)

- Pérdida de paquetes en un sentido (one-way)
- RTT (traceroute)

Monitoreo Pasivo

El monitoreo pasivo se basa en la obtención de datos a partir de recolectar y analizar el tráfico que circula por la red. Se emplean diversos dispositivos como sniffers, ruteadores, computadoras con software de análisis de tráfico y en general dispositivos con soporte para snmp (Simple Network Management Protocol o en español Protocolo simple de administración de red), rmon (Monitoreo remoto de redes) y netflow (protocolo desarrollado por CISCO Systems para coleccionar información del tráfico de red). Este enfoque no agrega tráfico en la red como lo hace el activo. Es utilizado para caracterizar el tráfico en la red y para contabilizar su uso.

Técnicas de monitoreo pasivo:

Solicitudes remotas

Mediante SNMP: Esta técnica es utilizada para obtener estadísticas sobre la utilización de ancho de banda en los dispositivos de red, para ello se requiere tener acceso a dichos dispositivos. Al mismo tiempo, este protocolo genera paquetes llamados *traps* que indican que un evento inusual se ha producido.

Otro método de acceso: Se pueden realizar scripts que tengan acceso a dispositivos remotos para obtener información importante para monitorear. En esta técnica se pueden emplear módulos de perl, ssh con autenticación de llave pública, etc.

Captura de tráfico

Se puede llevar a cabo de dos formas:

1 Mediante la configuración de un puerto espejo en un dispositivo de red, el cual hará una copia del tráfico que se recibe en un puerto hacia otro donde estará conectado el equipo que realizará la captura; y
2 Mediante la instalación de un dispositivo intermedio que capture el tráfico, el cual puede ser una computadora con el software de captura o un dispositivo extra. Esta técnica es utilizada para contabilizar el tráfico que circula por la red.

Análisis de tráfico

Esta técnica se utiliza para caracterizar el tráfico de la red, es decir, para identificar el tipo de aplicaciones que son más utilizadas. Se puede implementar haciendo uso de dispositivos *probe* que envíen información mediante RMON o a través de un dispositivo intermedio con una aplicación capaz de clasificar el tráfico por aplicación, direcciones IP origen y destino, puertos origen y destino, etc.

Flujos

También utilizado para identificar el tipo de tráfico utilizado en la red. Un flujo es un conjunto de paquetes con:

- La misma IP origen y destino
- El mismo puerto TCP origen y destino
- El mismo tipo de aplicación.

Los flujos pueden ser obtenidos de ruteadores o mediante dispositivos que sean capaces de capturar tráfico y transformarlo en flujos. También es usado para tareas de facturación (billing).

2.3.6.2 Estrategia de monitoreo

Antes de implementar un esquema de monitoreo se deben tomar en cuenta los elementos que se van a monitoreo así como las herramientas que se utilizarán para esta tarea.

¿Qué se debe monitorear en una red?

Una consideración muy importante es delimitar el espectro sobre el cual se va a trabajar. Existen muchos aspectos que pueden ser monitoreados, los más comunes son los siguientes:

- Utilización de ancho de banda
- Consumo de CPU
- Consumo de memoria
- Estado Físico de las conexiones
- Tipo de tráfico
- Alarmas
- Servicios (Web, correo, base de datos)

Es importante definir el alcance de los dispositivos que van a ser monitoreados, puede ser muy amplio y se puede dividir de la siguiente forma.

- **Dispositivos de Interconexión.** Ruteadores, switches, hubs, firewall
- **Servidores.** Web, Mail, DB
- **Red de Administración.** Monitoreo, Logs, Configuración.

2.3.6.3 Métricas de una red

La definición de métricas permitirá establecer patrones de comportamiento para los dispositivos que serán monitoreados. También hay diversos tipos de métricas que pueden ser declarados, dependerán de las necesidades particulares de cada red. Las métricas deben ser congruentes con los objetos a monitorear que fueron señalados en el punto anterior. Algunos ejemplos son:

- Métricas de tráfico de entrada y salida
- Métricas de utilización de procesador y memoria
- Métrica de estado de las interfaces
- Métrica de conexiones lógicas

A cada métrica se le asigna un valor promedio, el cual identifica su patrón de comportamiento.

2.3.6.4 Alarmas

Las alarmas son consideradas como eventos con comportamiento inusual. Las alarmas más comunes son las que reportan cuando el estado operacional de un dispositivo o servicio cambia. Existen otros tipos de alarmas basado en patrones previamente definidos en nuestras métricas, son valores máximos conocidos como umbrales o *threshold*. Cuando estos patrones son superados se produce una alarma, ya que es considerado como un comportamiento fuera del patrón. Algunos tipos de alarmas son:

- Alarmas de procesamiento
- Alarmas de conectividad
- Alarmas ambientales
- Alarmas de utilización
- Alarmas de disponibilidad (estado operacional)

2.3.6.5 Elección de herramientas de monitoreo

Existe un gran número de herramientas para resolver el problema del monitoreo de una red. Las hay tanto comerciales como basadas en software libre. La elección depende de varios factores, tanto humanos, económicos como de infraestructura:

- El perfil de los administradores, sus conocimientos en determinados sistemas operativos.
- Los recursos económicos disponibles.
- El equipo de cómputo disponible.

En esta ocasión se hará énfasis en tres herramientas:

Cacti

Es una completa solución para el monitoreo de redes. Utiliza RRDTool para almacenar la información de los dispositivos y aprovecha sus funcionalidades de graficación. Proporciona un esquema rápido de obtención de datos remotos, múltiples métodos de obtención de datos (snmp, scripts), un manejo avanzado de templates, y características de administración de usuarios. Además, ofrece un

servicio de alarmas mediante el manejo de umbrales. Todo ello en una sola consola de administración, fácil de configurar.

Net-SNMP

Conjunto de aplicaciones para obtener información vía snmp de los equipos de interconexión. Soporta la versión 3 del protocolo la cual ofrece mecanismos de seguridad tanto de confidencialidad como de autenticación. Provee de manejo de *traps* para la notificación de eventos.

Nagios.

Aplicación para el monitoreo de servicios, hosts que pertenecen a una red. Es capaz de monitorear si un servicio se encuentra activo o no, o si un hosts se encuentra operacional o no. Muestra el estadio operacional de todos los servicios y hosts en un ambiente Web. Envía notificaciones mediante mail o *pager* cuando el estado operacional de un elemento a monitorear cambia.

2.3.7 Internet

Internet es una red de ordenadores conectados entre sí, que permite a los usuarios compartir información.

2.3.7.1 Formas de conexión

En la actualidad los usuarios disponen de dos formas básicas de conectarse a Internet:

a) Mediante un Proveedor de Servicios de Internet (PSI), que es una compañía (Telefónica, Cable) que permite, ingresar (pagando sólo el coste de la llamada) o mediante una cuota mensual, conectarse a los ordenadores de su red, que ya está conectada a Internet y, así, disponer, también, de acceso. La conexión del ordenador a la red del PSI puede hacerse de varias maneras, lo que redunda en el precio y la velocidad de conexión: mediante un módem conectado a la línea telefónica convencional (la misma que se utiliza para las llamadas de voz normales), mediante una línea RDSI, ADSL o una conexión por cable.

b) A través de una red de área local: en este caso, el ordenador del usuario está conectado a una red de área local que, a su vez, está conectada a Internet mediante un PSI de la forma comentada anteriormente.

Sea cual sea la conexión escogida, el primer paso será el de configurar el ordenador, para poder hacer uso de dicha conexión, con los parámetros de configuración que proporcione el PSI o el administrador de red.

2.3.8 Protocolos

Las redes de computadores, al igual que otros tipos de redes de comunicación, utilizan diferentes protocolos (conjunto de reglas) para entenderse. Los dispositivos que conectamos en red actualmente son muy heterogéneos, impidiendo que solo puedan ser interconectados haciendo uso de hardware. Por ello se requiere el uso de software y hardware un tanto genérico.

2.3.8.1 Modelo de capas

Con el objetivo de hacer esta interconexión por medio de software, se han realizado diferentes trabajos para organizarlo de manera tal que el diseño de nuevo software y hardware se haga de una forma más fácil. Para lograr esto, los sistemas de red están organizados en capas como se observa en la figura 2.11.

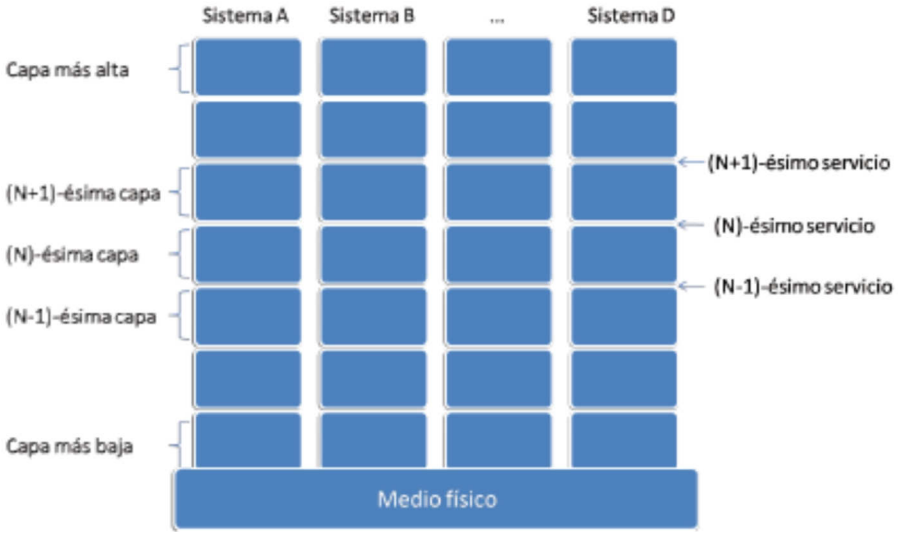


Figura 2.11 Sistemas, capas y servicios
Fuente: José Salvador Portugal Luna - Protocolo de Red Ligero para Redes Inalámbricas de Monitoreo y Control que Utilizan el Estándar IEEE 802.15.4

Donde cada una está arriba de otra, formando una pila de capas, dependiendo del tipo de red que se esté utilizando será el conjunto de capas que se utilicen.

El propósito de cada capa es brindar servicios a la capa que se encuentra directamente arriba de ella, de esta manera se encapsula la complejidad de cada uno de los servicios, la capa superior hace una petición de un servicio y la capa inferior lo satisface. En la Figura 2.11 se muestra cómo están organizadas conceptualmente las capas.

La capa N de un dispositivo se comunica con la capa N en otro haciendo uso de un lenguaje conocido como protocolo. Un protocolo es un acuerdo entre las partes que se estén comunicando que especifica cómo debe ser el proceso de comunicación.

A un conjunto de capas y protocolos se le conoce como arquitectura de red, la especificación de una arquitectura debe contener la suficiente información para permitir que alguien sea capaz de hacer un software o hardware que trabaje en alguna capa con el protocolo apropiado. La arquitectura de la red no especifica cómo es la implementación ni las interfaces, ya que no es necesario que las interfaces de todos los dispositivos de la red sean iguales, sólo es importante que cada capa haga un uso adecuado del protocolo establecido.

A la lista de protocolos usados en cierto sistema, donde cada capa utiliza un protocolo se le conoce como pila de protocolos.

Cuando una capa de un dispositivo se comunica con la capa del mismo nivel en otro no lo hace directamente, sino a través de la capa que se encuentra debajo de ella y tampoco lo hace porque ella quiera comunicarse sino porque la capa superior se lo ha pedido. A excepción de la capa de aplicación, la cual es la única que inicia la comunicación por ser la más alta del modelo, por otro lado, la capa más baja que es la capa física si se comunican directamente. La Figura 2.12 muestra la forma en que se comunican capas del mismo nivel.

Figura 2.12 Relación entre un servicio y un protocolo.
Fuente: José Salvador Portugal Luna - Protocolo de Red Ligero para Redes Inalámbricas de Monitoreo y Control que Utilizan el Estándar IEEE 802.15.4

Debido a que cada capa le solicita servicios a la capa inferior, la capa superior manda información que la capa inferior toma como datos y agrega un encabezado o la encapsula para poder transmitirla con el protocolo adecuado de esa capa mostrado en la figura 2.11, a su vez la capa inferior se la pasa a la capa que está debajo de ella y se repite el mismo procedimiento. Por ejemplo si se utiliza un modelo de 5 capas, la capa de aplicación en la capa 5 produce un mensaje y se lo pasa a la capa 4 para que lo transmita, la capa 4 le agrega un encabezado al inicio del mensaje para identificarlo y permitir que la capa 4 de la máquina remota lleve la secuencia de los paquetes recibidos y si le falta alguno entonces haga la petición, posteriormente la capa 4 se lo pasa a la capa 3 la cual divide el mensaje en un tamaño preestablecido según sea el protocolo que se esté utilizando en la capa 3 y además agrega a cada parte un encabezado.

Después la capa 3 envía cada uno de los segmentos a la capa 2 que agrega información al inicio y al final del paquete y se lo envía a la capa 1 para la transmisión física. Del otro lado, en la máquina receptora, cada capa va desempaquetando los mensajes quitándole la información que le agregó su contraparte en la máquina transmisora y únicamente pasa la información que recibió la capa de su mismo nivel. Entre la información que cada capa le agrega al mensaje se encuentra el direccionamiento, el control de errores (ya que los medios físicos no garantizan que lleguen al otro lado) y el control de flujo.

Las capas pueden ofrecer dos tipos de servicios: orientados a conexión y no orientados a conexión. Los orientados a conexión primeramente establecen un canal por donde se hará la comunicación, después se transmiten los mensajes de la

información y por último se libera el canal, mientras que en los no orientados a conexión cada mensaje es enviado por diferentes canales o caminos y puede ser que no lleguen en el orden que fueron transmitidos, entonces aquí es donde interviene el protocolo que se esté usando en cada capa para garantizar que todos los datos que fueron enviados sean los que recibió la máquina remota.

2.3.8.2 Tareas de las capas

Existen diferentes caracterizaciones de las capas de los sistemas de comunicación, una de las más utilizadas es la de TCP/IP, que cuenta con 5 capas, aplicación, transporte, red, enlace de datos y física, pero el modelo de referencia es el de Interconexión de Sistemas Abiertos (OSI, Open System Interconnection) lanzado en 1984 por Organización Internacional para la Estandarización (ISO, International Organization for Standardization). El modelo OSI figura 2.13 define 7 capas, aplicación, presentación, sesión, transporte, red, enlace de datos y nivel físico (ISO/IEC7498-1, 1994). Aunque este modelo no es muy reciente, las tareas que indica que realiza cada capa se siguen manteniendo como referencia hasta la actualidad.

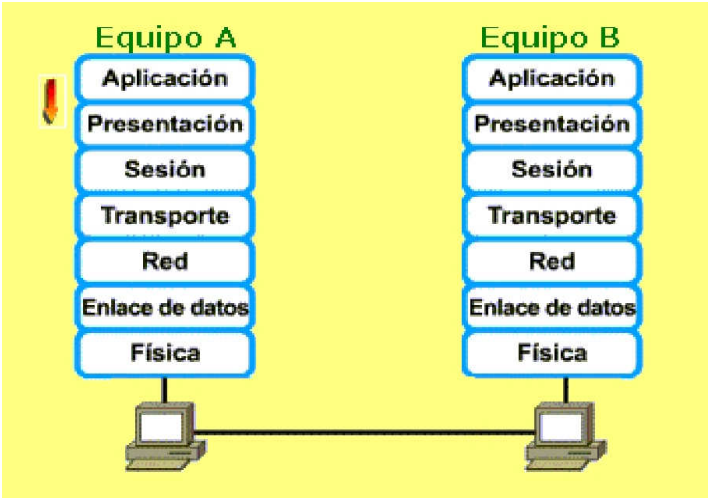


Figura 2.13 Modelo OSI.
Fuente: http://www.uazuay.edu.ec/estudios/sistemas/teleproceso/apuntes_1/modelo_osi.htm

Capa de aplicación

Ofrece a las aplicaciones (de usuario o no) la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones

para intercambiar datos, como correo electrónico (POP y SMTP), gestores de bases de datos y servidor de ficheros (FTP). Hay tantos protocolos como aplicaciones distintas y puesto que continuamente se desarrollan nuevas aplicaciones el número de protocolos crece sin parar.

Cabe aclarar que el usuario normalmente no interactúa directamente con el nivel de aplicación. Suele interactuar con programas que a su vez interactúan con el nivel de aplicación pero ocultando la complejidad subyacente. Así por ejemplo un usuario no manda una petición "HTTP/1.0 GET index.html" para conseguir una página en html, ni lee directamente el código html/xml.

Capa de presentación

El objetivo de la capa de presentación es encargarse de la representación de la información, de manera que aunque distintos equipos puedan tener diferentes representaciones internas de caracteres (ASCII, Unicode, EBCDIC), números (little-endian tipo Intel, bigendian tipo Motorola), sonido o imágenes, los datos lleguen de manera reconocible.

Esta capa es la primera en trabajar más el contenido de la comunicación que en cómo se establece la misma. En ella se tratan aspectos tales como la semántica y la sintaxis de los datos transmitidos, ya que distintas computadoras pueden tener diferentes formas de manejarlas. La capa de presentación también permite cifrar los datos y comprimirlos para ocupar menos ancho de banda. En pocas palabras es un traductor.

Capa de sesión

Esta capa establece, gestiona y finaliza las conexiones entre usuarios (procesos o aplicaciones) finales. Ofrece varios servicios que son cruciales para la comunicación, como son:

- Control de la sesión a establecer entre el emisor y el receptor.
- Control de la concurrencia.
- Mantener puntos de verificación (check points), que sirven para que, ante una interrupción de transmisión por cualquier causa, la misma se pueda

reanudar desde el último punto de verificación en lugar de repetirla desde el principio.

El servicio provisto por esta capa es la capacidad de asegurar 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 muchos casos, los servicios de la capa de sesión son parcialmente, o incluso, totalmente prescindibles.

Capa de transporte

Su función básica es aceptar los datos enviados por las capas superiores, dividirlos en pequeñas partes si es necesario, y pasarlos a la capa de red. En el caso del modelo OSI, también se asegura que lleguen correctamente al otro lado de la comunicación. Otra característica a destacar es que debe aislar a las capas superiores de las distintas posibles implementaciones de tecnologías de red en las capas inferiores, lo que la convierte en el corazón de la comunicación. En esta capa se proveen servicios de conexión para la capa de sesión que serán utilizados finalmente por los usuarios de la red al enviar y recibir paquetes.

Estos servicios estarán asociados al tipo de comunicación empleada, la cual puede ser diferente según el requerimiento que se le haga a la capa de transporte. Por ejemplo, la comunicación puede ser manejada para que los paquetes sean entregados en el orden exacto en que se enviaron, asegurando una comunicación punto a punto libre de errores, o sin tener en cuenta el orden de envío. Una de las dos modalidades debe establecerse antes de comenzar la comunicación para que una sesión determinada envíe paquetes, y ése será el tipo de servicio brindado por la capa de transporte hasta que la sesión finalice.

Capa de red

La capa de red, según la normalización OSI, es una capa que proporciona conectividad y selección de ruta en la red para interconectar dos dispositivos. Es el tercer nivel del modelo OSI y su misión es conseguir que los datos lleguen desde el origen al destino aunque no tengan conexión directa. Ofrece servicios al

nivel superior (nivel de transporte) y se apoya en el nivel de enlace, es decir, utiliza sus funciones. Para realizar su tarea, puede asignar direcciones de red únicas, interconectar subredes distintas, encaminar paquetes y utilizar un control de congestión.

Capa de enlace de datos

El nivel de enlace es el segundo del modelo OSI. Recibe peticiones del nivel de red y utiliza los servicios del nivel físico. El objetivo del nivel de enlace es conseguir que la información fluya, libre de errores, entre dos máquinas que estén conectadas directamente (servicio orientado a conexión). Para lograr este objetivo tiene que montar bloques de información (llamados tramas en este nivel), dotarles de una dirección de nivel de enlace, gestionar la detección o corrección de errores, y ocuparse del control de flujo entre equipos (para evitar que un equipo más rápido desborde a uno más lento).

Capa de física

La capa física del modelo de referencia OSI es la que se encarga de las conexiones físicas de la computadora hacia la red, tanto en lo que se refiere al medio físico (medios guiados: cable coaxial, cable de par trenzado, fibra óptica y otros tipos de cables; medios no guiados: radio, infrarrojos, microondas, láser y otras redes inalámbricas); características del medio (por ejemplo, tipo de cable o calidad del mismo; tipo de conectores normalizados o en su caso tipo de antena; etc.) y la forma en la que se transmite la información (codificación de señal, niveles de tensión/intensidad de corriente eléctrica, modulación, tasa binaria, etc.).

Es la encargada de transmitir los bits de información a través del medio utilizado para la transmisión. Se ocupa de las propiedades físicas y características eléctricas de los diversos componentes; de la velocidad de transmisión, si ésta es uni o bidireccional (simplex, dúplex o full-dúplex). También de aspectos mecánicos de las conexiones y terminales, incluyendo la interpretación de las señales eléctricas/electromagnéticas.

Se encarga de transformar una trama de datos proveniente del nivel de enlace en una señal adecuada al medio físico utilizado en la transmisión. Estos impulsos pueden ser eléctricos (transmisión por cable) o electromagnéticos (transmisión sin cables). Estos últimos, dependiendo de la frecuencia/longitud de onda de la señal pueden ser ópticos, de micro-ondas o de radio. Cuando actúa en modo recepción el trabajo es inverso; se encarga de transformar la señal transmitida en tramas de datos binarios que serán entregados al nivel de enlace.

