Universidad Nacional Autónoma De Nicaragua
Unan-Managua
Recinto Universitario Rubén Darío
RURD
Facultad De Ciencias E Ingeniería
Departamento de Tecnología

Implementación de un sistema de vigilancia y control de eventos con acceso a través de red, en el área de tesorería en la UNAN – Managua recinto Rubén Darío.

AUTORES: *Br.: Martha Alicia Jarquin Cerda*

Br.: Leslie Vladimir Torrez Alburto

TUTOR: *Msc.: Álvaro Segovia*

MANAGUA, NICARAGUA

Contenido

LISTA DE FIGURAS

LISTA DE TABLAS

Agradecimiento:

Mi gratitud, principalmente está dirigida al Dios Todopoderoso por haberme dado la existencia y permitido llegar al final de mi carrera.

A mis padres por haberme apoyado en todo momento, por sus consejos, sus valores, por la motivación constante que me ha permitido ser una persona de bien, pero más que nada, Por los ejemplos de perseverancia y constancia que los caracterizan y que me ha infundado siempre, por el valor mostrado para salir adelante y por su amor.

Quiero agradecerles enormemente a mis hermanos Carlos Alberto y Misael por haberme apoyado siempre en todo el recorrido de mi carrera

A todos quienes de una u otra forma han colocado un granito de arena para el logro de este Trabajo de Grado, agradezco de forma sincera su valiosa colaboración

Martha Alicia Jarquin Cerda

Dedicatorias.

A Dios por haberme permitido llegar hasta este punto y haberme dado salud para lograr mis objetivos, además de su infinita bondad y amor.

A mis padres quienes permanentemente me apoyaron con espíritu alentador, contribuyendo incondicionalmente a lograr las metas y objetivos propuestos.

A mi abuela Zulema por ser una de las personas más importante de mi vida y por siempre apoyarme con consejos , a mi tía Johanna y mi tía Yadira por ser mujeres fuerte, las cuales han llegado a ser una gran espiración para mi formación como persona

A mi tío Mayron que si no hubiera sido por el yo no hubiera culminados este trabajo de grado

¡Gracias a ustedes!

Martha Alicia Jarquin Cerda

Dedicatoria

A mi padre Dios puesto que me brinda sabiduría, amor y paciencia el cual me llena de bendiciones de oportunidades para alcanzar mis sueños dándome la valentía para sobrepasar las adversidades permitiéndome luchar por mis metas.

A mi madre que hizo un enorme esfuerzo por permitir culminar mis estudios, gracias por todo mama por darme una carrera para mi futuro y por creer en mí, por brindarme tu fortaleza por ser madre y padre para mí. Te lo agradezco se que hemos pasado momentos difíciles pero siempre has estado ahí apoyándome y brindándome todo tu amor por todo esto te lo agradezco de todo corazón que estés conmigo a mi lado, gracias mama.

Leslie Vladimir Torrez Aburto

Agradecimiento

Primeramente agradezco a Dios por regalarme vida y permitirme culminar mis estudios universitarios, gracias padre.

A la (UNAN – Managua) puesto que nos brindó el conocimiento y los recursos necesarios que nos ayudaron para el desarrollo del proyecto y a la elaboración final de este.

A los profesores que me brindaron su sabiduría en varios campos del conocimiento a lo largo de la carrera ayudándome así en varios aspectos que requerí para el desarrollo del proyecto.

Gracias a nuestros compañeros de clase que de varias maneras siempre estuvieron acompañándonos y ayudándonos en los momentos que requeríamos ayuda , por compartir conocimientos con nosotros , por compartir vivencias con nosotros y darnos sentimientos de alegría, amor , cariño que nos dejaran muchas enseñanzas y experiencias.

Finalmente no puedo dejar de agradecer la compañía de mis familiares y amigos a lo largo de este proyecto, gracias a todos.

Leslie Vladimir Torrez Aburto

I. Justificación

Actualmente la labor de vigilancia en el área de tesorería de la universidad autónoma de Nicaragua (UNAN-Managua) consta de un guarda de seguridad en el área externa de ventanilla (área de atención al público) únicamente en el horario de atención al público (8am - 6pm) y rondas periódicas fuera de este horario, no existe ningún agente de seguridad o supervisor en el área interna de esta área.