2.3.9 Servicios

Básicamente Internet se usa para buscar y compartir información. A esta información se puede acceder de diversas formas, lo que da lugar a los distintos servicios de Internet. Los principales servicios son los siguientes:

- **Navegación web.** Consiste en consultar páginas web pasando de unas a otras conociendo sus direcciones o utilizando los hipervínculos que hay entre ellas.
- **Correo electrónico.** Es la posibilidad de contar con una dirección en la que recibir mensajes de otros usuarios y desde la que mandar mensajes.
- **Foros.** Son tablones de anuncios agrupados por temas, en los que los usuarios depositan su mensaje o contestan a los de otros, encadenándose largas secuencias de respuestas.
- **Chat.** Es la posibilidad de comunicarnos en tiempo real con otras personas en salas públicas o privadas.
- **Mensajería instantánea.** Brinda la posibilidad de avisar cuando algún conocido se conecta a Internet, para poder establecer una comunicación en tiempo real directamente.
- **Transferencia de archivos (FTP).** Es un servicio que permite la transferencia de archivos en Internet.
- **Las listas de correo o listas de distribución.** Es algo similar a los foros pero los mensajes que envían los usuarios no van a un lugar público, el foro, sino al correo de cada uno de los miembros de la lista.
- **Intercambio de archivos.** Con este nombre se hace referencia a un servicio que permite a usuarios particulares intercambiar archivos de sus

ordenadores sin la intervención de servidores externos (FTP). Este servicio ha impulsado la copia y distribución ilegal de software y música, pues se ha vuelto complicado buscar un culpable al ser los usuarios particulares los que intercambian los archivos.

A estos servicios se accede de una forma similar, según lo que se conoce como la arquitectura cliente-servidor. En Internet hay ordenadores que son servidores web (ofrecen páginas web), otros que son servidores de correo (ofrecen la posibilidad de tener en ellos una cuenta de correo), hay también servidores de Chat, de foros, y para acceder a cada uno de estos servicios es necesario ser lo que se conoce como un cliente (para solicitar la información): Mozilla es un cliente web o navegador, Evolution es un cliente de correo, Mozilla Mail es un cliente de foros (y de correo), Xchat de IRC o gFTP de FTP.

Cualquier ordenador puede convertirse en un servidor (de páginas web, de correo, FTP, etc) sólo con instalar el programa adecuado.

2.3.10 Empresa

Una empresa es una unidad económico-social, integrada por elementos humanos, materiales y técnicos, que tiene el objetivo de obtener utilidades a través de su participación en el mercado de bienes y servicios. Para esto, hace uso de los factores productivos (trabajo, tierra y capital).

Las empresas puedan clasificarse según la actividad económica que desarrollan. Así, nos encontramos con empresas del sector primario (que obtienen los recursos a partir de la naturaleza, como las agrícolas, pesqueras o ganaderas), del sector secundario (dedicadas a la transformación de bienes, como las industriales y de la construcción) y del sector terciario (empresas que se dedican a la oferta de servicios o al comercio).

Otra clasificación válida para las empresas es de acuerdo a su constitución jurídica. Existen empresas individuales (que pertenecen a una sola persona) y societarias (conformadas por varias personas). En este último grupo, las

sociedades a su vez pueden ser anónimas, de responsabilidad limitada y de economía social (cooperativas), entre otras.

Las empresas también pueden ser definidas según la titularidad del capital. Así, nos encontramos con empresas privadas (su capital está en mano de particulares), públicas (controladas por el Estado), mixtas (el capital es compartido por particulares y por el Estado) y empresas de autogestión (el capital es propiedad de los trabajadores).

INTERCOMPU, empresa dirigida por su dueño y gerente Lic. Darwin Dávila, la empresa tiene como objetivos:

- Venta y asesoramiento en la adquisición de todas las marcas de equipos de cómputo.
- Instalación de redes estructuradas de datos.
- Soporte técnico en sistemas de impresión de tinta continua.
- Reparación y mantenimiento de equipos de cómputo.
- Prestación y comercialización de servicios de Internet.

Cuenta con las áreas:

- Administrativa: compuesta del gerente-propietario y la contadora.
- Laboratorio y área técnica: compuesta por el técnico.

2.4 Hipótesis

¿La implementación de un sistema de monitoreo y control de redes inalámbricas optimizará el servicio de Internet de la empresa Intercompu?

2.5 Señalamiento de variables

2.5.1 Variable independiente

- Sistema de monitoreo y control de redes inalámbricas.

2.5.2 Variable dependiente

- Servicio de Internet de la empresa Intercompu.

CAPÍTULO III

METODOLOGÍA

3.1 Enfoque

La investigación tuvo un enfoque cuantitativo puesto que fue necesario conocer las causas y factores referentes a los sistemas de monitoreo y control de redes inalámbricas, explicativa basándose en la necesidad de conocer los hechos ligados a la empresa; la información consultada sirvió de sustento para interpretar de manera científica, siendo analizados los beneficios que traen los sistemas de monitoreo y control en la asignación de anchas de banda, obteniendo resultados favorables para la empresa.

3.2 Modalidad básica de la investigación

3.2.1 Investigación bibliográfica - documental

Se realizó una investigación bibliográfica - documental para obtener información sobre las tecnologías empleadas en la monitoreo y control de redes inalámbricas, se recopiló información que sirvió de apoyo en la realización de esta investigación.

3.2.2 Investigación de campo – experimental

Se realizó una investigación de campo – experimental para poder aplicar los conocimientos adquiridos en pos de encontrar la solución al problema presente en la empresa Intercompu, implementándose soluciones y medición de resultados.

3.3 Nivel o tipo de investigación

3.3.1 Exploratorio

Se realizó una investigación que permitió conocer las características actuales de los sistemas de monitoreo y control de redes inalámbricas así como su forma de implementación.

3.3.2 Descriptivo

El proceso investigativo fue descriptivo porque analizó los sistemas de monitoreo y control de redes inalámbricas, conociendo las ventajas, consecuencias y dificultades que atraviesan con el resto de tecnologías de servicios para red.

En la empresa se estudió la arquitectura existente de red, tanto alámbrica como inalámbrica, encontrando los principales focos de problemas y adaptando un sistema de monitoreo y control de redes.

3.4 Población y muestra

Para la población se ha tomado en cuenta los siguientes datos:

Tabla 3.1 Población

Descripción	Cantidad
Usuarios actuales provistos del servicio de Internet	10
Personal de la Empresa	3
TOTAL	13

Realizado: Carlos Ailaca

Debido al tamaño de la población, la muestra estará conformada por los diez usuarios actuales provistos del servicio de Internet porque son clientes a los que se les distribuye el servicio de Internet permanentemente.

3.5 Operacionalización de variables

Concepto	Dimensiones	Indicadores	Ítems	Tec.-Inv.
Variable Independiente: Sistema de monitoreo y control de redes inalámbricas.- comprende un sistema que constantemente monitoriza una red de computadoras en busca de componentes defectuosos o lentos en un ambiente inalámbrico.	1.- Tipos de monitoreo en red.	Hardware y software para el monitoreo en red.	1.- ¿Cuáles son los tipos de monitoreo en red?	Bibliografía.
	2.- Tecnologías empleadas en el monitoreo de redes inalámbricas.	Para una red alámbrica o red inalámbrica.	2.-¿Cuáles son las Tecnologías para la aplicación del monitoreo en redes inalámbricas?	Bibliografía.
	3.- Enlaces.	Medios guiados o no guiados, por la relación funcional.	3.- ¿Cómo se realiza el acceso de los enlaces a la red?	Bibliografía.
	4.- Control del servicio a ofrecer.	Seguridad al acceso a la red.	4.- ¿Cuáles son los servicios que ofrecen el monitoreo al acceder a la red?	Bibliografía.
Variable Dependiente: Optimizar el servicio de Internet de la empresa Intercompu	1.- Calidad del servicio.	Gerente y clientes.	1.-¿La empresa necesita una optimización del servicio de Internet ?	Entrevista y encuesta.
	2.- Diseño e implementación del sistema de monitoreo y control para la empresa Intercompu.	Establecimiento. Estudio y Análisis de los equipos.	2.- ¿Cuáles son los aspectos a optimizar en el servicio actual de Internet?	Encuesta, observación y experimentación.

Tabla 3.2 Operacionalización de variables
Realizado: Carlos Ailaca

3.6 Recolección de información

3.6.1 Plan de recolección de información

El instrumento para la recolección de información fue la Internet, los libros relacionados al monitoreo y control de redes inalámbricas, en ellos se realizó una búsqueda enfocada al objetivo planteado en esta investigación.

La entrevista que relacionó los datos referentes a la empresa y la situación actual, de la cual se obtuvo información de primera fuente realizando un cuestionario.

Una encuesta que obtuvo información importante respecto al servicio de Internet que brinda la empresa Intercompu, destacando puntos vitales que a la empresa interesa.

La observación fue de gran importancia obteniendo datos directos de la realidad, y las circunstancias que permitieron verificar los hechos, dando de esta forma la veracidad a la investigación.

3.7 Procesamiento de la información

3.7.1 Plan que se empleará para procesar la información recogida

a. Entrevista.
b. Encuesta.
c. Revisión.
d. Limpieza de la información.

CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

ENTREVISTA

Para brindar una solución a la propuesta de un sistema de monitoreo y control vinculado a redes inalámbricas en la empresa INTERCOMPU, se aplicó una entrevista al gerente de la empresa con la finalidad de establecer los servicios que va a mejorar y ofrecer, se instauró las siguientes preguntas:

Entrevistado: Lic. Darwin Dávila **Entrevistador:** Carlos Ailaca

1. **¿Qué clase de servicios de comunicación oferta la empresa en la actualidad?**

Estamos ofreciendo Internet banda ancha a los vecinos, el ancho de banda que se distribuye no está estipulado todavía.

2. **¿Qué clase de servicios desea incorporar en la red inalámbrica existente?**

Por el momento deseo solo mejorar la distribución de la red controlando a cada usuario el ancho de banda proporcionado; y estipular una tarifa de precios.

3. **¿Cuál cree que es la distancia máxima que el sistema va a monitorear y controlar en las conexiones inalámbricas?**

Creo que sería bueno unos quinientos metros a la redonda.

4. **¿Qué ubicación considera que sería la adecuada para la puesta del servidor?**

Creo que sería desde el laboratorio para poder manipular y ver si están actuando con los otros equipos.

5. **¿Piensa que sería necesario incorporar un equipo al usuario para mantener el monitoreo y control de la red inalámbrica?**

Claro; de ser necesario, estaremos más seguros de cuanto está llegando, cuánto está utilizando; si de pronto hay otro tipo de percances en el internet.

Análisis:

El ancho de banda de Internet distribuido hacia los usuarios no tiene estipulado un control; la mejora en la distribución de Internet estaría basada en el control del ancho de banda a cada usuario estipulando una tarifa de conexión a la red inalámbrica; el gerente tiene una aspiración de cubrir una extensión de 500 metros a la redonda. La ubicación de los equipos estaría en el laboratorio y si fuera necesario incorporar equipos que permitan el control del servicio a cada usuario estos se implementarían.

Interpretación:

La situación de la empresa Intercompu distribuyendo el servicio de Internet de banda ancha a los usuarios actuales resulta ineficiente en el control de ancho de banda asignado a cada uno de los usuarios que integran la red, teniendo en cuenta que desea el gerente ampliar el servicio a más usuarios que se encuentren en un radio de 500 metros a la redonda de la ubicación de la empresa Intercompu se precisa mejorar las condiciones actuales en el software y hardware; y legalizar la distribución del servicio; el área para los equipos requeridos en la empresa existe, así como, la intención de incorporar dispositivos de control del servicio a los usuarios si fuere necesario.

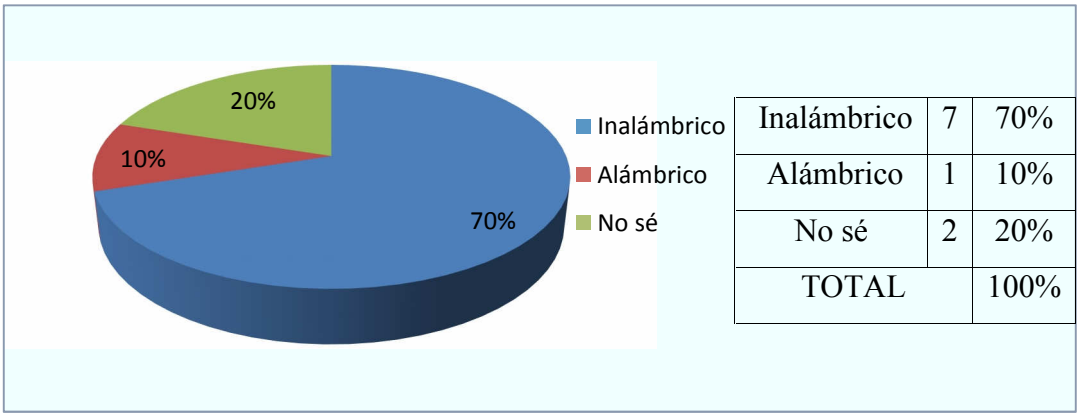
ENCUESTA

Por otra parte, se realizó una encuesta a los usuarios actuales provistos del servicio de internet conectado a la red de la empresa Intercompu.

Tamaño de la muestra:
Encuestados: 10 personas = 100%

Preguntas:

1. **¿El acceso de servicio de internet que le suministra la empresa Intercompu es?**



Inalámbrico	7	70%
Alámbrico	1	10%
No sé	2	20%
TOTAL		100%

Figura 4.1 Modo de acceso al servicio de internet.
Realizado: Carlos Ailaca

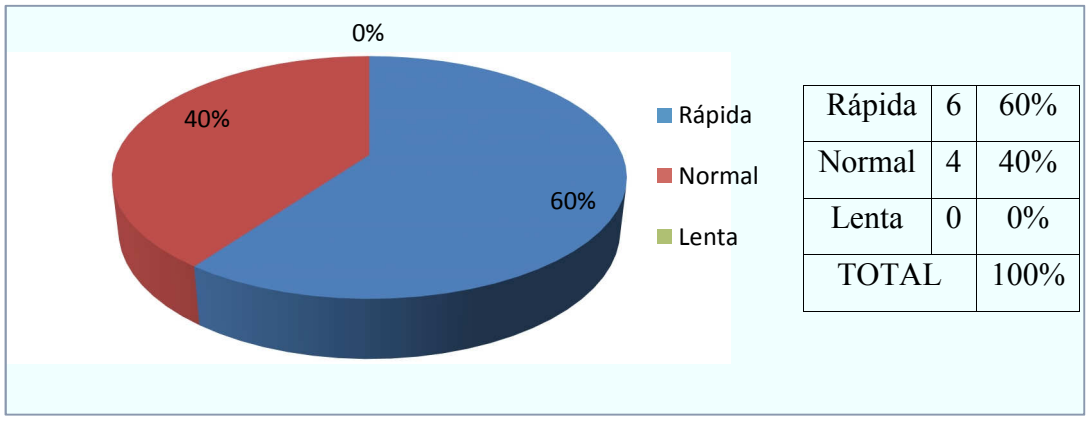
El 70% que corresponde a 7 votos.
El 10% que corresponde a 1 voto.
El 20% que corresponde a 2 votos.

Los resultados exponen que el 70% de clientes tienen acceso de servicio de internet vía inalámbrica, y un 20% tienen vía alámbrica, y solo un 10% no sabe qué tipo de acceso tiene.

Interpretación

El porcentaje de usuarios de la red que saben el tipo de conexión que disponen es alto; aunque, efectivamente se disponga de 6 conexiones inalámbricas por parte de la empresa hacia sus usuarios, es importante tener en cuenta esta información.

2. ¿La velocidad de navegación que usted percibe es?



Rápida	6	60%
Normal	4	40%
Lenta	0	0%
TOTAL		100%

Figura 4.2 Percepción de velocidad de navegación.
Realizado: Carlos Ailaca

El 60% que corresponde a 6 votos.

El 40% que corresponde a 4 votos.

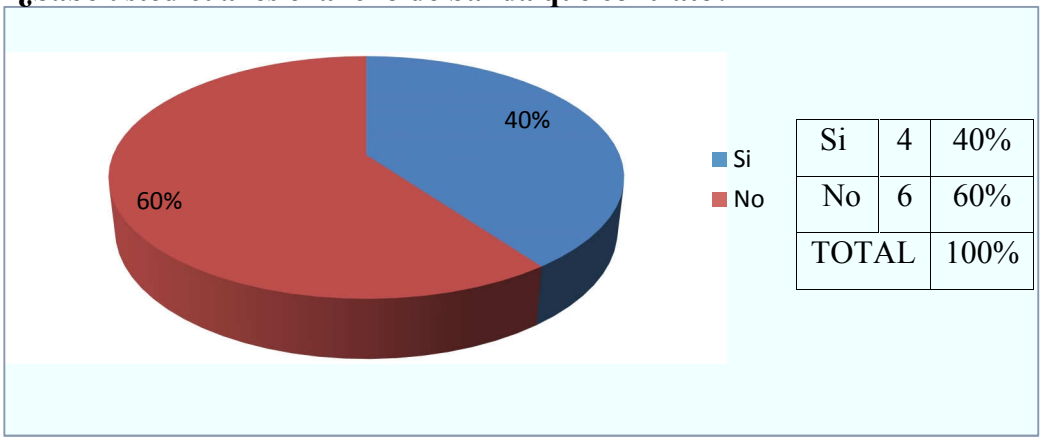
El 0% que corresponde a 0 votos.

Estos resultados demuestran que un 60% de los clientes perciben una navegación rápida de internet, y un 40% que es normal, nadie percibe que sea lenta.

Interpretación

La navegación en Internet es percibida como rápida para la mayoría de usuarios, y nadie percibe que sea lenta, dando a notar que los dispositivos de red (router, switch) de la empresa satisfacen las necesidades requeridas, no interfiriendo en la normal navegación en Internet.

3. ¿Sabe usted cual es el ancho de banda que contrato?



Si	4	40%
No	6	60%
TOTAL		100%

Figura 4.3 Conocimiento de ancho de banda contratado.
Realizado: Carlos Ailaca

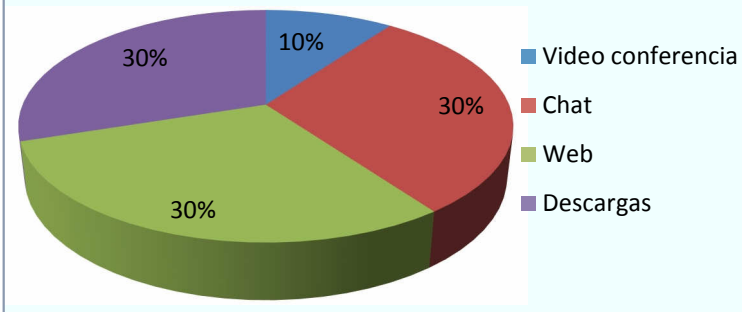
El 40% que corresponde a 4 votos.
El 60% que corresponde a 6 votos.

Los resultados explican que el 40% sabe el ancho de banda que ha contratado, mientras que el 60% no lo sabe.

Interpretación

Demuestra que la mayoría de usuarios no sabe qué tipo de ancho de banda contrataron; aunque, en la actualidad toda la red cuenta con un acceso a Internet de ancho de banda de 2Mbps;

4. ¿Qué servicios de internet usa con frecuencia?



Video conferencia	2	10%
Chat	6	30%
Web	6	30%
Descargas	6	30%
TOTAL		100%

Figura 4.4 Frecuencia de uso de servicios de internet.
Realizado: Carlos Ailaca

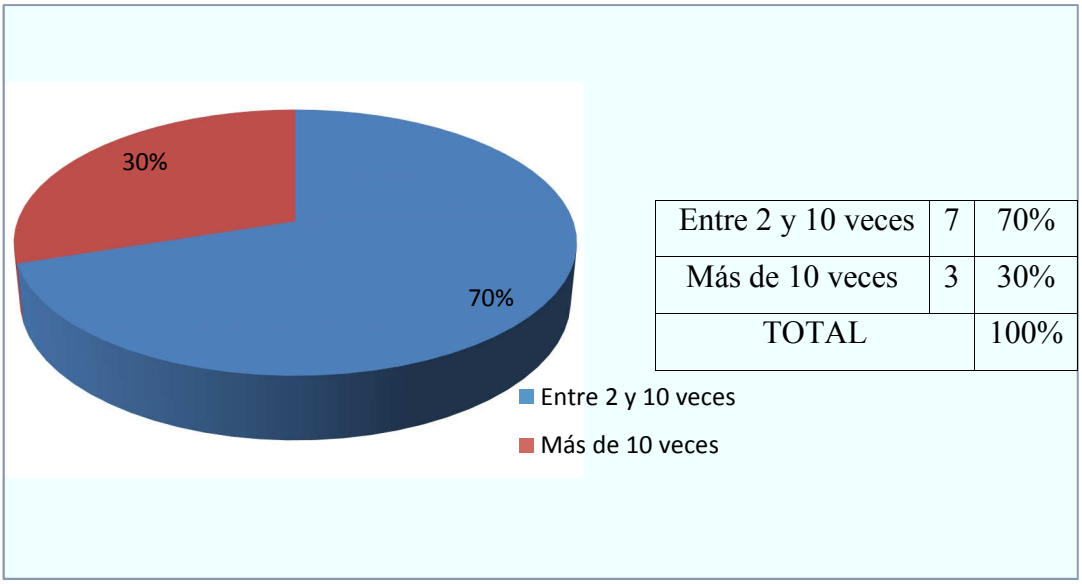
El 10% que corresponde a 2 votos.
El 30% que corresponde a 6 votos.
El 30% que corresponde a 6 votos.
El 30% que corresponde a 6 votos.

Estos resultados señalan que el 20% utiliza el servicio de internet para video conferencia, el 30% lo utiliza para chat, otro 30% para Web y otro 30% lo utilizan para descargas.

Interpretación

La mayoría de usuarios tienen un uso relativamente normal de los servicios de internet; aunque, hay que tener presente que los usuarios que utilizan los servicios de video conferencia y descargas con frecuencia pueden afectar en el rendimiento de la red.

5. ¿Cuántas veces al día accede a internet?



Entre 2 y 10 veces	7	70%
Más de 10 veces	3	30%
TOTAL		100%

Figura 4.5 Acceso por día a internet.
Realizado: Carlos Ailaca

El 70% que corresponde a 7 votos.

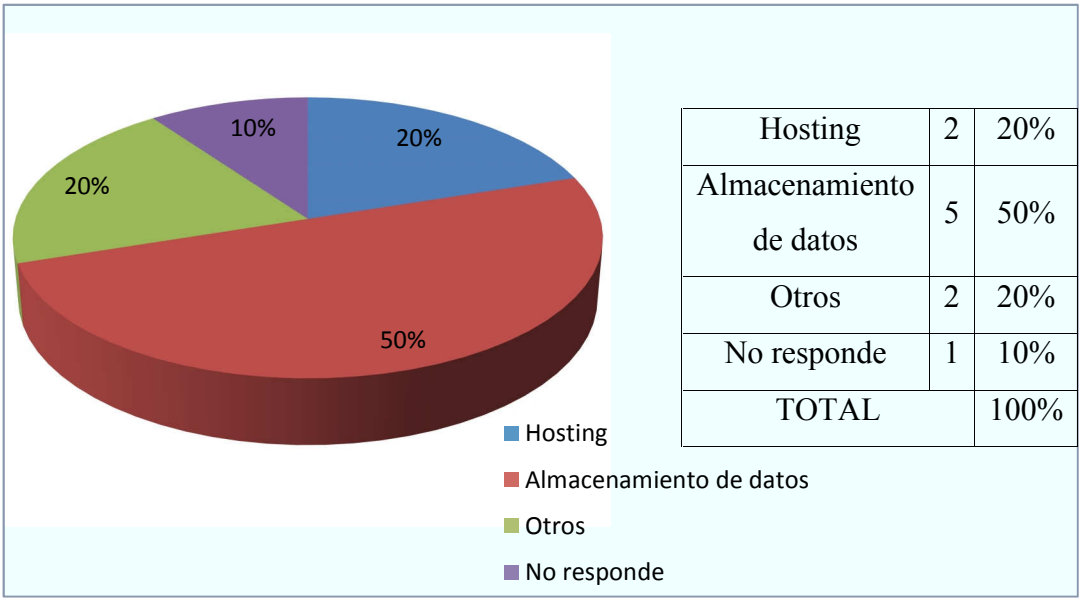
El 30% que corresponde a 3 votos.

Los resultados indican que el 70% accede a internet de entre 2 a 10 veces al día, mientras que un 30% lo hace más de 10 veces al día.

Interpretación

Los datos demuestran que el acceso a Internet por la mayoría de los usuarios de la red es moderada; aunque, el menor porcentaje de usuarios realizan un acceso a Internet con una utilización alta; se evidencia la necesidad de un control en la red.

6. ¿Qué otro tipo de servicio requeriría en un futuro?



Hosting	2	20%
Almacenamiento de datos	5	50%
Otros	2	20%
No responde	1	10%
TOTAL		100%

Figura 4.1 Servicios requeridos en un futuro.
Realizado: Carlos Ailaca

El 20% que corresponde a 2 votos.

El 50% que corresponde a 5 votos.

El 20% que corresponde a 2 votos.

El 10% que corresponde a 1 voto.

Estos resultados demuestran que un 20% desearía en un futuro Hosting, un 50% desearía el almacenamiento de datos, otro 20% desearía otro tipo de servicio y un 10% no responde.

Interpretación

Los datos demuestran que la mitad de los usuarios en un futuro requerirían usar un servicio de almacenamiento de datos vía red; dando, una información considerable para la empresa en sus planificaciones posteriores.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones:

De acuerdo a la investigación y el análisis realizado se presentan las siguientes conclusiones:

- A pesar que a los usuarios de Internet de la empresa Intercompu, a los cuales se distribuye el servicio, no señalan que su conexión otorgada tenga problemas, a la empresa le es vital controlar el tráfico de red y el ancho de banda asignada a cada usuario; tanto para su red alámbrica como para su red inalámbrica.
- La flexibilidad y versatilidad que las redes inalámbricas brindan, permite lograr la incorporación de más usuarios a la red de una forma sencilla, por tal motivo el gerente de la empresa Intercompu desea ampliar el servicio; pero, esto también acarrea problemas de seguridad, debido al modo de conexión por medio de ondas electromagnéticas, temiendo que cualquier usuario no autorizado con conocimientos prácticos de informática pudiera acceder de manera ilegal a la red de Intercompu en la actualidad.
- La empresa Intercompu no posee un control y monitoreo de los servicios de red, ni de la distribución de internet, por consiguiente la optimización de los recursos disponibles es primordial, sin embargo las formas de monitorear una red dependerá en muchas ocasiones de la capacidad económica que tenga la empresa en la adquisición de equipos para lograr este propósito, teniendo en cuenta que se puede hacerlo de manera activa o pasiva según las necesidades.

- Se pudo observar que la empresa distribuye Internet de una manera informal, a sus usuarios más cercanos en un radio de 53m; debido a la característica de la red y a la señal inalámbrica la cual no abarca una extensión geográfica extensa, la señal es interceptada por los usuarios que receptan la SSID (Service Set IDentifier / Identificador de servicio) y al otorgarles la clave acceden a la red.

5.2 Recomendaciones:

- Hay que tener en cuenta cuales son los servicios de internet más usados para poder obtener un control eficaz del tráfico en la red, a pesar que los usuarios no tengan en cuenta que ancho de banda contrataron la navegación de internet debe ser óptimo.
- El tener presente la seguridad en la red alámbrica e inalámbrica de la empresa es un asunto de importancia, se debería considerar las mejores herramientas en el control específicamente de la red inalámbrica ya que por su naturaleza es más vulnerable.
- El conocer los factores que se desea monitorear en la red como el estado del enlace, el tráfico en la red entre otras cosas son esenciales, los equipos que van a interactuar para este propósito deben cumplir con las características optimas de operación.
- Es necesario que la empresa realice la formalización de la distribución del servicio de Internet con las autoridades pertinentes, al no hacerlo puede acarearle a la empresa drásticas sanciones y para poder implementar un proyecto que abarque una área geográfica más extensa es necesario otro tipo de estudio referente a formación ISP (Proveedor de servicios de Internet).

CAPÍTULO VI

PROPUESTA

6.1 Datos informativos

Nombre del proyecto:

"SISTEMA DE MONITOREO Y CONTROL DE REDES INALÁMBRICAS PARA OPTIMIZAR EL SERVICIO DE INTERNET DE LA EMPRESA INTERCOMPU"

Empresa: Intercompu.

Ciudad: Ambato.

Dirección: Av. Bolivariana 2-13 y Provincia de Pastaza.

Investigador: Carlos Vinicio Ailaca Ramírez.

Tutor: Ing. M.Sc. Marco Jurado

6.2 Antecedentes de la propuesta

El creciente avance de la tecnología inalámbrica en el campo de las comunicaciones ha mejorado el acceso y optimizado los recursos en las redes de computadores, en la actualidad ha conseguido ser muy requerida en las redes empresariales por su flexibilidad, y por la capacidad de adaptarse fácilmente a la movilidad; teniendo en cuenta este principio la red inalámbrica de la empresa Intercompu fue enfocada a solucionar el problema de conectividad para sus usuarios que se encuentran alrededor de la empresa; y que tenían como dificultad

la extensión de cables para su conexión. En el presente los enlaces inalámbricos existentes han aumentado teniendo la necesidad de establecer un control al tráfico y la seguridad en la red inalámbrica; recientemente los costes de los dispositivos y equipos tendieron a bajar por lo que la empresa innovo sus equipos de comunicación pero no ha establecido el control requerido.

Con el aumento de las conexiones inalámbricas hacia los usuarios, se ha hecho evidente para la empresa la necesidad de implementar un sistema que realice un monitoreo del estado de la red, mejorando los controles y aplicaciones que vinculen al desenvolvimiento normal en la actividad de la red, teniendo presente que en los enlaces inalámbricos actuales la vulnerabilidad es latente y cualquier agente externo a la empresa puede interceptar las ondas de radiofrecuencias emitidas por los equipos de comunicación inalámbrica, aunque están configurados con las seguridades normales implementadas en los dispositivos de comunicación en el presente estas seguridades ya no son suficientes.

Basándose en el desarrollo y mejoras de la tecnología inalámbrica, la empresa Intercompu ha considerado la incorporación de un sistemas de monitoreo y control de su red tanto alámbrica como inalámbrica, teniendo estimado que existe un sinnúmero de herramientas disponibles para el control y monitoreo de redes tanto de tipo LAN como redes WAN y MAN respectivamente; en las telecomunicaciones, y específicamente en el campo de las redes basadas en la conmutación de paquetes. La iniciativa que está presente en este trabajo, incluye como requisito indispensable y planteado como objetivo personal; sea cualquier herramienta o herramientas escogidas para cumplir el objetivo general de este trabajo, dicha herramienta, debe ser desarrollada utilizando software de código abierto basado en GNU (General Public License).

6.3 Justificación

La importancia de éste proyecto está sustentado en la necesidad de distribuir internet de una manera ordenada y confiable a usuarios que por diferentes circunstancias, ya sea de tipo técnico o lógico no pudieron conseguirlo. Los

diferentes mecanismos para el correcto control y seguridad de la red inalámbrica fue el motivo de este proyecto.

La implementación de un sistema de monitoreo y control de redes inalámbricas para optimizar el servicio de internet de la empresa Intercompu; se estructuró de manera técnica-metodológica, priorizando las necesidades de la empresa y usuarios.

El sistema de monitoreo y control de redes inalámbricas, fue respaldado con la tecnología adecuada para su propósito. Teniendo la estructura metodológica necesaria para establecer las etapas requeridas para el ajuste del sistema de monitoreo y control de redes inalámbricas en la empresa Intercompu.

Este trabajo se enfocó en la manipulación de las redes inalámbricas con el fin de obtener un control de las actividades de red tales como tráfico, ancho de banda, y seguridad. Una vez determinada la red en la empresa Intercompu y equipos disponibles se consideró la implementación de un sistema de monitoreo y control idóneo para las necesidades existentes. Dando como resultado un sistema de monitoreo y control pasivo, con el que se optimizará los recursos existentes.

6.4 Objetivos

6.4.1 Objetivo general

- Implementar en la red inalámbrica un sistema pasivo de monitoreo y control utilizando software libre para distribuir de forma segura el servicio de Internet en la empresa Intercompu.

6.4.2 Objetivos específicos

- Analizar el estado actual de la red de la empresa Intercompu.
- Determinar las herramientas necesarias para el sistema de control y monitoreo pasivo en redes inalámbricas seguras.
- Implementar el sistema pasivo de control y monitoreo en forma física y lógica, eficiente para la distribución del servicio de Internet en la empresa Intercompu.

6.5 Análisis de factibilidad

6.5.1 Factibilidad operativa

El presente trabajo es factible operativamente debido a que cuenta con todos los elementos necesarios para su manejo, el sistema de monitoreo de red se lo implementó sobre software libre procurando la atención en los enlaces inalámbricos; los equipos que se inspeccionan se encuentran en la empresa, el administrador de red debe poseer conocimientos básicos sobre el manejo de software libre.

6.5.2 Factibilidad económica

El proyecto es factible en lo económico, los recursos necesarios para su normal desempeño existen y están a disposición. El beneficio adquirido para la empresa se presenta al momento en que se eligió la plataforma de software libre para implementar este proyecto debido a su reducido costo y gran soporte ya que existe una comunidad mundial que mantiene el software.

6.5.3 Factibilidad técnica

El proyecto tiene la factibilidad técnica, existe el hardware y software necesarios para la implementación del sistema de monitoreo, los requerimientos técnicos de este proyecto están supeditados por el software a implementarse para obtener un funcionamiento óptimo.

6.6 Fundamentación

6.6.1 Análisis de la red de Intercompu

Introducción

Para abordar la explicación de este proyecto en forma correcta, se debería primero analizar el estado actual en el que se encuentra la red de Intercompu, se presentará de una manera global y detallada los aspectos que interesan saber sobre la red de la empresa Intercompu, obteniendo de esta forma los problemas reales de esta red,

procurando observar las debilidades y fortalezas de la misma y así llegar a optar por soluciones adecuadas, y optimizando los recursos disponibles.

La red de Intercompu tanto LAN como WLAN, está configurada de manera doméstica, pero aun así ha logrado satisfacer las necesidades requeridas por los usuarios.

6.6.1.1 Descripción de la red

La red actual implementada en la empresa Intercompu está conformada por un dispositivo de Telecomunicaciones para la conexión a Internet, que consiste en un modem-router de marca Huawei modelo EchoLife HG520c, el cual es instalado por la Corporación Nacional de Telecomunicaciones (CNT), este dispositivo cuenta con cuatro puertos RJ45 fastethernet 10/100 Base T y un puerto RJ11 para realizar la conexión de internet por vía telefónica mediante el servicio de ADSL[5]. Además cuenta este modelo con tecnología inalámbrica y una antena dipolo de 2.5dBi de ganancia para proveer de conectividad inalámbrica el cual se encuentra desactivado.

El modem Huawei se encuentra conectado a un router inalámbrico de marca TRENDnet modelo TEW-639GR el cual posee cuatro puertos LAN RJ45 fastethernet 10/100/1000 y un puerto WAN RJ45 y conexión inalámbrica bajo el estándar 802.11b/g/n por medio de sus tres antenas de 4dBi de ganancia este a la vez se encuentra conectado hacia un switch de marca D-Link modelo DES-1008D con ocho puertos RJ45 fastethernet 10/100 el cual distribuye el internet a través de cuatro puertos para los dos computadores de laboratorio , uno de gerencia y uno para contabilidad; usando un puerto para conectar a un access point de marca D-Link modelo DWL-2100AP con una antena de 5dBi de ganancia otro puerto que conecta a otro switch de marca NEXXT Solutions con ocho puertos fastethernet 10/100 y el ultimo puerto disponible del switch D-Link conecta a un computador de un cliente, el switch NEXXT Solución conecta a dos clientes y dos

[5]ADSL: Asymmetric Digital Subscriber Line o línea de abonado digital asimétrica es un tipo de tecnólogia de línea DSL. Consiste en una transmisión analógica de datos digitales apoyada en el par simétrico de cobre, no debe superar los 5,5Km medidos desde la Central Telefónica.

computadores de la área técnica. En la figura 6.1 se muestra un diagrama de la red actual de la empresa Intercompu.

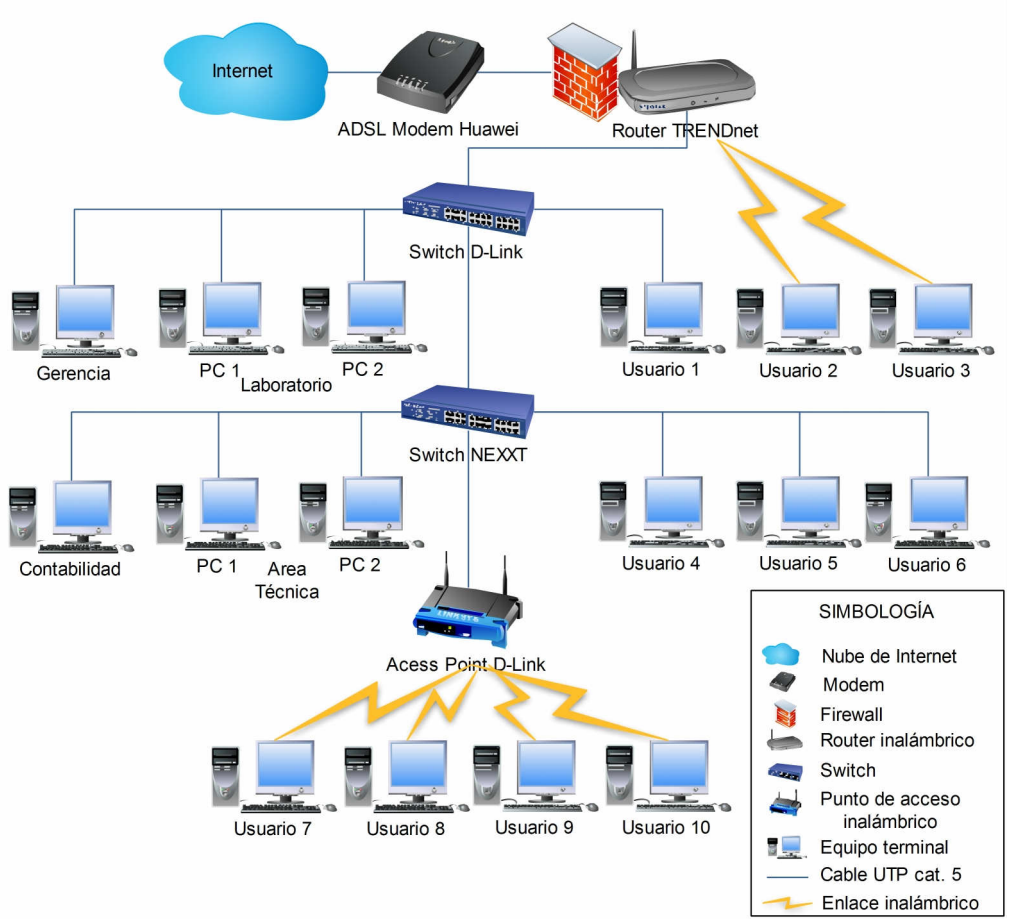


Figura 6.1 Diagrama de la red actual de Intercompu.
Realizado: Carlos Ailaca

6.6.1.2 Funcionamiento de la red

La empresa Intercompu tiene contratado con la CNT un ancho de banda de 2Mbps para línea telefónica comercial por medio de la tecnología ADSL. La CNT instaló un modem router Huawei con acceso permanente a internet de banda ancha. Este modem está configurado predeterminadamente por la CNT y activado el servicio DHCP para cinco máquinas, la configuración WAN es controlada vía red por la CNT y la configuración para la red interna fue modificada desactivando el servicio de conexión inalámbrica; la red interna LAN configurada cuenta con el servicio de DHCP a partir de la IP 192.168.1.2 hasta la IP 192.168.1.6 teniendo como puerta de enlace la IP 192.168.1.1. Conectado al router inalámbrico usando la IP 192.168.1.2

Los DNS (Sistema de Nombres de Dominio) para la WAN tanto primario como secundario son 186.42.193.2 y 200.107.10.52 respectivamente; la NAT (Network Address Translation) esta activada, no así el firewall que se encuentra desactivado.

En el router inalámbrico TRENDnet está configurado de manera que obtenga automáticamente la IP por parte del modem para tener el acceso a internet, mientras que la configuración para la red interna LAN de la misma forma que en el modem el servicio de DHCP (Protocolo de Configuración Dinámica de Host) está activado generando IP desde 192.168.20.100 hasta la IP 192.168.20.200, renovando las IP cada día para los diferentes equipos que estén conectados en la red y con una IP 192.168.20.1 como puerta de enlace.

El servicio inalámbrico del router está configurado para que opere en la frecuencia 2.4GHz con un modo compatible para los estándares 802.11 b, g y n. Trabajando en el canal de frecuencia 6 (2437MHz).

El router inalámbrico TRENDnet es el que administra la red de Intercompu, se encuentra activado el firewall y se conecta a los switchs y al Access Point los cuales se encargan de distribuir a las máquinas el servicio de internet.

El Access Point D-Link esta conecto normalmente al switch nexxt, trabaja en la frecuencia de 2.4 GHz bajo el estándar 802.11g y en el canal de transmisión 3.

Los dos puntos de enlaces inalámbricos proporcionados tanto por el router inalámbrico como por el Access Point con el aumento de una antena de 5dBi, ha permitido las conexiones en los alrededores de la empresa; teniendo en cuenta que el Access Point tiene una función especial de trabajar en modo turbo lo cual al activarla adquiere un aumento de la capacidad de transmitir de 54MBps a 108MBps y también mejorando la potencia de transmisión a tres máquinas que se conectan de manera inalámbrica se incorporó una tarjeta de red que aprovecha esta función especial debido a su distancia y capacidad de cobertura del Access Point.

6.6.1.3 Cobertura de accesos inalámbricos de la red Intercompu

Los accesos inalámbricos de la red que la empresa Intercompu realiza a los usuarios que se ubican alrededor de la empresa, están sujetados a las tecnologías de redes WiFi las cuales están bajo los estándares 802.11 anteriormente descritas, permitiendo así el funcionamiento de los dispositivos para la transmisión inalámbrica de la empresa.

A continuación en la figura 6.2 se mostrará el rango efectivo de las radiaciones inalámbricas en la frecuencia de 2.4GHz tanto en el estándar IEEE 802.11g como en el estándar IEEE 802.11n de los diferentes dispositivos implementados actualmente en la empresa Intercompu.

Figura 6.2 Rango efectivo de radiaciones inalámbricas red Intercompu.
Realizado: Carlos Ailaca

La señal del router inalámbrico TRENDnet circunscribe el circulo externo color amarillo, teniendo una potencia de la señal del 65% en vista directa a una distancia de 53m, esta calidad de la señal varía dependiendo los obstáculos que se encuentran como edificaciones, donde la potencia de la señal baja un 20% al 35%.

Mientras que la señal del Access Point D-link que circunscribe el circulo interno color rojo, tiene una potencia de la señal del 60% en configuración normal a una distancia de 20m en vista directa, con la antena de 2.5 dBi y al aumentar la

ganancia de la antena cambiándole por una antena de 5 dBi la potencia de la señal marca 70% a la misma distancia en vista directa. Las variaciones de la potencia de la señal por obstáculos es este caso son mucho más notorias que las del router; la potencia de la señal baja en un rango de 35% al 45%.

Estas mediciones se las realizó con el programa Xirrus Wi-Fi Monitor versión 1.1 instalado en una portátil Acer con sistema operativo Windows 7.

6.6.2 Estándar IEEE 802.11 - Aspectos técnicos

El estándar 802.11 para redes LAN inalámbricas incluye una serie de enmiendas. Las enmiendas contemplan principalmente las técnicas de modulación, gama de frecuencia y la calidad del servicio (QoS). Como todos los estándares 802 del IEEE, el IEEE 802.11 cubre las primeras dos capas del modelo de OSI (Open Systems Interconnection), es decir la capa física (L1) y la capa de enlace (L2).

La sección siguiente describirá lo que implica cada una de esas capas en términos de estándares inalámbricos.

6.6.2.1 Capa 1 (802.11 PHY)

La PHY (Physical layer/ capa física) tiene como finalidad transportar correctamente la señal que corresponde a 0 y 1 de los datos que el transmisor desea enviar al receptor. Esta capa se encarga principalmente de la modulación y codificación de los datos.