El área de tesorería de la unan Managua en la actualidad no cuentan con un sistema de vigilancia automatizado que permita vigilar y auditar el flujo de personas y otros eventos que sucedan en esta área ya sea en horario de atención o fuera del mismo.

En repetidas ocasiones se han presentado diversas irregularidades, tales como pérdidas de dinero, ingresos no autorizados y/o fuera de horario laboral e incidentes con los clientes que realizan transacciones en esta área. Las cuales por falta de un sistema de vigilancia han sido muy difíciles de esclarecer.

II. Resumen

El proyecto a desarrollar está ubicado en el área de tesorería de la (UNAN-MANAGUA) recinto universitario Rubén El área de tesorería como centro de pagos de diferentes tipos cuenta en la actualidad de un guarda de seguridad en el área externa y un sistema de alarma, no cuenta con un sistema de vigilancia automatizado que permita vigilar y auditar el flujo de personas.

Al implementar un sistema de vigilancia automatizado en esta área por medio de cámaras IP se puede tener un monitoreo de eventos e incidentes tanto en el área externa como interna de dicha área, cuando hablamos de un sistema de vigilancia automatizado nos referimos a todo tipo de aparatos para la detección inmediata o sistemática, la visualización de un proceso con ayuda técnica, sensores u otros sistemas de vigilancia como una cámara IP.

Las cámaras IP son una parte fundamental de los sistemas de vigilancia que permiten evaluar mejor la situación en puntos críticos tales como este centro de pagos donde se puede monitorear mediante los sistemas basados en una cámara IP,

La plataforma será LINUX usar esta tiene sus ventajas es libre esto significa que la (UNAN-Managua) no tiene que pagar licencia a ninguna casa desarrolladora de software ya que LINUX se distribuye bajo GNU por lo tanto el código fuente tiene que estar siempre accesible.

El software para la monitorización y manipulación de las cámaras IP será zoneminder es una aplicación para LINUX con el cual podremos capturar, analizar, grabar y monitorizar el contenido de las cámaras.

Entre las características especiales de zoneminder destaca que podemos programar los horarios de funcionamiento de las cámaras, así como el modo de grabación, podemos elegir entre fotografías en secuencia o grabar vídeo de manera continua.

III. Introducción

Un sistema de vigilancia refiere a todo tipo de aparatos para la detección inmediata, sistemática y protocolaria, de la la visualización o vigilancia de un proceso con ayuda técnica, sensores u otros sistemas de vigilancia, como por ejemplo una cámara.

La función de los sistemas de vigilancia es de poder intervenir en un proceso como una alarma, cuando el proceso no se efectúa de la forma deseada. Los sistemas de vigilancia son una clase especial de protocolos en la que se controlan diferentes tipos de parámetros. Las videocámaras son una parte fundamental de los sistemas de vigilancia que permiten evaluar mejor la situación en puntos críticos. Los sistemas de vigilancia basados en una IP son cada vez más comunes, pues se instalan de forma rápida y sencilla, se pueden ampliar fácilmente y es posible usarlos y configurarlos a través de cualquier ordenador.

Los sistemas de vigilancia IP, comprimen las imágenes y audio capturados por las cámaras y micrófonos y transmiten por una red de datos Local o Internet (LAN / WAN) y pueden ser accedidos desde uno o varios puntos en cualquier lugar del mundo mediante computadoras convencionales (o hardware especialmente diseñado) para descomprimir los datos, visualizarlos, analizarlos, grabarlos, incluso generar acciones de manera automática en respuesta a diferentes eventos pre-definidos o a voluntad de un operador.

Aunque su nombre es "servidor de video", generalmente el dispositivo también es capaz de transmitir y recibir audio, así como señales de control para mover o hacer acercamiento de las cámaras análogas que se conecten al mismo y que soporten esas funciones (según el modelo y fabricante).

Una cámara IP tiene su propia dirección IP y un web server para gestionar la comunicación en la red. Todo lo que se precisa para la visualización de las imágenes a través de la red se encuentra dentro de la misma unidad. Una cámara IP puede describirse como una cámara y un ordenador combinados. Algunos modelos pueden incluir entradas para alarmas y salida de relé.