Técnicas de modulación

Un aspecto importante que influencia la transferencia de datos es la técnica de modulación elegida. A medida que los datos se codifican más eficientemente, se logran tasas o flujos de bits mayores dentro del mismo ancho de banda, pero se requiere hardware más sofisticado para manejar la modulación y la demodulación de los datos.

La idea básica detrás de las diversas técnicas de modulación usadas en IEEE 802.11 es utilizar más ancho de banda del mínimo necesario para mandar un “bit” a fin de conseguir protección contra la interferencia. La manera de esparcir la

información conduce a diversas técnicas de modulación. Las técnicas de modulación que se utilizan en los dispositivos de la empresa son las siguientes:

DSSS (Direct Sequence Spread Spectrum)

El DSSS (espectro esparcido por secuencia directa) implica que para cada bit de datos, una secuencia de bits (llamada secuencia seudoaleatoria, identificada en inglés como PN) debe ser transmitida. Cada bit correspondiente a un 1 es substituido por una secuencia de bits específica y el bit igual a 0 es substituido por su complemento. El estándar de la capa física 802.11 define una secuencia de 11 bits (10110111000) para representar un "1" y su complemento (01001000111) para representar un "0". En DSSS, en lugar de esparcir los datos en diferentes frecuencias, cada bit se codifica en una secuencia de impulsos más cortos, llamados chips, de manera que los 11 chips en que se ha dividido cada bit original ocupan el mismo intervalo de tiempo. Esta técnica de modulación ha sido común desde el año 1999 al 2005.

OFDM (Orthogonal Frequency-Division Multiplexing)

OFDM (modulación por división de frecuencias ortogonales), algunas veces llamada modulación multitono discreta (DMT) es una técnica de modulación basada en la idea de la multiplexación de división de frecuencia (FDM). FDM, que se utiliza en radio y TV, se basa en el concepto de enviar múltiples señales simultáneamente pero en diversas frecuencias.

En OFDM, un sólo transmisor transmite en muchas (de docenas a millares) frecuencias ortogonales. El término ortogonal se refiere al establecimiento de una relación de fase específica entre las diferentes frecuencias para minimizar la interferencia entre ellas.

Una señal OFDM es la suma de un número de subportadoras ortogonales, donde cada subportadora se modula independientemente usando QAM (modulación de fase y amplitud) o PSK (modulación de fase). Esta técnica de modulación es la más común a partir del 2005.

Frecuencia

Los estándares 802.11b y la 802.11g usan la banda de los 2,4GHz ISM[6] definida por la UIT (Unión Internacional de Telecomunicaciones). Los límites exactos de esta banda dependen de las regulaciones de cada país, pero el intervalo que se encuentra en los equipos es el más comúnmente aceptado que va desde 2,4GHz a 2,4835GHz.

La banda sin licencia de los 2.4GHz se volvió últimamente muy "ruidosa" en áreas urbanas, debido a la alta penetración de las WLAN y otros dispositivos que utilizan el mismo rango de frecuencia, tal como hornos de microondas, teléfonos inalámbricos y dispositivos Bluetooth. La banda de los 5GHz tiene la ventaja de tener menos interferencia, pero presenta otros problemas debido a su naturaleza.

Las ondas de alta frecuencia son más sensibles a la absorción que las ondas de baja frecuencia. Las ondas en el rango de los 5GHz son especialmente sensibles al agua, a los edificios circundantes u otros objetos, debido a la alta absorción en este rango. Esto significa que una red 802.11a es más restrictiva en cuanto a la línea de la vista y se requieren más puntos de acceso para cubrir la misma área que una red 802.11b. Para la misma potencia de transmisión las celdas resultantes son más pequeñas.

6.6.2.2 Capa 2 (802.11 MAC)

La capa de transmisión de datos de 802.11, se compone de dos partes:

1. Control de acceso al medio (MAC)
2. Control lógico del enlace (LLC)

La subcapa LLC de 802.11 es idéntica a la de 802.2 permitiendo una compatibilidad con cualquier otra red 802, mientras que la subcapa MAC presenta cambios sustanciales para adecuarla al medio inalámbrico.

La subcapa MAC (L2) es común para varios de los estándares 802.11, y sustituye al estándar 802.3 (CSMA/CD – Ethernet) utilizado en redes cableadas, con

[6] ISM: Industrial, Scientific and Medical; son bandas reservadas internacionalmente para uso no comercial de radiofrecuencia electromagnética en áreas industrial, científica y médica.

funcionalidades específicas para radio (los errores de trasmisión son más frecuentes que en los medios de cobre), como fragmentación, control de error (CRC-Cyclic Redundancy Check), las retransmisiones de tramas y acuse de recibo, que en las redes cableadas son responsabilidad de las capas superiores.

Método de acceso al medio

El protocolo de acceso al medio en redes Ethernet cableadas es el CSMA/CD, basado en la detección de colisiones y la subsiguiente retransmisión cuando éstas ocurren. En redes inalámbricas que utilizan la misma frecuencia para transmitir y recibir, es imposible detectar las colisiones en el medio, por lo que el mecanismo de compartición del medio se modifica tratando de limitar las colisiones y usando acuse de recibo (ACK) para indicar la recepción exitosa de una trama. Si el transmisor no recibe el ACK dentro de un tiempo preestablecido, supone que la transmisión no fue exitosa y la reenvía. Este protocolo se conoce como CSMA/CA, donde CA se refiere a "Collision Avoidance", es decir, tratar de evitar las colisiones. Este método no es tan eficiente como el CSMA/CD porque hay que esperar el ACK antes de poder continuar utilizando el canal, y el mismo ACK consume tiempo de transmisión.

Además, para transmisión a grandes distancias el tiempo de espera por el ACK puede ser significativo debido a que las ondas de radio tardan 2ms en ir y volver a una distancia de 300Km. Esencialmente, CSMA/CA utiliza unos tiempos de espera obligatorios de longitud variable entre tramas sucesivas para evitar las colisiones. Estos tiempos se denominan espaciamiento entre tramas, "Interframe Spacing", y su valor depende del estado previo del canal. Opcionalmente también se pueden utilizar mecanismos de reserva del canal, en una técnica conocida como RTS/CTS (Ready to Send/Clear to Send) que garantiza el acceso al medio a expensas de tiempos de transmisión aún más largos.

El acceso al medio es controlado por el uso de diversos tipos de interframe spaces (IFS) o espacio entre tramas, que corresponde a los intervalos de tiempo que una estación necesita esperar antes de enviar datos. Los datos prioritarios como

paquetes de ACKs o de RTS/CTS esperarán un período más corto (SIFS) que el tráfico normal.

Por estos motivos nunca se puede lograr que el 802.11b tenga un rendimiento tan bueno como el CSMA/CD o tecnologías basadas en TDMA (Time division Multiple Access/Acceso Múltiple por División de Tiempo).

6.6.2.3 Enmiendas de IEEE 802.11

Las enmiendas más aceptadas de la familia de IEE 802.11 son actualmente las b, a, y g. Todas ellas han alcanzado los mercados masivos con productos de costo accesibles. Otras enmiendas son [c-f], [h-j], n y s que son correcciones, actualizaciones o extensiones de las anteriores. Se describirá un poco las b, g, s y n.

IEEE 802.11b

IEEE 802.11b incluye mejoras del estándar original 802.11 para el soporte de tasas de transmisión más elevadas (5,5 y 11Mbit/s). IEEE 802.11b usa el mismo método de acceso y la misma técnica DSSS definidas en el estándar IEEE 802.11 original.

Un dispositivo basado en IEEE 802.11b puede transmitir hasta 11 Mbit/s, y reducirá automáticamente su tasa de transmisión cuando el receptor empiece a detectar errores, sea debido a la interferencia o a la atenuación del canal, cayendo a 5,5Mbit/s, después a 2, hasta llegar a 1 Mbit/s, cuando el canal sea muy ruidoso. Las tasas de transmisiones de datos más bajas son menos sensibles a la interferencia y a la atenuación puesto que están utilizando un método más redundante para codificar los datos (las exigencias de relación de señal y ruido son menos exigentes a tasas de transferencias de datos más bajas).

IEEE 802.11g

En junio de 2003, se ratificó una tercera enmienda al estándar 802.11 con la denominación de IEEE 802.11g y funciona en la misma banda del 802.11b.

802.11g usa la misma técnica de modulación que el 802.11a (ODFM) por lo tanto funciona con una tasa máxima de transferencia de datos de 54 Mbit/s. Para asegurar la interoperabilidad con el 802.11b, en las tasas de datos de los 5,5 y los 11Mbps se revierte a CCK+DSSS (como 802.11b) y usa DBPSK/DQPSK + DSSS para tasas de transferencias de 1 y 2 Mbps.

La interoperabilidad 802.11g con 802.11b es una de las razones principales de su masiva aceptación. Sin embargo, sufre el mismo problema en 802.11b con respecto a interferencia (demasiados puntos de acceso urbanos) puesto que funcionan en la misma banda de frecuencia.

IEEE 802.11s

IEEE 802.11s es el estándar en desarrollo para redes Wi-Fi malladas, también conocidas como redes Mesh. La malla es una topología de red en la que cada nodo está conectado a uno o más nodos. De esta manera es posible llevar los mensajes de un nodo a otro por diferentes caminos.

Según la normativa 802.11 actual, una infraestructura Wi-Fi compleja se interconecta usando LANs fijas de tipo Ethernet. 802.11s pretende responder a la fuerte demanda de infraestructuras WLAN móviles con un protocolo para la autoconfiguración de rutas entre puntos de acceso mediante topologías multisalto. Dicha topología constituirá un WDS (Wireless Distribution System) que deberá soportar tráfico unicast, multicast y broadcast. Para ello se realizarán modificaciones en las capas PHY y MAC de 802.11 y se sustituirá la especificación BSS (Basic Service Set) actual por una más compleja conocida como ESS (Extended Service Set). En noviembre de 2006 aparecieron los primeros borradores.

IEEE 802.11n

La última enmienda del 802.11 es IEEE 802.11n apunta a alcanzar una tasa teórica de 600 Mbit/s que sería 40 veces más rápida que la de 802.11b y 10 veces más que la de 802.11a o la 802.11g. La norma 802.11n aprovecha muchas de las enmiendas previas pero la gran diferencia es la introducción del concepto de

MIMO[7]. MIMO implica utilizar varios transmisores y múltiples receptores para aumentar la tasa de transferencia y el alcance.

IEEE 802.11e

Con el estándar 802.11e, la tecnología IEEE 802.11 soporta tráfico en tiempo real en todo tipo de entornos y situaciones. Su objetivo es introducir nuevos mecanismos a nivel de la capa MAC para soportar los servicios que requieren garantías de QoS (Quality of Service), por lo que es de importancia crítica para aplicaciones sensibles a retrasos temporales como la VoIP y el streaming multimedia. Gracias a este estándar será posible, por ejemplo, utilizar aplicaciones de VoIP o sistemas de vídeovigilancia de alta calidad con infraestructura inalámbrica.

Para cumplir con su objetivo, IEEE 802.11e emplea una nueva técnica llamada HCF (Hybrid Coordination Function), que define dos formas de acceder al canal, EDCA y HCCA, cada una de las cuales puede llevar asociadas varias clases de tráfico.

IEEE 802.11i

Este estándar está dirigido a batir la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación, especialmente en WEP. El estándar abarca los protocolos 802.1x, TKIP (Protocolo de Claves Integra – Seguras – Temporales), y AES (Estándar de Cifrado Avanzado). Se implementa un subconjunto de este estándar en WPA y totalmente en WPA2. El estándar 802.11i fue ratificado en Junio de 2004.

Diversidad Espacial

MIMO aprovecha la propagación por multitrayectoria para mejorar el rendimiento (o para reducir la tasa de errores) en vez de tratar de eliminar los efectos de las reflexiones en el trayecto de propagación como hacen los otros estándares. En

[7] MIMO: Es el acrónimo en inglés de Multiple-input Multiple-output (en español, Múltiple entrada múltiple salida). Se refiere específicamente a la forma como son manejadas las ondas de transmisión y recepción en antenas para dispositivos inalámbricos como enrutadores.

términos simples, MIMO se aprovecha de lo que otros estándares consideran como obstáculo a la multitrayectoria.

Cuando una señal de radio es enviada por el aire, puede alcanzar al receptor a través de diferentes trayectos El receptor recibe primero la señal directa de línea de vista y un tiempo después, ecos y fragmentos de la señal que ha sido reflejada en edificios o en otros obstáculos. Normalmente, estos ecos y fragmentos son vistos como ruido de la señal buscada, pero MIMO es capaz de usar esa información proveniente de trayectos indirectos para mejorar la señal principal. Esto resulta en una señal más limpia (menos ruido) y alcance mayor. Inclusive, a distancias cortas, es posible la transmisión aun cuando la línea de vista esté bloqueada, cosa muy difícil con las versiones anteriores de 802.11. Esto se conoce como transmisión sin línea de vista (NLOS: Non Line of Sight).

Multiplexación por división espacial (SDM)

Otra característica que MIMO incluye es el uso de muchos transmisores para la misma secuencia de datos, de ahí la llamada multiplexación por división espacial (SDM). Un conjunto de secuencias de datos independientes se envía dentro de un mismo canal, aumentando así el rendimiento de la transmisión en proporción al número de secuencias empleadas. Puesto que MIMO requiere antenas y procesamiento adicional, necesariamente los equipos que lo emplean son más costosos.

6.6.2.4 Rango y Cobertura

EEE 802.11 es un protocolo para LAN inalámbrica (uso interior) que fue diseñado para operar en pequeñas celdas (hasta 100 metros).En la fase de diseño nunca fue considerado rendimiento pobre en enlaces a distancias largas, y sufre además del problema del “nodo oculto (hidden node)”.

El método de acceso en IEEE 802.11 (CSMA/CA) supone que todos los nodos que se están comunicando con el punto de acceso pueden “oírse” entre sí y se basa en esto para evitar colisiones. Las colisiones en IEEE 802.11 pueden ser evitadas si todos los nodos pueden detectar con eficacia si se ocupa el canal o no.

Desafortunadamente, este requerimiento no siempre puede ser satisfecho cuando se implementa el IEEE 802.11 en ambientes abiertos.

Cuando más de 10 (algunos dicen 20) estaciones están asociadas al mismo punto de acceso y la tasa de colisiones aumenta, los tiempos de espera para el acceso al medio y las retransmisiones introducen demoras considerables que disminuyen el rendimiento efectivo.

IEEE 802.11 funciona mal cuando muchos usuarios son asociados a un punto de acceso en un ambiente exterior. Para resolver algunos de estos problemas, ciertos fabricantes ofrecen soluciones no estándar basadas el "sondeo del cliente" o reservación de ancho de banda controlándolo desde la capa IP. En el sondeo, el punto de acceso decide en qué momento se concede a una estación el uso del canal. El problema de "nodo oculto" no es nada nuevo y tan pronto como el IEEE 802.11 fue estandarizado se propusieron modificaciones en el MAC del IEEE 802.11 para resolver el problema (como las de Karlnet, TurboCell, WORP etc.). Muchas otras soluciones llegaron a estar disponibles pero la interoperabilidad entre los vendedores no estaba garantizada. En el reciente estándar IEEE 802.11e el MAC fue actualizado para incluir "sondeo o interrogación" y hacer las implementaciones interoperables.

6.6.2.5 Estándar optimizado WiMAX[8]

A continuación se mencionará el estándar WiMAX para saber claramente que tecnología se utiliza para abarcar un área más extensa y que ventajas de diseño se obtuvo con este estándar, que es lo contrario a lo que sucede en las redes inalámbricas con el estándar IEEE 802.11.

Con WiMAX que utiliza el estándar IEEE 802.16 fue creada para ser una solución MAN inalámbrica y fue diseñada como una solución para exteriores desde el principio. IEEE 802.16 está diseñado para operar en un tamaño de celda típico de 7 a 10 kilómetros y puede manejar distancias de hasta 50 kilómetros. El problema del "nodo oculto" fue resuelto desde la primera fase de diseño, mediante DAMA-

[8] Estándar optimizado WiMAX: Se menciona este tópico por la necesidad de saber que tecnología usar en caso de tratar de cubrir una área más extensa.

TDMA (Demand assigned Multiple Access - Time Division Multiple Access) para el enlace ascendente (uplink) donde la estación base asigna ranuras de tiempo a cada estación. DAMA-TDMA usa el mismo principio que las redes de satelitales donde las estaciones clientes no pueden "escucharse" entre sí.

Para operar mejor en ambientes donde no hay línea de vista (NLOS), IEEE 802.16 incluye una modulación más compleja basada en OFDM utilizando transformada rápida de Fourier (FFT) de 256-puntos en vez de los 64 puntos empleados en IEEE 802.11 a/g lo que le confiere un mejor rendimiento en ausencia de línea de vista. IEEE 802.16 puede tolerar 10 veces más retardo de multitrayectoria que 802.11. IEEE 802.16 puede hacer un uso mejor de los recursos disponibles en el aire puesto que la estación base adjudica ranuras de tiempo a los suscriptores usando algoritmo de programación dinámica. El número de suscriptores no afecta al número de colisiones ni la retransmisión de paquetes.

Como se mencionaba antes, el "nodo oculto" afecta la cobertura del IEEE 802.11 que trabaja mejor en ambientes internos o en soluciones punto a punto. Las posibilidades en IEEE 802.16 para dedicar un cierto ancho de banda a un suscriptor en términos de TDMA, sin preocuparse sobre "nodos ocultos", permite la introducción de antenas inteligentes. Una antena inteligente combina múltiples elementos con capacidad de procesamiento de señal y puede optimizar el diagrama de radiación de la antena automáticamente. El IEEE 802.16 permite técnicas avanzadas de antenas y esto hace posible un mejor planeamiento de las celdas.

IEEE 802.16 ha incluido también soporte para redes mesh[9]. En redes mesh cada estación de suscriptor es también parte de la infraestructura de enrutamiento. IEEE 802.16 hace una modulación más inteligente y "adaptativa" que el IEEE 802.11 y permite la optimización de las tasas de datos para cada suscriptor, permitiendo a la estación base modificar los esquemas de modulación enlace por enlace. Una estación suscriptora cercana a la estación base puede usar una modulación de alta tasa de datos como 64 QAM, mientras que una señal débil proveniente de una estación suscriptora más alejada tal vez pueda usar 16 QAM o

[9] Mesh: Es una red inalámbrica en malla.

QPSK. La modulación adaptativa incluida en el MAC de IEEE 802.16 también permite tener diferentes métodos de modulación para los enlaces descendentes y ascendentes.

6.6.3 Software libre

El software libre está basado en la libertad que tienen los usuarios de ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software. Precisamente, significa que los usuarios de los programas tienen las cuatro libertades esenciales.

- La libertad de ejecutar el programa, para cualquier propósito (libertad 0).
- La libertad de estudiar cómo trabaja el programa, y cambiarlo para que haga lo que usted quiera (libertad 1). El acceso al código fuente es una condición necesaria para ello.
- La libertad de redistribuir copias para que pueda ayudar al prójimo (libertad 2).
- La libertad de distribuir copias de sus versiones modificadas a terceros (la libertad 3). Si lo hace, puede dar a toda la comunidad una oportunidad de beneficiarse de sus cambios. El acceso al código fuente es una condición necesaria para ello.

Un programa es software libre si los usuarios tienen todas esas libertades. Entonces, debería ser libre de redistribuir copias, tanto con o sin modificaciones, ya sea gratis o cobrando una tarifa por distribución, a cualquiera en cualquier parte. El ser libre de hacer estas cosas significa, entre otras cosas, que no tiene que pedir o pagar el permiso.

También debería tener la libertad de hacer modificaciones y usarlas en privado, en su propio trabajo u obra, sin siquiera mencionar que existen. Si publica sus cambios, no debería estar obligado a notificarlo a alguien en particular, o de alguna forma en particular.

6.6.3.1 GNU/Linux

GNU/Linux es uno de los términos empleados para referirse a la combinación del núcleo o kernel libre similar a Unix denominado Linux, que es usado con

herramientas de sistema GNU. Su desarrollo es uno de los ejemplos más prominentes de software libre; todo su código fuente puede ser utilizado, modificado y redistribuido libremente por cualquiera bajo los términos de la GPL (Licencia Pública General de GNU, en inglés: General Public License) y otra serie de licencias libres.

6.6.3.2 Distribuciones GNU/Linux

A las variantes entre las uniones de programas y tecnologías, a las que se les adicionan diversos programas de aplicación de propósitos específicos o generales se las denomina distribuciones se puede observar su arquitectura en la figura 6.3. Su objetivo consiste en ofrecer ediciones que cumplan con las necesidades de un determinado grupo de usuarios. Algunas de ellas son especialmente conocidas por su uso en servidores y supercomputadoras donde tiene la cuota más importante del mercado.

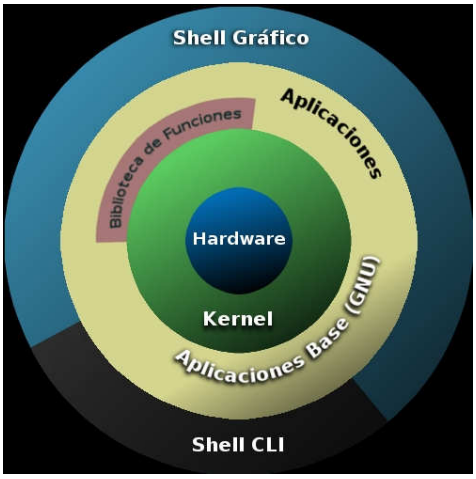


Figura 6.3 Arquitectura de distribuciones GNU/Linux.
Fuente: http://es.wikipedia.org/wiki/Distribuci%C3%B3n_Linux

Según un informe de IDC (International Data Corporation), GNU/Linux es utilizado por el 78% de los principales 500 servidores del mundo, otro informe le da una cuota de mercado de 89% en los 500 mayores supercomputadores. Con menor cuota de mercado el sistema GNU/Linux también es usado en el segmento de las computadoras de escritorio, portátiles, computadoras de bolsillo, teléfonos móviles, sistemas embebidos, videoconsolas y otros dispositivos.