IV. Objetivos

a. Objetivo general:

Implementar el monitoreo de eventos e incidentes tanto en las zonas externas e internas del área de Tesorería de la Universidad Nacional Autónoma de Nicaragua (UNAN-Managua), mediante la implementación de un sistema de vigilancia, a través de la red.

b. Objetivo especifico

1. Implementar un sistema de vigilancia accesible a través de la red.
2. Garantizar la vigilancia constante y permanente del área de Tesorería de la Universidad Nacional Autónoma de Nicaragua (UNAN-Managua).
3. Auditar los eventos que ocurren en el área de Tesorería de la (UNAN-Managua) mediante la vigilancia.

V. Fundamentación teórica:

a. Sistema de vigilancia

Un sistema de vigilancia refiere a todo tipo de aparatos cuya utilización es para la detección inmediata, sistemática y de forma protocolaria, de la visualización de un proceso, con ayuda técnica especializada, lo que puede incluir sensores entre otros equipo. La función de los sistemas de vigilancia es de poder intervenir en el momento oportuno en un proceso a través de alarma, cuando el proceso no se efectúa de la forma deseada.

Generalmente un sistema de seguridad no es sólo un servicio aislado sino una combinación de elementos físicos y electrónicos o una combinación de ambos, y fundamentalmente un compromiso, por parte del usuario, de utilizar apropiadamente los sistemas.

Los sistemas de vigilancia van evolucionando de acuerdo a las nuevas necesidades de los usuarios (empresas, hogares, etc.) facilitando cada vez más su control y seguridad, a través de los infaltables sistemas y proyectos tecnológicos, que son complementados con otras tecnologías, como por ejemplo con equipos computacionales, que son de gran utilidad para entregar mejores productos y servicios de seguridad.

Entre los equipos de seguridad más importantes tenemos las cámaras de vigilancia, dentro de esta categoría podemos señalar las cámaras IP (o cámara de red).

Un sistema de video vigilancia IP está compuesto por cámaras de seguridad que permiten el monitoreo de lugares que requieren observación. Estos sistemas de vigilancia funcionan al asignarle a la cámara de seguridad una dirección IP fija y pública. Lo que permite que las imágenes emitidas desde las cámaras, puedan ser vistas en tiempo real desde cualquier lugar y por varias personas a la vez, (si fuese necesario), a través de un computador o notebook. Es importante mencionar que este tipo de cámaras permite grabar imágenes o secuencias en nuestro PC, dejando evidencia del monitoreo.

5. Cámara IP

Una cámara IP no es más que una unidad de captura de imagen y que las emite directamente a la red (Intranet o internet), nos entrega la señal de video en forma digital, es decir en unos y ceros. Existen dos clases de cámaras IP, las creadas por fábricas procedentes del mundo de TI (Tecnología de Información, es decir, computadores) y las creadas por fábricas procedentes del mundo de la seguridad electrónica tradicional.

Las primeras son elementos que buscan llevar video a sitio remotos, bajo condiciones favorables, sin una misión especial, más que la de comunicar. Éstas fueron las consecuencias obvias y naturales de las tecnologías de Videoconferencia que revolucionaron, hace algunos años, la forma de trabajo en muchas compañías. Son elementos cuya misión no necesariamente es seguridad.

Hoy en día se han generalizado y están de moda, gracias al avance de la capacidad de proceso y almacenamiento, sumado al avance en técnicas de procesamiento digital de señales y por supuesto a los precios bajos, consecuencia de esto mismo. En este grupo de cámaras tenemos marcas para satisfacer todos los gustos, precios, colores y tamaños. Son elementos, cuya labor es captar una imagen de video, transmitirla por una red de datos.