Entre las diez distribuciones más populares que se según el sitio web http://distrowatch.com/ se obtuvieron para septiembre de 2011 son:

1. Ubuntu
2. Mint
3. Fedora
4. Arch
5. openSUSE
6. Debian
7. CentOS
8. Bodhi
9. ArchBang
10. PCLinuxOS

6.6.4 Determinación de las herramientas a implementar

Introducción

Las herramientas disponibles en el campo de las telecomunicaciones, y específicamente en el área de las redes basadas en la conmutación de paquetes, para el monitoreo de redes son variadas dependiendo de las necesidades inmersas que tenga la red y la empresa. Las herramientas basadas en soporte de software libre son una muy buena alternativa para satisfacer los requerimientos de las empresas o instituciones en la actualidad.

6.6.4.1 Distribución ubuntu

Ubuntu es una distribución GNU/Linux que ofrece un sistema operativo para ordenadores de escritorio y con soporte para servidores.

Basada en Debian GNU/Linux, Ubuntu concentra su objetivo en la facilidad de uso, la libertad de uso, los lanzamientos regulares (cada 6 meses) y la facilidad en la instalación. Ubuntu está patrocinado por Canonical Ltd., una empresa privada fundada y financiada por el empresario sudafricano Mark Shuttleworth.

El nombre de la distribución proviene del concepto zulú y xhosa de Ubuntu, que significa "*humanidad hacia otros*" o "*yo soy porque nosotros somos*".

Al ser baasado en Debian (una de las distribuciones más respetadas, tecnológicamente avanzadas y mejor soportadas), Ubuntu pretende crear una distribución que proporcione un sistema GNU/Linux actualizado y coherente para la informática de escritorio y servidores. Incluye una cuidadosa selección de los

paquetes de Debian, y mantiene su poderoso sistema de gestión de paquetes que nos permite instalar y desinstalar programas de una forma fácil y limpia.

Ubuntu proporciona un entorno robusto y funcional, adecuado para uso doméstico como profesional. Ubuntu trabaja en las arquitecturas i386 (procesadores 386/486/Pentium(II/III/IV) y Athlon/Duron/Sempron processors), AMD64 (Athlon64, Opteron y los nuevos procesadores Intel de 64 bits), PowerPC (iBook/Powerbook, G4 y G5) y ARM.

LTS (Long-Term Support)

Cada versión de Ubuntu está soportada al menos durante 18 meses con actualizaciones genéricas y de seguridad. Ubuntu LTS es una versión especial preparada para un uso empresarial, y está soportada durante 3 años para versiones de escritorio y durante 5 años para servidores. El proceso de desarrollo de Ubuntu LTS está concentrado en una serie de áreas como:

- Garantía de calidad
- Localización
- Certificación

Como resultado, de la posibilidad de configurar una distribución Ubuntu durante un periodo de tiempo mayor de lo normal se la identifica como (LTS) o (Long-Term Support) (Soporte a Largo Plazo).

La última versión LTS de Ubuntu es la 10.04 "Lucid Lynx" lanzada el 29 de abril de 2010.

Requerimientos del sistema

Cualquier equipo capaz de ejecutar una variante de Unix , sin necesidad de instalar un entorno gráfico:

Tabla 6.1 Requerimientos de Hardware para Ubuntu 10.04 LTS.

Mínimos	Recomendado
Torre PC estándar	Torre servidor o Rack
Intel Celeron/AMD Sempron 2.0GHz	Intel Core2Quad/AMD Phenom 2.0GHz
512 MB RAM	1 GB RAM
5 GB de espacio en disco duro	10 GB de espacio en disco duro
NIC 10/100 BASE-T	NIC 10/100 BASE-T

Realizado: Carlos Ailaca

6.6.4.2 Herramientas para el control y monitoreo de red

Hay muchas variedades de herramientas que ofrece la Free Software Foundation FSF (Fundación para el desarrollo de Software Libre), de las cuales se han escogido un grupo de ellas para el análisis y entendimiento de sus funcionamiento logrando así acoger soluciones idóneas, para cumplir el objetivo principal de este proyecto. Hay que tomar en cuenta los reconocimientos y las recomendaciones publicadas por las diferentes entidades y grupos, alrededor del mundo, desarrolladores y usuarios, afiliados a la FSF, estas herramientas son:

Iproute2

Iproute2 es un paquete de utilidades desarrollado por Alexey Kuznetsov y disponible bajo el nombre de Iproute. Este paquete es un conjunto de herramientas muy potentes para administrar interfaces de red y conexiones en sistemas Linux. la cual tiene muchas ventajas sobre instrucciones como route, ping, trace.

Este paquete reemplaza completamente las funcionalidades presentes en ifconfig, route, y arp y las extiende llegando a tener características similares a las provistas por dispositivos exclusivamente dedicados al ruteo y control de tráfico.

Este paquete se encuentra incluido en distribuciones de Debian y RedHat con versiones del núcleo mayores a 2.2.

Contenido de IPRoute2

Programas instalados: arpd, ctstat (enlace a lnstat), genl, ifcfg, ifstat, ip, lnstat, nstat, routef, routel, rtacct, rtmon, rtpr, rtstat (enlace a lnstat), ss y tc

❖ **Descripciones cortas**

arpd	Demonio ARP a nivel de usuario, útil en redes realmente grandes en las que la implementación ARP del núcleo es insufuciente, o cuando se configura un "honeypot".
ctstat	Utilidad para el estado de la conexión.
ifcfg	Un guión del intérprete de comandos que actúa como envoltorio para el comando **ip**.
ifstat	Muestra las estadísticas de las interfaces, incluida la cantidad de paquetes enviados y recibidos por la interfaz.
ip	El ejecutable principal. Tiene diferentes funciones: **ip link <*dispositivo*>** permite a los usuarios ver el estado del dispositivo y hacer cambios. **ip addr** permite a los usuarios ver las direcciones y sus propiedades, añadir nuevas direcciones y borrar las antiguas. **ip neighbor** permite a los usuarios ver los enlaces de vecindad, añadir nuevas entradas de vecindad y borrar las antiguas. **ip rule** permite a los usuarios ver las políticas de enrutado y cambiarlas. **ip route** permite a los usuarios ver las tablas de enrutado y cambiar las reglas de las tablas. **ip tunnel** permite a los usuarios ver los túneles IP y sus propiedades, y cambiarlos. **ip maddr** permite a los usuarios ver las direcciones multienlace y sus propiedades, y cambiarlas. **ip mroute** permite a los usuarios establecer, cambiar o borrar el enrutado multienlace. **ip monitor** permite a los usuarios monitorizar continuamente el estado de los dispositivos, direcciones y rutas.
lnstat	Proporciona estadísticas de redes Linux. Es un sustituto generalista y con características más completas para el antiguo programa **rtstat**.
nstat	Muestra las estadísticas de la red.
routef	Un componente de **ip route**. Este es para refrescar las tablas de enrutado.
routel	Un componente de **ip route**. Este es para listar las tablas de enrutado.

rtacct Muestra el contenido de /proc/net/rt_acct.

rtmon Utilidad para la monitorización de rutas.

rtpr Convierte la salida de **ip -o** a un formato legible

rtstat Utilidad para el estado de rutas.

ss Similar al comando **netstat**. Muestra las conexiones activas.

tc Ejecutable para el control del tráfico. Este es para las implementaciones Quality Of Service (QOS, Calidad de Servicio) y Class Of Service (COS, Clase de Servicio).
tc qdisc permite a los usuarios establecer la disciplina de colas.
tc class permite a los usuarios establecer clases basadas en la planificación de las disciplinas de colas.
tc estimator permite a los usuarios hacer una estimacón del flujo de red en una red.
tc filter permite a los usuarios establecer el filtrado de paquetes QOS/COS.
tc policy permite a los usuarios establecer las políticas QOS/COS.

Usos del Iproute

Esto es lo que nos permite hacer este código.

- Unificar los comandos relacionados con la gestión del tráfico IP, sea de redes, de interfaces, etc.
- Uso de tablas de routing múltiples.
- Creación de túneles IP
- Reserva de ancho de banda
- Gestión de direcciones multicast
- Gestión de tablas ARP
- Monitorización de los periféricos, direcciones y rutas.

freeRADIUS

Figura 6.4 Logo del proyecto freeRADIUS.
Fuente: http://freeradius.org/

FreeRADIUS es uno de los servidores RADIUS más modular y rica en características disponible hoy en día; que lo convierte en uno de los más utilizados y potentes servidores RADIUS de clase AAA, es el proyecto iniciado en 1999 por Alan DeKok y Miquel van Smoorenburg (quien colaboró anteriormente en el desarrollo de Cistron RADIUS). Ha sido escrito por un equipo de desarrolladores que tienen décadas de experiencia colectiva en la implementación y despliegue de software de RADIUS, en ingeniería de software, y en la gestión de paquetes Unix. El producto es el resultado de la sinergia entre muchos de los nombres más conocidos en implementaciones libres de RADIUS basados en software, incluyendo varios de los desarrolladores de Debian GNU / Linux, y se distribuye bajo la GNU GPL (versión 2).

El servidor FreeRADIUS se está utilizando en todo el mundo en instalaciones a gran escala que abarca múltiples servidores de radio con millones de usuarios y sesiones.

Actualmente incluye soporte para LDAP, SQL y otras bases de datos, así como EAP, EAP-TTLS y PEAP, incluyendo soporte para todos los protocolos comunes de autenticación y bases de datos.

Acerca de RADIUS

RADIUS (Remote Authentication Dial-In User Service) es un protocolo de autenticación, autorización y manejo de cuentas de usuario originalmente desarrollado por Livingston Enterprises y publicado en 1997 como los RFC 2058 y 2059. Es utilizado para administrar el acceso remoto y la movilidad IP, como ocurre en servicios de acceso por modem, DSL, servicios inalámbricos 802.11 o servicios de VoIP (Voice over IP o Voz sobre IP). Este protocolo trabaja a través del puerto 1812 por UDP.

La autenticación gestionada por este protocolo se realiza a través del ingreso de un nombre de usuario y una clave de acceso. Esta información es procesada por un dispositivo NAS (Network Access Server) a través de PPP (Point-to-Point Protocol o Protocolo Punto-a-Punto) siendo posteriormente validada por un servidor RADIUS a través del protocolo correspondiente valiéndose de diversos esquemas de autenticación, como PAP (Password Authentication Protocol o Protocolo de Autenticación de Clave de acceso), CHAP (Challenge-Handshake Authentication Protocol) o EAP (Extensible Authentication Protocol), y permitiendo el acceso al sistema.

Características

Algunas de las características con las que cuenta freeRADIUS se enumeraran a continuación:

- Provee 50 archivos de diccionario.
- Viene con soporte para LDAP, MySQL, PostgreSQL, bases de datos Oracle.
- Es compatible con EAP, con EAP-MD5, EAP-SIM, EAP-TLS, EAP-TTLS, EAP-PEAP, y Cisco LEAP sub-tipos.
- Es compatible con proxy, con conmutación por error y equilibrio de carga.
- Se ha llegado a una versión 1.0 estable, con mejoras incrementales que se añade y probados todos los días.
- está bien adaptado para su implementación en redes de cualquier tamaño.
- es compatible con los últimos protocolos de red.

Nagios

Figura 6.5 Logo del proyecto Nagios de Nagios Enterprise.
Fuente: http://www.nagios.org/

Nagios se constituye como una herramienta para el monitoreo de sistemas y redes de computadoras. Nagios fue diseñado como una plataforma extremadamente sólida para el monitoreo, organización y alerta de las diferentes redes y sistemas antes mencionados.

Nagios integra sobre esta pasarela, una variedad de poderosas herramientas, el aprovechamiento al máximo de estas herramientas y sistemas no solo involucra el entender como Nagios funciona, sino el comprender y analizar de manera detenida, cual es el trabajo que desempeña el sistema que se va a monitorear, esta relación es extremadamente importante, ya que Nagios como herramienta no es una fuente de conocimiento sobre la complejidad del sistema a monitorear, sino que, se constituye en una herramienta casi indispensable, para entender dicha complejidad.

Características

Algunas de las características con las que cuenta Nagios se enumeraran a continuación:

- Monitoreo de recursos de sistema en servidores de red.
- Carga del procesador.
- Consumo de recursos de disco.
- Uso de memoria de procesos RAM.
- Estado de servicios críticos (EXPLORER.EXE, SMTP, POP3, HTTP, SSH, DNS, SAMBA, etc.).
- Monitoreo bases de datos MySQL, Postgres, Oracle, SQL Server etc.
- Monitoreo de equipos de red activos, hosts, (Switch, Router, Hubs, CPE, NetWare, etc.).
- Monitoreo de Equipos compatibles con IP (Impresoras IP, Cámaras CCTV, Sensores de proximidad, temperatura, iluminación IP).
- Notificación y Alerta personalizadas, del estado de hosts, sistemas y servicios en caso de presentarse inconvenientes en los mismos, a través de diferentes sistemas de comunicación (E-mail, Pagers, SMS a teléfonos móviles, Alertas Sonoras, Gráficas o definidas por el usuario).
- Diseño de Plugins totalmente personalizables para adaptar el sistema acorde a nuestras necesidades.
- Habilidad para definir jerarquías y relaciones entre los diferentes hosts, sistemas y servicios de red.

- Detallado informe gráfico y textual, diario, semanal, mensual, etc., del comportamiento de los sistemas a monitorizarse.
- Integración y compatibilidad con otras herramientas de monitoreo para trabajar al servicio de Nagios.
- Publicación de mapas de red, alertas gráficas y configuración a través de su servidor WEB apache2 incluido, con validación de contraseñas y usuarios.

NAGIOS se vale de una amplia gama de herramientas para cumplir con las especificaciones de monitoreo del usuario, la información recopilada por tal o cual herramienta, entregada a NAGIOS, es procesada e interpretada por este, con el fin de tomar decisiones, ejecutando scripts, desarrollados por el usuario, para corregir determinado inconveniente en la red.

NAGIOS no está diseñado para realizar tareas específicas como muchos otros sistemas, a diferencia de estos, NAGIOS no se constituye como una simple herramienta, sino como un elaborado sistema de administración de red, todas los sistemas de monitoreo que se implementen sobre la red, pueden ser administrados por NAGIOS, toda la información que estos generen será almacenada por NAGIOS, para su posterior análisis y notificación al administrador de la red.

6.7 Metodología. Modelo operativo

6.7.1 Implementación del servidor en la red

En la figura 6.6 se puede observar la ubicación del servidor en la red, en cuanto a su topología.

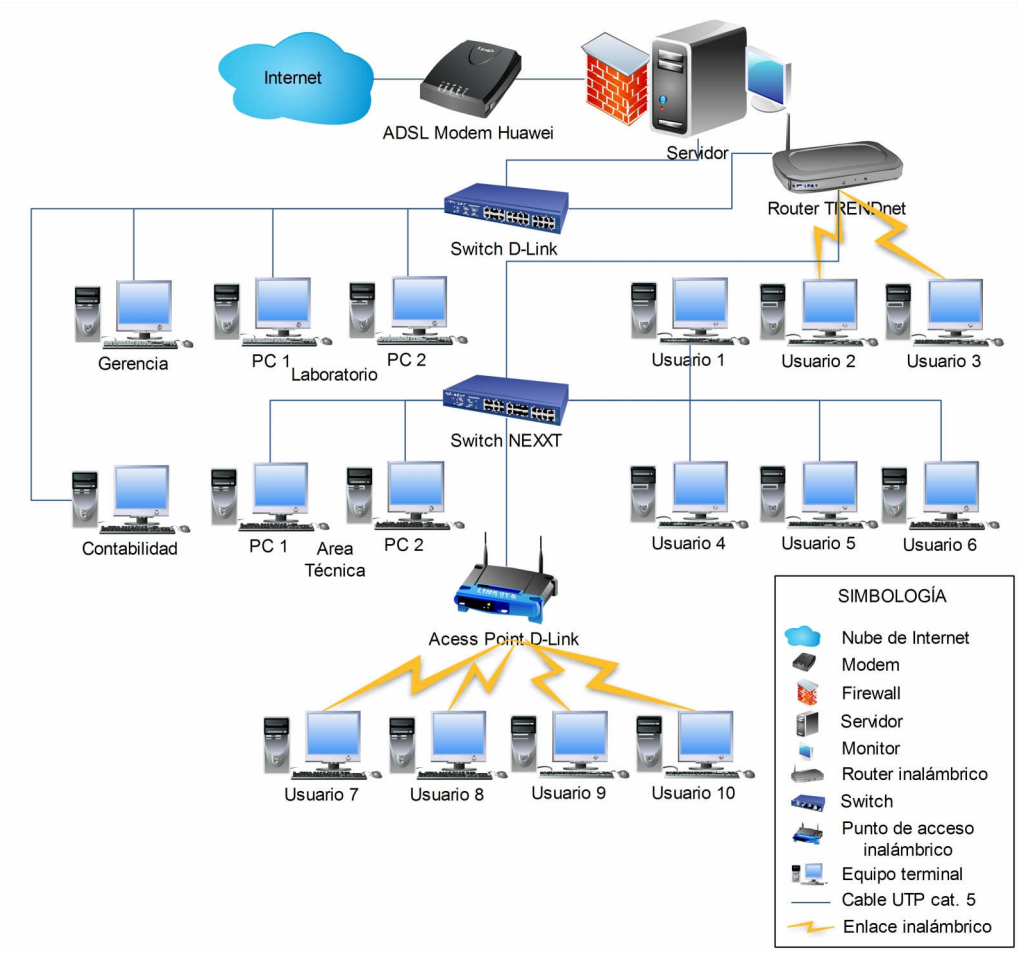


Figura 6.6 Ubicación del servidor en la red.
Realizado: Carlos Ailaca

6.7.1.1 Dispositivos del servidor

Para el ensamblaje del servidor se utilizó; primordialmente los siguientes dispositivos:

- Un mainboard Biostar G41-M7.
- Procesador Intel Dual Core de 3GHz.
- Memoria RAM Patriot de 2GB DDR3.
- Disco Duro Wester Digital de 500GB.
- Tarjeta Ethernet D-Link 10/100/1000.
- Lector de DVD LG.

6.7.1.2 Instalación del sistema operativo Ubuntu Server

Con el disco de instalación de Ubuntu Server 10.04 LTS, se realizó los siguientes pasos para la instalación que se detalla a continuación:

1. Se cambió la secuencia de arranque del servidor para poder acceder al disco de instalación de Ubuntu Server.
2. Una vez realizado esto, el servidor arrancó desde el disco desplegando la primera pantalla de selección del idioma se escogió español y posteriormente la pantalla de instalación como se muestra en la figura 6.7.

Figura 6.7 Pantalla de instalación de Ubuntu Server 10.04 LTS.
Realizado: Carlos Ailaca

3. Se seleccionó el país entre las opciones desplegadas, se marcó Ecuador.
4. Seleccionó el idioma del teclado; en un comunicado que da la opción de detectar automáticamente o hacerlo manual se lo hizo manual así que se respondió No a la pregunta.
5. Se desplegó un conjunto de opciones a escoger se escogió España y de ahí se desplego otras opciones en la que se escogió España – Macintosh considerada la más completa como se ve en la figura 6.8.

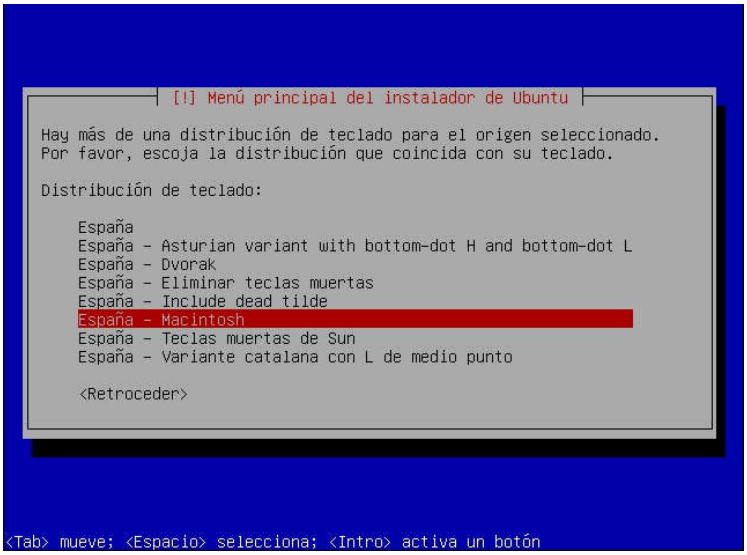


Figura 6.8 Selección de idioma del teclado.
Realizado: Carlos Ailaca

6. Una vez seleccionado el idioma del teclado se empiezó a cargar los componentes del sistema y al finalizar aparece la pantalla se muestra la figura 6.9 donde se debe de ingresar el nombre de la máquina.

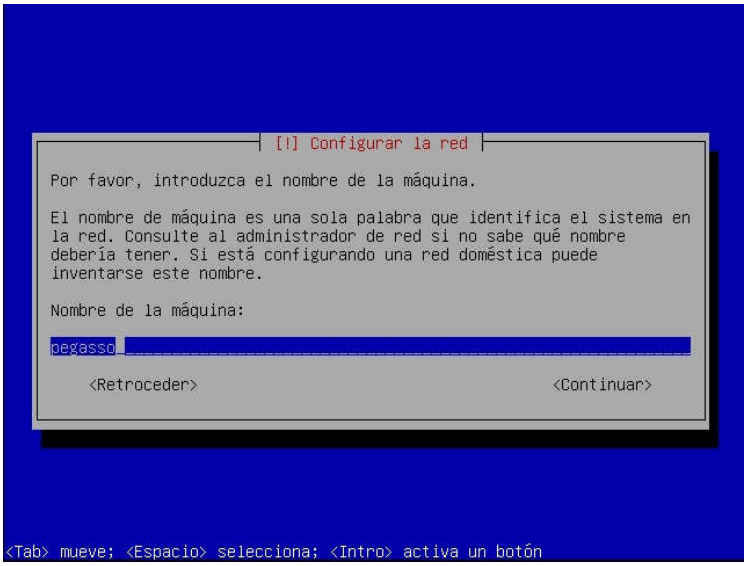


Figura 6.9 Nombre de la máquina en la red.
Realizado: Carlos Ailaca

7. Se configura el reloj y se presenta un comunicado de la ubicación, donde se observa que basada a la configuración anterior está en la zona América/Guayaquil a lo que se responde Sí y se configura el reloj y la red.
8. En la pantalla de particionado de disco se seleccionó particionado de disco manual asignando para el /boot 100MB y con el proceso de particionado LVM (Logical Volume Manager); para disco para raíz "/" 4GB, para "swap" 4GB y para "var" 2GB de disco duro como se ve en la figura 6.10.

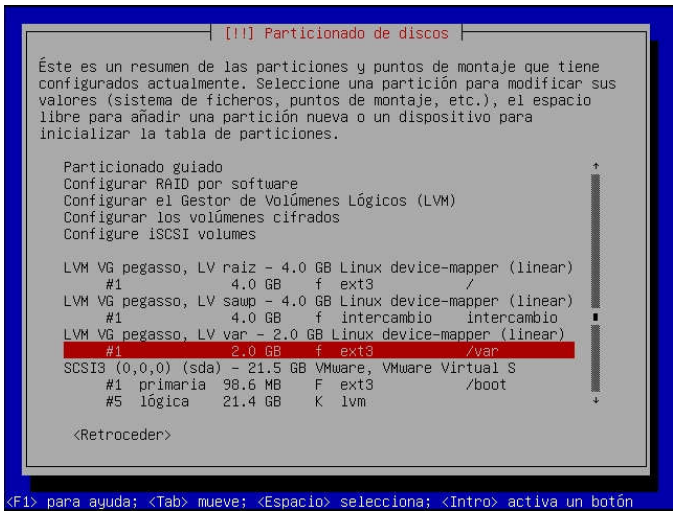


Figura 6.10 Particionado de disco duro.
Realizado: Carlos Ailaca

El LVM (Administración Lógica de Volúmenes, o Logical Volume Management), en inglés, existe como un conjunto de herramientas que le permite manejar el almacenamiento en disco de una manera muy flexible. Entre otras cosas, permite un control poderoso sobre las particiones (por ejemplo, cambiar tamaño sin reiniciar) y hace que operaciones como cambios en dispositivos sean relativamente sencillas. LVM actúa como una alternativa a la manera estándar de administrar las particiones en disco.

Entre las particiones fundamentales del sistema, tenemos:

- Partición de Intercambio o SWAP, esta representa la memoria virtual del sistema, a menudo se suele dimensionar está en el doble de la memoria RAM disponible en el sistema.
- Partición principal, esta alojara al fichero raíz o root representado por el símbolo / , puede tener la extensión que uno desee, cabe recalcar que

el sistema de ficheros que maneja Linux es del tipo ext3, un sistema de locación de espacio en disco diferente al manejado por Windows, sea NTFS o FAT32, este sistema de ficheros aloja los por clusters la información de manera ordenada y no randómica, haciendo más lento el almacenamiento, pero mucho más rápido el acceso sin opción a fragmentación de la información.

9. Una vez realizado la partición se aceptó los cambios en el disco y el programa empieza instalando el sistema base, luego aparece la ventana de configuración de usuarios y contraseñas como se muestra en la figura 6.11 .

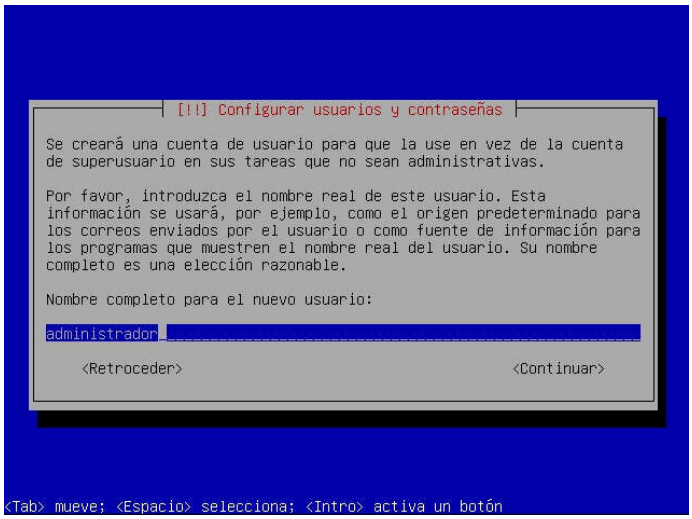


Figura 6.11 Configuración usuarios y contraseñas.
Realizado: Carlos Ailaca

10. Escribimos la contraseña del usuario y confirmamos, en la ventana donde pide un proxy se seleccionó No, debido a que no se lo tiene y continuamos, empiezó a cargar más archivos de sistema operativo.
11. Se muestra una ventana donde se presenta las opciones de las actualizaciones de seguridad, se seleccionó que se actualice automáticamente.
12. Después se muestra una ventana donde hay programas que se pueden instalar se eligió OpenSSH server y se continuo.
13. Al terminar de instalarse los paquetes, el sistema presenta una ventana de configuración de grub-pc es el gestor de arranque del sistema, como es el único sistema que está presente se seleccionó Si para que se instale en el registro principal.

14. Al terminar la instalación nos pide extraer el disco de instalación y el sistema se reinicia; al reiniciarse esta lista la instalación del sistema operativo Ubuntu server 10.04 LTS, para acceder al sistema ingresamos en login (usuario que se creó) y la contraseña; finalmente está listo el servidor para instalar las demás herramientas como se muestra en la figura 6.12.

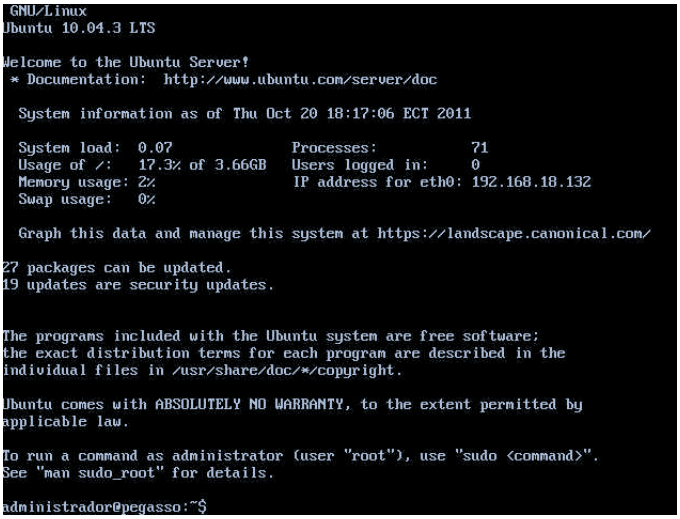


Figura 6.12 Sistema operativo Ubuntu Server ejecutado.
Realizado: Carlos Ailaca

6.7.1.3 Instalación de iproute2

El conjunto de herramientas iproute, también conocido como iproute2, es una colección de utilidades para redes y control de tráfico. Estas herramientas de comunicación está con el kernel de Linux a través de la interfaz (rt) netlink, proporcionando características avanzadas que no están disponibles a través de los comandos de herramientas de red tales como “ifconfig” y “route”.

Para instalar este paquete en Ubuntu, se utilizó el siguiente comando:

$ sudo apt-get install iproute

Para saber sobre el paquete instalado, se puede usar dpkg(descripción del paquete) así:

$ dpkg -s iproute

Como se pudo constatar al momento de aplicar el comando de instalación para iproute este paquete de herramientas ya viene incluido en el kernel del sistema operativo de Ubuntu Server 10.04 LTS.

6.7.1.4 Instalación de freeRADIUS

La herramienta freeRADIUS es compatible con el sistema operativo Ubuntu Server por lo que al momento de ingresar el comando de instalación se instaló sin ninguna novedad.

Para instalar esta herramienta se ingresó el siguiente comando:

$ sudo apt-get install freeradius

Se puedo comprobar que se instaló correctamente aplicando el comando dpkg –s freeradius.

Para poder trabajar con la Interfaz Gráfica que viene en la herramienta freeRADIUS llamada DialUp Admin se tuvo primero que instalar el servidor Apache y el programa PHP para creación de páginas Web, en nuestro caso, las versiones instaladas corresponden a "Apache 2.2.14-5ubuntu8.6" y "PHP 5.3.2-1ubuntu4.10", todos estos programas se encuentran activos en el mismo computador.

Para la instalación de Apache se utilizó el siguiente comando:

$ sudo apt-get install apache2

Para la instalación de PHP, se utilizó lo siguiente:

$ sudo apt-get install php5

Para poder almacenar la información de los usuarios se instaló los servidores de base de datos MySQL; al instalar el mysql-server durante la instalación se requirió una contraseña de root(usuario administrador); para realizar la instalación se requirió los siguientes comandos:

$ sudo apt-get install mysql-server

$ sudo apt-get install mysql-client

6.7.1.5 Instalación de Nagios

Antes de empezar a instalar Nagios en Ubuntu Server es necesario instalar otros paquetes, es posible que ya se tenga instalado algunos de estos paquetes:

- Apache 2
- PHP
- GCC: librerías de desarrollo y compilación
- GD: librerías de desarrollo

Como ya se tiene instalado los anteriores como son Apache y PHP nos faltaría GCC y GD, para ello se realizó lo siguiente:
$ sudo apt-get install build-essential ; para GCC

y para GD:

$ sudo apt-get install libgd2-xpm-dev

Al instalar nagios se visualizó una pantalla en la que pide que clase de configuración se requiere, se seleccionó sin configurar debido a que se lo realizara manualmente en lo posterior y después pide ingresar una contraseña para el administrador de nagios; para lograr su instalación se utilizó lo siguiente:
$ sudo apt-get install nagios3

6.7.2 Configuración de las herramientas en el servidor

6.7.2.1 Configuración para la administración del ancho de banda

Configurando el archivo de interfaces de red el cual se encuentra en la dirección: /etc/network/interfaces.

Para configurar este archivo se utilizó el editor de texto nano ingresando en el terminal el siguiente comando:
$ sudo nano /etc/network/interfaces
Enseguida se mostró una pantalla en la que se ingresó lo siguiente:

```
#interface externa
auto eth0
iface eth0 inet dhcp
```

```
#interface interna
auto eth1
iface eth1 inet static
address 192.168.20.1
netmask 255.255.255.0
```

Una vez realizadas las configuraciones para que los cambios surtan efecto se escribe el comando siguiente:

```
$ sudo  /etc/init.d/networking restart
```

Gateway

Para que el servidor pueda proveer a la red interna de internet este debe rutear correctamente hacia el ISP siendo necesario correr la maquina como una gateway (pasarela) al contar con dos tarjetas de red es posible hacerlo.

Se configurara la interfaz de red eth1 para que sirva directamente a la red interna, esta tarjeta que tendrá una dirección IP clase C: 192.168.20.1, la que utilizaremos como default gateway para las maquinas internas. Dejando eth0 para el direccionamiento externo.

Para que el servidor funcione como un gateway y rutee los paquetes desde nuestra LAN hacia el mundo exterior y de regreso, se necesita que tenga habilitado el bit de IP forwarding, además de las reglas necesarias para que pueda enrutar paquetes. Esto se hace vía iptables.

Básicamente necesitamos tener tres juegos de reglas:

- Denegar las conexiones entrantes en eth0 (la interfaz de red externa)
- Permitir los paquetes salientes desde nuestra LAN, vía eth1
- Permitir que las conexiones establecidas regrese.

El siguiente Script 00-firewall se muestra a continuación:

```
#!/bin/sh
PATH=/usr/sbin:/sbin:/bin:/usr/bin
#
```

```
# borrando todas las reglas existentes.
#
iptables -F
iptables -t nat -F
iptables -t mangle -F
iptables -X

# Siempre acepte el trafico desde loopback
iptables -A INPUT -i lo -j ACCEPT

# Permitir conexiones establecidas, y las que no vengan desde fuera.
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -m state --state NEW -i ! eth0 -j ACCEPT
iptables -A FORWARD -i eth0 -o eth1 -m state --state
ESTABLISHED,RELATED -j ACCEPT

# Permitir conexiones salientes desde adentro de la LAN.
iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT

# Enmascarar.
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

# No forward de afuera hacia adentro.
iptables -A FORWARD -i eth0 -o eth0 -j REJECT

# Habilite ruteo.
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Es necesario que este script se ejecute al arrancar el sistema y tan pronto como las interfaces de red inicien. Para este propósito se guarda en el directorio /etc/network/if-up.d/. Todo lo que se encuentre en ese directorio es ejecutado cuando una interface se inicia, siempre y cuando el archivo sea ejecutable. Debido

a que los contenidos del directorio son ejecutados en orden, el script es nombrado 00-firewall.

Esto nos proveerá con un gateway básico. Ahora cualquier maquina dentro de la LAN es capaz de acceder a Internet.

Otra forma más sencilla de realizar este trabajo en el servidor es instalando el programa Firestarter, este programa se encuentra en los repositorios de Ubuntu, es totalmente intuitivo y fácil de configurar evitándonos este engorroso trabajo dado que el objetivo de este trabajo es diferente se considera esta opción para el gateway.

Control del ancho de banda en el servidor.

Se utilizó las herramientas que vienen incluida en Linux en el paquete iproute2:

- Un controlador de tráfico (tc)
- Un temporizador (htb).

Estas herramientas, al formar parte del propio sistema operativo tiene un elevado nivel de eficiencia y precisión.

La interface externa conectada al proveedor de Internet brinda un ancho de banda de 2Mbps eth0.

La interface interna conectada a la red interna que se configurará para funcionar a 10Mbps máximo eth1

Los usuarios pertenecen a la subnet 192.168.20.0/24. El Script que limitaría el ancho de banda tendría el siguiente contenido:

```
#!/bin/bash
#Se establece la placa de red interna.
DEV=eth1

#Se establece el camino al comando "tc", por si no está en el PATH
TC=tc ; este es el caso en el que esta en el PATH

#Se establecen los limites de ancho de banda a utilizar en Kbps.
```

```
RATE1=2000
RATE2=1000
RATE3=500
RATE4=250
RATE5=60

#Se elimina toda posible definición previa existente
$TC qdisc del dev $DEV root 2>&1 >/dev/null

#Se establecen las CLASES existentes, ademas de la CLASE root y la CLASE master que son necesarias para el funcionamiento del script.

#CLASE root y master
$TC qdisc add dev $DEV root handle 1: htb default 60
$TC class add dev $DEV parent 1: classid 1:1 htb rate ${RATE1}kbit

#CLASES y orden prioridad

#ClASE 1
$TC class add dev $DEV parent 1:1 classid 1:10 htb rate ${RATE}kbit ceil ${RATE}kbit prio 1
$TC qdisc add dev $DEV parent 1:10 handle 10: sfq perturb 10

#ClASE 2
$TC class add dev $DEV parent 1:1 classid 1:20 htb rate ${RATE2}kbit ceil ${RATE2}kbit prio 2
$TC qdisc add dev $DEV parent 1:20 handle 20: sfq perturb 10


#ClASE 3
$TC class add dev $DEV parent 1:1 classid 1:30 htb rate ${RATE3}kbit ceil ${RATE3}kbit prio 3
$TC qdisc add dev $DEV parent 1:30 handle 30: sfq perturb 10

#ClASE 4
$TC class add dev $DEV parent 1:1 classid 1:40 htb rate ${RATE4}kbit ceil ${RATE4}kbit prio 1
$TC qdisc add dev $DEV parent 1:40 handle 40: sfq perturb 10

#ClASE 5
$TC class add dev $DEV parent 1:1 classid 1:50 htb rate ${RATE5}kbit ceil ${RATE5}kbit prio 1
```

$TC qdisc add dev $DEV parent 1:50 handle 50: sfq perturb 10

#Se establecen los FILTROS.

FILTRO3 (USUARIOS a CLASE 3)
$TC filter add dev $DEV parent 1: protocol ip prio 1 u32 match ip dst 172.16.20.0/24 flowid 1:30
$TC filter add dev $DEV parent 1: protocol ip prio 1 u32 match ip src 172.16.20.0/24 flowid 1:30

#Para cambiar el ancho de banda descomentar las ordenes del filtro seleccionado.
#Fin del Script

El script se guardó como un archivo de texto normal, con nombre controlwb.sh y se le dan permisos de ejecución con la orden, sudo chmod a+x controlwb.sh

6.7.2.2 Configuración para enlaces inalámbricos seguros

Para configúralo se realizó lo siguiente:

Configurar FreeRADIUS con MySQL

Primero los bits de MySQL (creación del password bit y su usuario administrador). Se hizo lo siguiente en su Shell[10] :

mysqladmin -u root password 123456
mysql -u root –p

En MySQL shell se tecleó lo siguiente:

CREATE DATABASE radius;
GRANT ALL ON radius.* TO radius@localhost IDENTIFIED BY
"radpass";
exit;

Hay esquemas importantes de freeRADIUS. Los ejemplos de los esquemas se encuentran en este lugar:

/usr/share/doc/freeradius/examples/mysql.sql.gz.

Se descomprimió allí con Gunzip:

[10] Shell: intérprete de comandos

gunzip-d /usr/share/doc/freeradius/examples/mysql.sql.gz

Se realizó lo siguiente:

mysql -u root -p radius < /usr/share/doc/freeradius/examples/mysql.sql

Para mirar los esquemas password bit :

```
mysql -u root -p
use database radius;
show tables;
quit;
```

Ahora se edita: $sudo nano/etc/freeradius/sql.conf.

Se reinicia user/password/database los parámetros para reflejar los cambios (eg. radius/radpass/radius);

Activando el control NAS[11] de MySQL, en la línea

readclients = no y dejarlo readclients = sí

Editar el archivo/etc/freeradius/radius.conf y añadir una línea diciendo 'sql' a autoriaze {} la sección (que esta hacia el final del archivo). También añadir la línea diciendo 'sql' a la accounting {} en esta sección dice a FreeRadius almacenar registros contables en SQL también.

Opcionalmente añadir 'sql' a la session {} en esta sección si usted quiere hacer el uso de la detección simultánea. Opcionalmente añadir 'sql' al post-auth {} esta sección si usted quiere registrar todas las tentativas de autenticación a SQL. Aquí está la sección autorizar:

```
authorize {
        preprocess
        chap
        mschap
        suffix
        eap
        sql
```

[11] NAS: (del inglés Network Attached Storage) es el nombre dado a una tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento de un computador (Servidor) con ordenadores personales o servidores clientes a través de una red

```
        pap
}
```

Y la sección de la contabilidad:

```
accounting {
        detail
        sql
 }
```

Al ingresar el usuario de prueba in la base de datos, se ejecuta el MySQL shell y corre lo siguiente:

```
mysql -u root –p
mysql> use database radius;
mysql> INSERT INTO radcheck (UserName, Attribute, Value) VALUES
('sqltest', 'Password', 'testpwd');
mysql> select * from radcheck where UserName='sqltest';
mysql> exit
```

Se enciende Radius en el modo de depuración con el siguiente comando:

```
freeradius-X
```

Para ir a otro shell y ejecute la prueba:

```
radtest sqltest testpwd localhost 1812 testing123
```

En este momento se logra ver un mensaje Accept, indicando que el usuario está bien autentificado.

Dialup admin

Con el fin de instalar el dialup, el paquete debe ser descargado y descomprimido debido a su formato tar.gz. Y se coloca en un directorio determinado en el sistema (podría ser en cualquier lugar, pero usamos / usr / local / dialup_admin).

```
shell> xfvz de dialup_admin-X.XX.tar.gz
shell> mv dialup_admin / usr / local
```

El dialup admin contiene una serie de directorios necesarios para que el programa funcione. Nos dirigimos al directorio htdocs. Este directorio contiene los scripts php necesarios. A fin de que sea accesible a través de nuestro servidor web se debe establecer un vínculo simbólico entre los dos lugares. Partimos de que la DefaultRoot del servidor Web Apache es / var / www / htdocs

shell> ln-s / usr / local / dialup_admin / htdocs / var / www / htdocs / dialup

Para obtener un funcionamiento adecuado se debe de realizar lo siguiente:

Configuración de Apache

El Apache debe de ser configurado para ejecutar scripts PHP. Con el fin de hacerlo, se busca el archivo httpd.conf. Tenemos que entrar en las siguientes líneas dentro del httpd.conf:

LoadModule php4_module libexec/libphp4.so
AddModule mod_php4.c
AddType application / x-httpd-php. Php
AddType application / x-httpd-php. Php3 # Esto es muy importante ya que muchos de los scripts PHP de dialup admin tienen esta extensión

Desde el dialup admin no viene con ningún tipo de autorización administrativa interna, sería recomendable la seguridad y protegernos a nosotros mismo.

Se agregó lo siguiente a su archivo httpd.conf:

AuthName "Zona Restringida"
AuthType Basic
AuthUserFile / var / www / htpasswd
Require valid-user

Al cambiar; por supuesto, la ruta del directorio que coincide con la suya, así como el argumento AuthUserFile para indicar el lugar donde los nombres de usuario / contraseñas son almacenadas.

Con el fin de crear el archivo htpasswd de la utilidad htpasswd es necesario que se proporcione con el servidor web apache

Se crear nuestro primer usuario:

shell> htpasswd-c / var / www / htpasswd-m contraseña de administrador

Nota: El argumento-c no se debe utilizar a partir de ese momento, ya que crea un nuevo archivo de contraseñas.

En el próximo reinicio de apache el dialup (el directorio sólo es accesible por una verificación de usuario o contraseña que en nuestro caso es el administrador).

La autenticación HTTP que se ha configurado puede ser utilizada por dialup Admin cuando se conecta a las bases de datos SQL.

Cuando se conecta a la url http://localhost/dialup se debe ver la página de Dialup Admin.

Configurando Access Point

Una vez que el punto de acceso está configurado para utilizar el servidor RADIUS tenemos que añadir su dirección IP a la base de datos del servidor RADIUS, como se muestra en la figura 6.13.

Figura 6.13 Configuración Access Point router inalámbrico TRENDnet.
Realizado: Carlos Ailaca

Para añadir el nuevo Access Point, abrimos /etc/freeradius/clients.conf y añadir lo siguiente al final del archivo:

```
client 192.160.50.1 {
 secret = SET_IN_ACCESS_POINT  (prueba)
 shortname = trendnet
}

client 192.160.50.2 {
 secret = prueba1
 shortname = dlink
}
```

Donde SET_IN_ACCESS_POINT es el secreto que había ingresado en la configuración del Ponto de Acceso y 192.168.50.1 es la dirección del punto de acceso

6.7.2.3 Configuración para el monitoreo de la red

Para la configuración se realizó lo siguiente:

Configuración de parámetros en el archivo nagios.cfg

Para poder declarar host, servicios, contactos, etc, es necesario hacer algunos cambios en el archivos nagios.cfg, ademas de modificar otros que estan bajo el directorio de /etc/nagios3/conf.d/.
Vamos primeramente a modificar el archivo "nagios.cfg":

```
# nano /etc/nagios3/nagios.cfg
```

Dentro de este archivo buscaremos las lineas con instrucción "cfg_dir=" las cuales por defecto vienen comentadas, por lo que abajo de ese bloque, se crea una línea más, donde indicaremos el directorio en donde guardaremos nuestros archivos con la información de los host a monitorear. <table style="text-align: left; background-color: rgb(153, 153, 153); width: 100%; height: 100%;" border="0" cellpadding="2" cellspacing="2"> #cfg_dir=/etc/nagios3/servers

```
#cfg_dir=/etc/nagios3/printers
#cfg_dir=/etc/nagios3/switches
#cfg_dir=/etc/nagios3/routers
cfg_dir=/etc/nagios3/objetos/
```

En este archivo además podemos cambiar algunos parámetros adicionales al comportamiento del Nagios, tales como; notificaciones, tiempos, intervalos, etc. En todo caso, si se dejan los valores default es muy seguro que todo funcione muy cercano a los que ustedes buscan.

Configuración de los archivos de nagios

Para configurar los archivos de nagios se debió empezar por:

Crear contactos; en contacts_nagios2.cfg con el siguiente comando:

```
# nano /etc/nagios3/conf.d/contacts_nagios2.cfg
```

A través de este archivo, podremos enlistar los contactos para los cuales nos interesa enviar notificaciones de alarmas y monitoreo. El archivo "contacts_nagios2.cfg" se compone de dos partes:

- En la primera, declaramos los contactos con toda su información específica, tal es el caso de: nombre, alias, correo, periodo de notificación, etc.
- En la segunda parte, declaramos los grupos de contactos, en donde indicamos un nombre, un alias y además declaramos los miembros o contactos que pertenecerán a este grupo.

Tal como se muestra a continuación:

```
# In this simple config file, a single contact will receive all alerts.
define contact{
        contact_name                    root
        alias                           Root
        service_notification_period     24x7
        host_notification_period        24x7
        service_notification_options    w,u,c,r
        host_notification_options       d,r
        service_notification_commands   notify-service-by-email
        host_notification_commands      notify-host-by-email
        email                           root@localhost
                }

# Nuevo usuario, creado para el laboratorio de esta guía.
define contact{
```

```
contact_name                    Darwin
alias                           Darwin Davila
service_notification_period     24x7
host_notification_period        24x7
service_notification_options     w,u,c,r
host_notification_options       d,r
service_notification_commands   notify-service-by-email
host_notification_commands      notify-host-by-email
email                           daviladar@yahoo.com
}
```

Crear los Grupos de Dispositivos; en hostgroups_nagios2.cfg

```
# nano /etc/nagios3/conf.d/hostgroups_nagios2.cfg
```

A través de este archivo, podremos crear los grupos de host que requerimos para poder agrupar todos los dispositivos de la forma en que mejor nos resulte, por ejemplo: Hostgroup para servidores "HTTP", PING, SSH, etc.

Además de algunos grupos que el archivo contiene por defecto, agregaremos un grupo para los equipos de la red usuarios y agregaremos un miembro llamado "usuario1", que será el equipo para el cual monitorearemos el servicio de ping:

```
# Grupo para los equipos de usuarios
define hostgroup {
    hostgroup_name      usuarios
        alias           equipos de usuarios
        members         usuario1
    }
```

Modificar los Servicios; en services_nagios2.cfg

```
# nano /etc/nagios3/conf.d/services_nagios2.cfg
```

En este archivo, es donde podremos crear y modificar los diferentes servicios que queremos monitorear para los dispositivos que nos interese.

Será en este archivo donde declararemos los grupos de host que deseamos monitorear para los diferentes servicios, por ejemplo: Declaramos un servicio de ping para los equipos que pertenecen al grupo de "usuarios" de la siguiente manera:

```
# Servicio de Ping, para equipos de usuarios
define service {
        hostgroup_name                  usuarios
        service_description             PING
        check_command                   check_ping!100.0,20%!500.0,60%
        use                             generic-service
        notification_interval           0 ; set > 0 if you want to be renotified
                }
```

Creando los archivos para monitorear los equipos

Se inició la creación de los siguientes archivos:

Creación del directorio de host. Debemos crear el directorio bajo la ruta y el nombre que declaramos en el archivo de nagios.cfg. El cual quedó declarado como "objetos".

Para crearlo, lo hacemos de la siguiente manera:

```
# mkdir /etc/nagios3/objetos
```

Seguidamente se crear el primer archivo de configuración de dispositivos.

Dentro del directorio "/etc/nagios3/objetos", podremos crear y ordenar los archivos de host, sin un orden especifico, debido a que el servidor Nagios leerá cualquier archivo que esté dentro de esta ruta.

Pero para llevar de una forma ordenada todos los dispositivos, los podemos agrupar por clientes, tipos, modelos, importancia, etc.

En este caso, se creó un directorio llamado usuarios, para poner allí, todos los archivos de configuración de los diferentes equipos de los usuarios.

Entonces, creamos el directorio "usuarios" y dentro de este el archivo para monitorear los el router inalámbrico:

```
# mkdir /etc/nagios3/objetos/usuarios
```

El archivo lo creamos de una vez, con el editor de texto, en nuestro caso estamos utilizando "nano"; de la siguiente manera:

```
# nano /etc/nagios3/objetos/usuarios/equipos.cfg
```

Dentro de este archivo, escribiremos todos los parámetros necesarios, y tomando en cuenta algunos que ya hemos declarado en los archivos anteriormente editados:

```
# Este host es para el route de usuarios
define host{
host_name trendnet
alias route de usuarios
address 192.168.50.1
check_command check-host-alive
check_interval 5
retry_interval 1
max_check_attempts 5
check_period 24x7
process_perf_data 0
retain_nonstatus_information 0
contact_groups soportelevel2
notification_interval 30
notification_period 24x7
notification_options d,u,r
hostgroups usuarios
parents gateway
action_url https://192.168.50.1
}
```

Ahora se reinicia el servicio con el siguiente comando:

```
# /etc/init.d/nagios3 restart
```

6.8 Administración

La administración de este compendio de herramientas se la realiza por medio de un buscador web dentro de la red interna. El manejo de la seguridad de la red inalámbrica está sustentado por el servidor RADIUS y su manera de administrar es por medio de la interface de DialUp Admin como se muestra en la figura 6.14 y

la autorización del uso de la red inalámbrica la tiene que dar el administrador de la red al agregarle en el servidor por medio de esta interfaz como usuario autorizado.

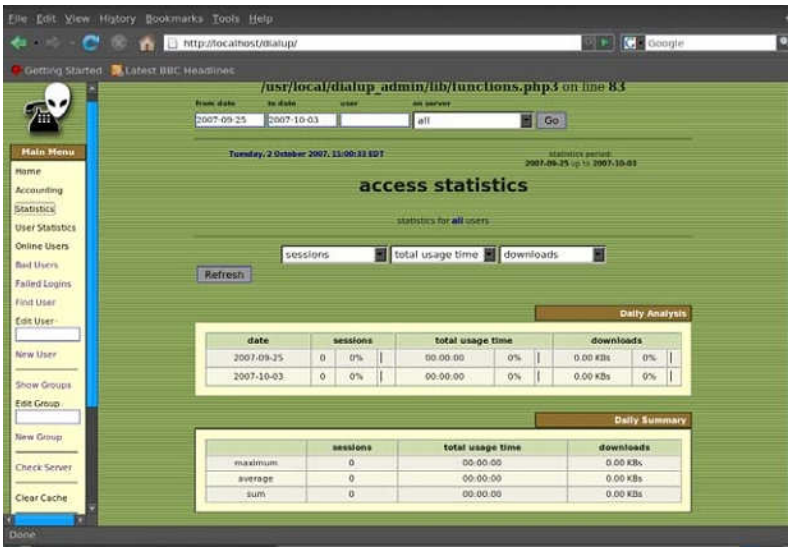


Figura 6.14 Interface DialUp Admin.
Realizado: Carlos Ailaca

De igual forma para observar que la red y equipos se encuentren funcionando correctamente se lo realiza por medio del programa Nagios y su visualización para el monitoreo de la red es por medio de un buscado web como se observa en la figura 6.15, y como se mencionaba en la parte de configuración, si se desea monitorear otro equipo se debe ingresar los datos del equipo en forma manual ya que este sistema no permite la configuración por medio del buscador y para hacerlo se debe ir a sus archivos internos dentro del sistema operativo Ubuntu en la dirección /etc/nagios3.

Figura 6.15 Interface Nagios.
Realizado: Carlos Ailaca

6.9 Presupuesto adicional

Debido a las condiciones y exigencias de operación del servidor, ya que estará en funcionamiento las 24 horas ininterrumpidas se sugiere considerar un presupuesto adicional en el que se incluye lo siguiente:

Tabla 6.2 Presupuesto adicional

1	Servidor HP ProLiant ML110 G7	$1000
2	APC Smart-UPS 2200VA USB & Serial 120V	$1020
TOTAL		$2020

Realizado: Carlos Ailaca

Con estos dispositivos adicionales se asegurara la estabilidad del servicio entregado hacia sus usuarios (clientes).

6.10 Conclusiones y recomendaciones

6.10.1 Conclusiones

- La gran capacidad de configuración que tiene el sistema operativo Ubuntu Server y sus óptimos respaldos y actualizaciones ha logrado que se situé en los primeros puestos; la robustez del sistema en cuanto a su kernel o núcleo y su estabilidad al no presentar bugs (errores en el software) es considerada por muchas empresas en la actualidad para desarrollar sus proyectos.

- Para el control de red en la optimización del ancho banda se consideró alternativas de fácil configuración pero según los usuarios y expertos avanzados, la aplicación de reglas claras como que se va a controlar y herramientas avanzadas como iproute e iptables lograría equiparar a dispositivos dedicados.

- La versatilidad que el servidor RADIUS posee, la hace una herramienta indispensable en redes y mucho más si son redes inalámbricas, la necesidad de autentificarse en la red es uno de sus pilares por la que se consideró su implementación, de este modo el nivel de seguridad se incrementa.

- La herramienta Nagios implementada para el monitoreo de red está enfocada a la obtención de estadísticas del funcionamiento de la red, por el momento para la empresa Intercompu esta herramienta no tiene la importancia debida, ya que no es una red extensa; pero se la implemento con perspectivas a futuro.

- Para asegurar la continua distribución del servicio de internet la utilización de equipos adecuados que soporten grandes exigencias es de considerarlo, aunque la prioridad para esta investigación fue optimizar los recursos existentes, la empresa Intercompu debe de adquirirlos si desea brindar un servicio de calidad.

6.10.2 Recomendaciones

- El óptimo funcionamiento del sistema operativo Ubuntu Server dependerá en mucho de los casos del soporte que tenga el kernel para los dispositivos incorporados en el hardware; considerando lo anterior es necesario verificar si

los dispositivos instalados son compatibles con el sistema caso contrario la realización de drives es una tarea engorrosa.

- La correcta configuración de aplicaciones específicas dependerá de la cantidad de conocimiento del administrador de red; con el continuo avance de la tecnología en redes es importante estudiar los temas referentes a las nuevas herramientas que están disponibles para el administrador de red entre las que se tiene al iproute del paquete iproute2 e iptables una herramienta de Netfilter.
- Los temas de seguridad en redes de tipo inalámbrica en la actualidad son muy requeridos por los administradores de redes, la correcta configuración de los equipos, el control de acceso de los usuarios; requiere que los administradores tengan alguna experiencia en esos ámbitos.
- Se debería tener en cuenta las necesidades de la red, la planificación para un crecimiento es por lo que debería ser necesario que la empresa comience a utilizar la herramienta Nagios para tener un monitoreo de la red y de esta manera se tomaría decisiones más acertadas.
- Se sugeriría realizar un estudio para la conformación de un ISP en la empresa Intercompu, en el que puede incluirse los dispositivos adicionales que se recomiendan en esta investigación.

REFERENCIAS BIBLIOGRÁFICAS

Libros y Manuales

Hurley C. (2007). *Penetration Tester's Open Source Toolkit*. Burlington: Syngress Publishing, Inc.

Walt D. (2011). *FreeRADIUS Beginner's Guide*. Birmingham: Packt Publishing Ltd.

Cayuqueo S. (2011). *Monitoria y análisis de Redes con Nagios*. Wiki Manuales Nagios.

Members of the Ubuntu Documentation Project. (2010). *Ubuntu Server Guide*. Canonical Ltd.

Direcciones Electrónicas

Anónimo (septiembre 2004). Introducción a las redes. Obtenida en 20 de julio de 2011, de http://fmc.axarnet.es/redes/tema_01_m.htm

Anónimo (octubre 2008). Seguridad en red inalámbricaWi-Fi (802.11 o Wifi). Obtenida el 6 de septiembre de 2011, de http://es.kioskea.net/contents/wifi/wifisecu.php3

Anónimo (n.d.). Capítulo 6. Instalación de los programas del sistema base. Obtenido el 26 de septiembre de 2011, de http://www.escomposlinux.org/lfs-es/lfs-es-6.0/chapter06/iproute2.html

Comunidad Ubuntu.es (mayo 2008). Documentación Técnica. Obtenida el 19 de septiembre de 2011, de http://doc.ubuntu-es.org/Documentaci%C3%B3n

CORed (2002). Documentación de control de redes índice. Obtenida el 20 de septiembre de 2011, de http://www.cored.df.gob.mx/cgi-bin/templatecored.pl?.State=documentacion&seleccion=/documentacion/c_redes_avz/index.html#iproute

Escudero A. (n.d.). Unidad 2: Estándares en Tecnologías Inalámbricas. Obtenida el 27 de agosto de 2011, de http://www.eslared.org.ve/tricalcar/02_es_estandares-

inalambricos_guia_v02%5B1%5D.pdf

García I. Montalvo M. Zavala X. Leyton E. (n.d.) Gestión de una red LAN inalámbrica utilizando herramienta propietaria SNMP. Obtenida el 1 de septiembre de 2011, de http://www.dspace.espol.edu.ec/bitstream/123456789/1406/1/2675.pdf

Godmol (junio 2007). Qué es y cómo crear una VPN. Obtenida el 7 de septiembre de 2011, de http://www.configurarequipos.com/doc499.html

Gouril (2008). [WiFi] Redes inalámbricas y seguridad. Obtenida el 5 de septiembre de 2011, de http://es.kioskea.net/faq/1160-wifi-redes-inalambricas-y-seguridad

Ilich L. (2007). Diseño de una red local inalámbrica utilizando u sistema de seguridad basado en protocolos WPA y 802.1x para un complejo hotelero. Obtenida el 11 de septiembre de 2011, de http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/219/LIZA_HERNANDEZ_ILICH_DISE%C3%91O_RED_LOCAL_PROTOCOLOS_WPA_802.1X.pdf?sequence=1

Members of the Ubuntu Documentation Project (2008). Ubuntu Server Guide. Obtenida el 19 de septiembre de 2011, de https://help.ubuntu.com/10.04/serverguide/C/index.html

Mendillo V. (octubre 2008). La seguridad en redes inalámbricas de área local (WLAN). Obtenida el 15 de septiembre de 2011, de http://www.cantv.com.ve/Portales/Cantv/Data/Eventos/SemanaSeguridad_2k8/Mendillo_SEMANADELA_SEGURIDAD_Cantv.pdf

Molina F. (n.d.). Seguridad en rede inalámbricas. Obtenida el 14 de septiembre de 2011, de http://www.acis.org.co/memorias/JornadasTelematica/IIJNT/Seguridad_en_Redes_Inalmbricas.ppt

Tapia J. (2009). Implementación de un sistema de medición y monitoreo de tráfico

IP basado en Software Libre, con el fin de realizar una planeación adecuada de las capacidades de la red WAN de la empresa ALIANZANET S.A. Obtenida el 30 de agosto de 2011, de http://repositorio.espe.edu.ec/bitstream/21000/115/1/T-ESPE-024913.pdf

ANEXOS

UNIVERSIDAD TÉCNICA DE AMBATO

Facultad de Ingeniería en Sistemas, Electrónica e Industrial

Encuesta sobre el acceso a los servicios de internet en la empresa Intercompu y su influencia en el desempeño de la red

Por favor responda con la mayor claridad las siguientes preguntas:

1. ¿El acceso de servicio de internet que le suministra la empresa Intercompu es?

Inalámbrico☐ Alámbrico☐ No sé ☐

2. ¿La velocidad de navegación que usted percibe es?

Rápida☐ Normal ☐ Lenta ☐

3. ¿Sabe usted cuál es el ancho de banda que contrato?

Si☐ ¿cuál es?.....; No ☐

4. ¿Qué servicios de internet usa con frecuencia?

Video conferencia ☐ Chat ☐ Web ☐ Descargas ☐

5. ¿Cuántas veces al día accede a internet?

Entre 2 y 10 veces☐ Más de 10 veces ☐

6. ¿Qué otro tipo de servicio requeriría en un futuro?

Hosting☐ Almacenamiento de datos ☐ Otros ☐

TRENDnet

wireless

300MbpsEnrutador inalámbrico N Gigabit

TEW-639GR(V1.0R)

El enrutador Gigabit inalámbrico N de 300Mbps ofrece una velocidad inalámbrica sin igual, cubrimiento y confiabilidad. Disfrute de hasta 14 veces la velocidad y 6 veces la cobertura de una conexión inalámbrica G *.

Los puertos Gigabit para red de área amplia o local transfieren sus datos rápidamente. La certificación Wi-Fi le garantiza un rendimiento de la potencia de señal inalámbrica óptima y compatible.

La antena con la avanzada tecnología múltiple entrada múltiple salida (MIMO) elimina los puntos muertos inalámbricos. El cifrado inalámbrico y un interruptor de activar/desactivar inalámbrico mantiene seguros sus datos. La configuración inalámbrica protegida (WPS) integra a otros adaptadores compatibles con WPS con el toque de un botón. Sin problemas transmita medios HD, descargue archivos, navegue y juegue a la velocidad Gigabit inalámbrica N.

bg Wi Fi n DRAFT CERTIFIED

Powered by an ENERGY STAR® qualified adapter for a better environment

GREENnet

Características

- 4 x 10/100/1000Mbps Auto-MDIX LAN ports
- 1 x 10/100/1000Mbps WAN port (Internet)
- Gigabit LAN ports for high speed network connectivity
- Compatible with most popular cable/DSL Internet service providers using Dynamic/Static IP, PPPoE, PPTP and L2TP
- Alta velocidad inalámbrica de hasta 300Mbps usando una conexión IEEE 802.11n
- 3 external antennas provide high-speed performance and expansive wireless coverage
- Protección Firewall avanzada con sistema de Traducción de direcciones de red (NAT) e Inspección de integridad de paquetes (SPI)
- Acceso restringido con Control de acceso a Internet, programación del tiempo y filtrado MAC
- Servidores virtuales preconfigurados y servicios de ALG (gateway a nivel de aplicación) integrados para aplicaciones especiales de Internet
- Plug and Play universal (UPnP) para la detección automática de dispositivos y para dar soporte en la configuración de aplicaciones de Internet
- Funcionalidad inalámbrica de activación/desactivación con conmutador WLAN para el encendido/apagado (on/off)
- Múltiples sesiones de transferencia para las aplicaciones VPN más populares (IPSec y PPTP)
- Fácil configuración con explorador Web usando las versiones mas recientes de Internet Explorer, FireFox, Safari y Chrome
- Configuración de seguridad inalámbrica de un toque usando el botón de la configuración protegida Wi-Fi (WPS) cuando se conecte a un dispositivo compatible con WPS
- Soporta (WMM) Wi-Fi Multimedia y (QoS) Quality of Service
- Seguridad inalámbrica completa con WPA/WPA2
- Compatible con los sistemas operativos de MAC OS y LinuxWindows 95/98/NT/2000/XP/2003 Server/Vista
- Garantía limitada de 3 años

300MbpsEnrutador inalámbrico N Gigabit
TEW-639GR(V1.0R)

Especificaciones

Hardware

Estándares	• Cableado: IEEE 802.3 (10Base-T), IEEE 802.3u (100Base-TX) y IEEE 802.3ab (1000BaseT) • Inalámbrico: IEEE 802.11b, IEEE 802.11g, IEEE 802.11n
WAN	• 1 puerto Auto-MDIX y de Auto-Negociación a 10/100/1000Mbps (internet)
LAN	• 4 puertos Auto-MDIX a 10/100/1000Mbps
Interuptor Activar/desactivar inalámbrico	• Encender y apagar LAN inalámbrica
Botón WPS	• Configuración Wi-Fi protegida (WPS) con otros dispositivos compatibles con WPS
Tipo de conexión	• IP dinámica, IP estática (fija), PPPoE, PPTP, L2TP
Cortafuegos NAT	• Entradas NAT configurables 3K; NAPT restringida • Rangos de IP, rangos de puerto y programación • Accionamiento de puertos para 24 aplicaciones especiales • Soporte ALG (soporte para activación/desactivación) –RTP/RTSP, AOL, FTP, ICMP, WMP/MMS, NetMeeting, SIP
WDS	• Compatible con sistema de distribución inalámbrico de activación/desactivación
UPnP	• 1.0 Compatible con UPnP IGD
DMZ	• Anfitrión DMZ, 24 servidores virtuales configurables y servidores para juegos
DNS	• Servidores DNS estáticos o asignados por WAN; 4 servicios verificados para DDNS
Control de acceso a Internet	• Acceso a internet por tiempo, filtración de servicios y de rango de puertos, restricción de dominios de Internet; 32 programaciones definidas por el usuario, 24 entradas de filtro de dirección MAC
Indicadores LED	• Adaptador eléctrico externo, LAN1~LAN4, WAN y WLAN
Adaptador de corriente	• Adaptador eléctrico externo 1A y 12V DC
Consumo eléctrico	• 779mA
Dimensiones (L x A x A)	• 180 x 122 x 30 mm (6.8 x 4.6 x 1.1 pulgadas)
Peso	• 350g (0.8 lb)
Temperatura	• Funcionamiento: 0°C~ 40°C (32°F~ 104°F); Almacenamiento: -20°C~ 60°C (-4°F~140° F)
Humedad	• Max. 90% (sin condensación)
Certificación	• CE, FCC

Inalámbrico

Frecuencia	• 2.412 ~ 2.472 GHz
Antena	• 3 antenas dipolo fijas de 4 dBi
Técnica de modulación	• 802.11n: BPSK, QPSK, 16QAM,64QAM con OFDM • 802.11b: CCK (11 y 5.5Mbps) DQPSK (2Mbps) DBSPK (1Mbps) • 802.11g: OFDM con BPSK, QPSK y Modulaciones Sub-Carrier (Subportadora) de 16/64-QAM
Transmisión de datos	• 802.11b: 11Mbps, 5.5Mbps, 2Mbps y 1Mbps • 802.11g: 54Mbps, 48Mbps, 36Mbps, 24Mbps, 18Mbps, 12Mbps, 9Mbps y 6Mbps • 802.11n: Hasta 300Mbps
Seguridad	• Cifrado: hardware AES/TKIP, 64/128-bit WEP (HEX/ frase clave – 11b/g) • 802.1X/EAP: EAP-TLE, EAP-TTLE/MSCHAPv2, PEAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC • WPA: WPA/WPA2, WPA-PSK/WPA2-PSK (AES-11b/g/n, TKIP-11b/g) • WPS: Compatible con PIN y PBC • Control de transmisión SSID
Salida de alimentación eléctrica	• 802.11b: 18dBm (típico) • 802.11g: 15dBm (típico) • 802.11n: 12dBm (típico) con HT20 o Ht40
Sensibilidad de recepción	• 802.11b: -84dBm (típico) @ 11Mbps • 802.11g: -72dBm (típico) @ 54Mbps • 802.11n: -68dBm (típico) con Ht20 -65dBm (típico) con HT40
Canales	• 1~11 (FCC), 1~13 (ETSI)

300MbpsEnrutador inalámbrico N Gigabit

TEW-639GR(V1.0R)

Solución en redes

Contenidos del paquete

- TEW-639GR
- Guía de instalación rápida multilingüe
- CD-ROM (guía del usuario)
- Cable ethernet Cat. 5 (1.5m / 4.9pi.)
- Adaptador de alimentación eléctrica (12V DC, 1A)

Productos Relacionados

TEW-624UB	Adaptador USB 2.0 inalámbrico-N 802.11g a 300Mbps
TEW-642EC	Tarjeta Express inalámbrica Wireless N
TEW-623PI	Adaptador PCI inalámbrico N-Draft a 300Mbps

Informacion de la orden

TRENDnet
20675 Manhattan Place,Torrance, CA 90501 USA
Tel: 1-310-961-5500
Fax: 1-310-961-5511
Web: www.trendnet.com
Email: sales@trendnet.com

Para ordenar por favor llame:

1-888-326-6061

D-Link®
Building Networks for People

108Mbps[1] Wireless Networking

DWL-2100AP

- **Up to 108Mbps[1] with D-Link 108G Products**
- **Improved Wireless Security with WPA and 802.1X Authentication**
- **SNMP Management Software Included**
- **More Mobility with WDS and Five Operational Modes**

2.4 GHz

ENHANCED SECURITY

SNMP MANAGEMENT SUPPORT

D-Link 108G

FREE 24/7 TECH SUPPORT (USA ONLY)*

AirPlus XTREME G®

802.11g/2.4GHz Wireless

108Mbps[1] Access Point

D-Link, the industry pioneer in wireless networking, introduces a performance breakthrough in wireless connectivity – **D-Link *Air*Plus *Xtreme G*™** series of high-speed devices now capable of delivering transfer rates up to 15x faster than the standard 802.11b with the new D-Link 108G. With the new *Air*Plus *Xtreme G* DWL-2100AP Wireless Access Point, D-Link sets a new standard for wireless access points.

With the D-Link 108G enhancement, the DWL-2100AP can achieve wireless speeds up to 15x in a pure D-Link 108G environment through the use of new wireless technologies such as Packet Bursting, Fast Frame, Compression & Encryption, and Turbo mode.These technologies enable a throughput high enough to handle video/audio streaming and future bandwidth-intense applications. The DWL-2100AP also supports SNMP v.3 for better network management with the provided Wireless AP Manager software that manages network configuration and firmware upgrades. For Enterprise networks, the DWL-2100AP supports network administration and real-time network traffic monitoring via D-Link's D-View Network Management software.

The DWL-2100AP features WDS (Wireless Distribution System) that can be configured to perform in any one of five modes: a Wireless Access Point, a Point-to-Point (PtP) bridge with another DWL-2100AP, a Point-to-Multipoint (PtMP) bridge, a Repeater for range extension, or as a Wireless Client. The WDS feature makes the DWL-2100AP an ideal solution for quickly creating and extending a wireless local area network (WLAN) in offices or other workplaces, or even at hotspots.

Wireless security is addressed as the DWL-2100AP uses WPA (Wi-Fi Protected Access) and 802.1X authentication to provide a higher level of security for data communication amongst wireless clients. The DWL-2100AP is also fully compatible with the IEEE 802.11b and 802.11g standards. With great manageability, versatile operation modes, solid security enhancement, the cost-effective D-Link *Air*Plus *Xtreme G* DWL-2100AP Wireless Access Point provides the ultra-fast wireless signal rates and everything else a network professional dreams of.

AirPlus XTREME G®

DWL-2100AP

802.11g/2.4GHz Wireless 108Mbps[1] Access Point

SPECIFICATIONS

Standards
- IEEE 802.11g
- IEEE 802.11b
- IEEE 802.11
- IEEE 802.3
- IEEE 802.3u

Device Management
- Web-Based – Internet Explorer v6 or later; Netscape Navigator v6 or later; or other Java- enabled browsers.
- SNMP v.3

Wireless Distribution System
- AP Client
- PtP Bridge
- PtMP Bridge
- Repeater

Security
- 64-, 128 152-bit WEP
- 802.1X (EAP-MD5, EAP-TLS, EAP-TTLS and EAP-PEAP)
- WPA —Wi-Fi Protected Access
- MAC Address Access Control (WPA-TKIP and WPA-AES)

Media Access Control
CSMA/CA with ACK

Wireless Frequency Range
2.4GHz to 2.4835GHz

Wireless Operating Range[2]
Indoors: Up to 328 ft (100 meters)
Outdoors: Up to 1312 ft (400 meters)

Modulation Technology
- Orthogonal Frequency Division Multiplexing (OFDM)
- Complementary Code Keying (CCK)
- DQPSK
- DBPSK

Wireless Transmit Power
15dBm (32mW) ± 2dB
(Control TX power level from full, 50%, 25%, 125% and min.)

Receiver Sensitivity
- 54Mbps OFDM, 10% PER,-66dBm)
- 48Mbps OFDM, 10% PER,-71dBm)
- 36Mbps OFDM, 10% PER,-76dBm)
- 24Mbps OFDM, 10% PER,-80dBm)
- 18Mbps OFDM, 10% PER,-83dBm)
- 12Mbps OFDM, 10% PER,-85dBm)
- 11Mbps CCK, 8% PER,-83dBm)
- 9Mbps OFDM, 10% PER,-86dBm)
- 6Mbps OFDM, 10% PER,-87dBm)
- 2Mbps QPSK, 8% PER,-89dBm)

External Antenna Type
1.0dB Dipole with reverse SMA connector

LEDs
- Power
- LAN (10/100)
- WLAN (Wireless Connection)

Temperature
- Operating: 32°F to 140°F (0°C to 40°C)
- Storing: 4°F to 149°F (-20°C to 65°C)

Humidity
95% maximum (non-condensing)

Power Input
Ext. Power Supply DC 5V, 2.0A

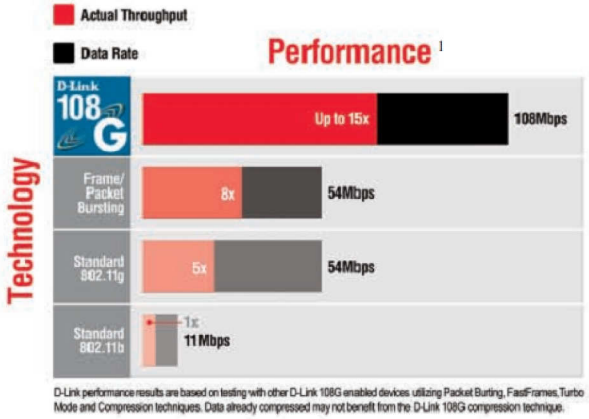
Safety & Emissions
• FCC • UL • VCCI • CSA • EN

Dimensions
- L = 5.6 inches (142mm)
- W = 4.3 inches (109mm)
- H = 1.2 inches (31mm)

Weight
0.44 lbs (200g)

Warranty
3 Year

[1] Maximum wireless signal rate derived from IEEE Standard 802.11g specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead lower actual data throughput rate.
[2] Environmental conditions may adversely affect wireless signal range.



D-Link®
Building Networks for People

HP ProLiant ML110 G7 Server

Data sheet

Affordability, reliability, and simplicity make the HP ProLiant ML110 G7 Server the ideal first server for growing businesses.

Are you using your desktop as a server? If yes, then it is time for a change. A growing business like yours, with its limited in-house IT support, needs a server that is compact and suits the budget—and also one that you can remotely manage.

The HP ProLiant ML110 G7 Server delivers true server reliability and functionality for growing businesses, branch offices, and remote locations—all for the price of a typical desktop computer. It perfectly matches your business needs and helps you adapt to the future with confidence.

What makes the HP ProLiant ML110 G7 Server an ideal first server?

Going beyond the proven ProLiant reliability, the ProLiant ML110 G7 Server is powered by the latest Intel® Xeon®, Intel Core™ i3, Intel Pentium®, or Intel Celeron® processor; network interface controllers (NICs); and DDR3 memory, which together enhance performance. PCI Express (PCIe) Gen2 slots, DIMM slots, drive bays, and server options help deliver the expandability that your growing business needs. Additionally, the HP SmartStart CD augments the installation process and helps you step up to your first server network with ease.

The optional trusted platform module (TPM) is an added advantage that brings further security to your IT architecture. Support for an energy-efficient redundant power supply (RPS) and integrated HP Integrated Lights-Out 3 (iLO 3) remote management software brings down operational expenses by reducing the number of physical visits to the server site—making it a practical and affordable solution.

More on HP iLO 3

HP Insight Control is essential server management software that helps deploy servers quickly, manage virtual or physical server health proactively, control servers from outside of the office, and streamline power consumption. HP iLO 3 is a standard component of the ProLiant ML110 G7 Server that facilitates remote server manageability. It includes an intelligent microprocessor, secure memory, and a dedicated network interface. In addition to providing world-class remote management functionality, iLO 3 is also responsible for managing the health of your server. For more information about HP iLO 3 for ProLiant servers, visit **www.hp.com/go/insightcontrol**.

Key features and benefits

Proven HP dependability and support

- HP conducts some of the most rigorous and thorough testing in the industry. This testing, along with a worldwide network of HP service professionals, allows you to deploy the ProLiant ML110 G7 Server with confidence.
- The ProLiant ML110 G7 Server inherits ProLiant reliability. Our tireless efforts on system testing and process control can provide you with a very dependable solution.

Ease to expansion and growth with changing business needs

- Delivers off-the-shelf functionality and expandability to grow with your business with features such as two NICs, DDR3 memory, SAS and SATA hard drives, PCIe Gen2 slots, and USB 2.0 ports
- Requires less upfront investment due to the server's modular design, and offers an easy-to-use and easy-to-configure platform because all major server components can be removed or reinstalled with reduced effort
- Helps remote locations or branch offices reduce server downtime and improve productivity with iLO 3—remote management capability from HP

A true server at a desktop price

- Compact and simple design for better manageability and low-cost expansion
- Efficient power usage and remote management to reduce overall operational costs
- Improved processor and memory performance for better results
- Advanced remote management software drives down the cost of managing your servers by reducing the number of physical visits.

Proven ProLiant reliability and data protection

- ECC memory helps protect your business from data loss and unplanned system downtime. Unlike standard memory, ECC memory can detect and correct single-bit errors.
- HP Smart Array options provide businesses with RAID mirroring and striping capabilities to protect critical data.
- The TPM hardware-based encryption and authentication feature provides increased data security.
- HP ProLiant 100 series servers have customizable features suitable for the varying usage needs of small and medium businesses and branch offices.
- RPS for better protection against data loss/attack and for essential productivity backup.

Ideal environment

Here is a quick checklist that can help you decide if the ProLiant ML110 G7 Server is the right solution for you.

Remote sites or branch offices of small- to medium-sized businesses running light applications, such as:

- File and print
- Web messaging
- Small vertical applications or databases
- Shared Internet access and LAN infrastructure

Budget-conscious businesses with the need for:

- An entry-level, single-processor server solution that is easy to use and easy to configure
- A reliable server that can protect your data 24x7
- A rack-mountable server that helps save data center space
- An affordable server that can be remotely managed and controlled
- An expandable server that can grow with your business needs

Technical specifications

HP ProLiant ML110 G7 Server

Processor and memory	
Processor family	Intel Xeon E3 series, Intel Core i3, Pentium, or Celeron processor
Number of processors	1
Maximum number of cores	4
Processors supported	E3-1280, E3-1270, E3-1240, E3-1230, E3-1220, i3-2120, i3-2100
Processor cores	Quad-core, Dual-core
Cache	8 MB Intel Smart Cache
Maximum processor speed	3.50 GHz
Memory type	PC3-10600E Unbuffered DDR3 ECC up to 1333 MHz
Memory slots	4 DIMM slots
Standard memory	2 GB or 4 GB, depending on model
Maximum memory	16 GB
Storage	
Storage type	Non-hot-plug 3.5 in. SAS Non-hot-plug 3.5 in. SATA
Drives supported	4 LFF HDD NHP and HP SAS/SATA 8 SFF
Maximum internal storage	8 TB
Maximum internal drives	4
Removable media bays	2
Expansion slots	**4 slots:** • Slot 1: PCIe Gen2, x16 (x16 connector), full height and full length • Slot 2: PCIe Gen2, x4 (x8 connector), full height and full length • Slot 3: PCIe Gen2, x4 (x8 connector), full height and full length • Slot 4: PCIe Gen2, x4 (x1 connector), full height and full length
Storage controller	HP Embedded Smart Array B110i SATA RAID Controller (RAID 0/1/10)
Operating system	
Windows	• Microsoft® Windows® Server 2008 for Embedded Systems - SP2 and R2 with SP1 • Microsoft Windows Server 2008, Standard Edition (x86 and x64) - SP2 and R2 with SP1 • Microsoft Windows Server 2008, Enterprise Edition (x86 and x64) - SP2 and R2 with SP1 • Microsoft Windows Server 2008, Web Server (x86 and x64) - SP2 and R2 with SP1 • Microsoft Windows Foundation Server 2008 (x64) - SP2 and R2 with SP1 • Microsoft Windows Server 2008 Embedded Systems (x64) - SP2 and R2 with SP1 • Microsoft Windows Small Business Server 2011 Essentials (Aurora) • Microsoft Windows Small Business Server 2011 • Microsoft Windows 8 Server
Linux	• RHEL 5 (includes KVM) • RHEL 6 (includes KVM) • SLES 10 (includes XEN) • SLES 11 (includes XEN)
Enabled OS	• OEL 6 • Asianux (latest version based on RHEL6) • CentOS (latest version based on RHEL6) • Debian (latest version) • Ubuntu (latest version) • Fedora (latest version) • OpenSUSE (latest version)

Technical specifications Continued

Deployment	
Form factor	Tower with rackmount option kit
Rack height	4U
System fans	Standard
Power supply	Standard 350 W non-hot-plug, non-redundant power supply (80% efficiency) RPS 460 W (92% efficiency)
Graphics card (tested)	64 MB; supports all display resolutions up to 1600 x 1200 @ 75 Hz NVIDIA Quadro 600 NVIDIA Quadro FX 380 LP
Port	10 USB 2.0
Networking	2 Intel 82574 Gigabit NIC
Remote management	HP Integrated Lights-Out 3 HP SmartStart CD
Warranty	Worldwide, except Brazil: 1-year parts/1-year labor/1-year onsite Brazil only: 3-year parts/1-year labor/1-year onsite

HP Financial Services

HP Financial Services provides innovative financing and financial asset management programs to help you cost-effectively acquire, manage, and ultimately retire your HP solutions. For more information, contact your local HP representative or visit **www.hp.com/go/hpfinancialservices**.

Take your organization to the next level of productivity and efficiency

For a simple, surprisingly affordable, and reliable server-based computing, choose the HP ProLiant ML110 G7 Server. Visit **www.hp.com/servers/ml110-g7** for more information.

HP Services

When technology works, business works.

HP Technology Services has a robust portfolio of packaged lifecycle support solutions that enable you to leverage ProLiant server support for better business outcomes.

Optimized Care: delivers superior performance and availability of crucial ProLiant systems through deployments and proactive management practices.

- HP ProLiant Server Hardware Installation
- 3-year HP 6-hour Hardware Support Onsite Call-to-Repair

Standard Care: maintains a high level of server availability along with expert help to cut the cost and complexity of implementing and supporting ProLiant servers.

- HP ProLiant Server Hardware Installation
- 3-year HP 24x7 4-hour response, Hardware Support Onsite Service

Basic Care: delivers minimum recommended support service level with expert advice, implementation, and support.

- HP ProLiant Server Hardware Installation
- 3-year HP 13x5 4-hour response, Hardware Support Onsite Service

All come with HP Insight Remote Support, available at no additional cost, delivering remote monitoring, diagnosis, and problem resolution.

Only HP brings together deep expertise, proactive and business-critical support, and a strong partner network.

For more information, visit **www.hp.com/services/proliant**.

Get connected

www.hp.com/go/getconnected

Current HP driver, support, and security alerts delivered directly to your desktop

4AA3-3719ENW, Created March 2011

APC Smart-UPS 2200VA USB & Serial 120V

SUA2200

APC Smart-UPS, 1980 Watts / 2200 VA,Entrada 120V / Salida 120V, Interface Port DB-9 RS-232, USB, SmartSlot
Incluye: DC con software, Cable RS-232 de señalización Smart del UPS, Cable USB, Manual del usuario

Salida

Capacidad de Potencia de Salida 1980 Vatios / 2200 VA
Máxima potencia configurable 1980 Vatios / 2200 VA
Tensión de salida nominal 120V
Eficiencia con carga completa 95%
Distorsión de tensión de salida Menos del 5% con carga completa
Frecuencia de salida (sincronizada a red eléctrica principal) 47 - 53 Hz para 50 Hz nominal,57 - 63 Hz para 60 Hz nominal
Factor de cresta hasta 5 : 1
Tipo de forma de onda Onda senoidal
Conexiones de salida

(8) NEMA 5-15R 

(2) NEMA 5-20R 

Entrada

Entrada de voltaje 120V

Frecuencia de entrada
50/60 Hz +/- 3 Hz (autosensible)

Tipo de enchufe
NEMA 5-20P

Longitud del cable
1.83 metros

Variación de tensión de entrada
para operaciones principales
82 - 144V

Variación de tensión de entrada adaptable para operaciones principales
75 - 154V

Baterías y autonomía

Tipo de batería
Batería sellada de plomo sin necesidad de mantención con electrolito suspendido: a prueba de filtración

Tiempo típico de recarga
3 hora(s)

Cartucho de repuesto de batería
RBC55

Cantidad de cartuchos de batería de recambio
1

Duración típica de reserva
a media carga
24.1 minutos (990 Vatios)

Duración típica de reserva
con carga completa
6.7 minutos (1980 Vatios)

Tabla de duración
Smart-UPS

Comunicaciones y manejo

Puerto de interfaz
DB-9 RS-232,USB,SmartSlot

Cantidad de interfaces SmartSlot™
1

Panel de control
Visualizador de estatus LED con gráfico de barras de carga y batería y en línea: En línea: Batería en actividad: Batería de reemplazo: e indicadores de sobrecarga

Alarma audible
Alarma de batería encendida: alarma distintiva de carga de batería baja: retrasos configurables

Interruptor de emergencia (EPO)
Sí

Proteção contra surtos e filtragem

Clasificación de energía de sobrecarga (Joules)
459 Joules

Filtrado
Filtrado completo de ruidos multipolares: sobretensión tolerable de 0,3% IEEE: tiempo de respuesta de cierre cero: cumple con UL 1449

Físico

Dimensiones de altura máxima
432.00 mm

Dimensiones de anchura máxima
196.00 mm

Dimensiones de profundidad máxima
546.00 mm

Peso neto
50.91 KG

Peso de embarque
60.91 KG

Altura de envío
559.00 mm

Anchura de envío
381.00 mm

Profundidad de envío
762.00 mm

Color
Negro

Unidades por tarima
3.00

Ambiental

Ambiente operativo
0 - 40 °C

Humedad relativa de operación
0%

Elevación de operación
0-3000 metros

Temperatura de almacenamiento
-15 - 45 °C

Humedad relativa de almacenamiento
0%

Elevación de almacenamiento
0-15000 metros

Ruido audible a 1 metro de la superficie de la unidad
45.00 dBA

Disipación térmica en línea
275.00 BTU/hora

Conformidad

Aprobaciones
CSA,FCC Part 15 Clase A,UL 1778
Garantía estándar
Reparación o reemplazo por 2 años,garantías opcionales en el lugar de trabajo disponibles,garantías extendidas opcionales disponibles
Environmental Compliance
RoHS 7b Exemption

**Tiempo de recarga del 90% de la capacidad total de la batería luego de una descarga hasta el apagado utilizando una carga clasificada para la mitad del régimen de carga completa del UPS.