Las cámaras son unidades que manejan lentes autoiris (DC o Video), lentes zoom, poseen chips (CCD o similar) de altas resoluciones y excelente desempeño a baja iluminación. Sus circuitos digitales poseen DSP para efectuar ajustes de color y dar un excelente rango de BLC. Sus circuitos que manejan niveles de ruido bajos y soportan amplio rangos de temperatura y humedad relativa. Poseen ajustes (digitales con menú sobre el video ó mediante DIP switch) de todo tipo, en donde puedo hacer ajuste manual de blancos y controlar la velocidad del Shutter. Puede hacerse ajustes de fase para sincronizar las cámaras y puede hacerse ajustes mecánicos de level para sacar todo el provecho del lente autoiris. Pueden cambiar de modo monocromático a color y su resolución puede alterarse de acuerdo al nivel de iluminación. Las más nuevas incorporan detectores de movimiento en cada cámara y permiten hacer estos

ajustes vía remota mediante la misma conexión de video. Son elementos que fueron pensados y fabricados para permanecer encendidos 24 horas. La única diferencia es que no entregan en un conector BNC, la señal de video NTSC, en forma análoga, sino que entregan la señal de forma digital en un conector RJ45.

5.1.1. Ángulo de visión

El ángulo de visión de una cámara IP hace referencia a la zona de cobertura que se observa con el uso de este equipo, este ángulo de visión varía en función del modelo de la cámara, longitud focal y la distorsión del lente.

En la figura 1. Se indica cómo se mide el ángulo de visión de una cámara.

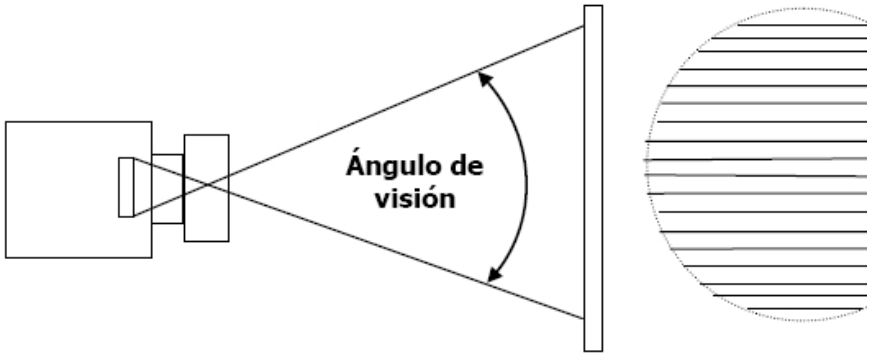


Fig. 1. Ángulo de Visión.

5.1.2. Como se comprime la información

Simplemente para que las imágenes digitalizadas lleguen a su destino con buena resolución y velocidad, usando la mínima cantidad de recursos de la red de datos existente. Es decir usando el menor Ancho de Banda (BW) posible.

Recordemos que el ancho de banda es la máxima velocidad de transmisión simultánea que un medio de comunicación puede transmitir. Esta dado numéricamente en bits por segundo (bps).

Como la información de video se compone de 30 imágenes por segundo y cada imagen a buena resolución (VGA, D1 o superior), entonces un segundo de video ocuparía (30x640x480x3x8) 211 Mbps aproximadamente, velocidad gigante comparada con la velocidad de las redes de datos disponibles hoy en día (menor a 10Mpbs en el 85% de los casos). Una buena etapa de compresión, reduce a 2Mbps aproximadamente y esto hace que sea viable transmitir video por las redes actuales.

Dentro de una cámara IP, la señal digital y comprimida, es entregada a través de una tarjeta de red de tipo Ethernet, estándar existente en la gran mayoría de redes actuales. Finalmente la información es ordenada siguiendo protocolos de transmisión conocidos y usados en las redes de cómputo. Por lo tanto es necesario que la cámara maneje múltiples protocolos, como HTTP, SMTP, DHCP, UDP, TCP/IP, HMTL, entre otros.

La cámara IP se comporta como un nodo más de la red, es decir como un miembro más de los equipos que están identificados con una dirección IP, por lo tanto puede accederse a ella con solo direccionarla adecuadamente desde cualquier otro PC en la red.

5.2. Estándares de compresión de vídeo

Para la transmisión de las imágenes, dada la gran cantidad de datos que compone los archivos audio/vídeo, es necesario recurrir a las herramientas de compresión. La ventaja que se obtiene con estas herramientas es la disminución de datos para transferir, pero por otro lado la compresión conlleva también una alta degradación de la calidad de la imagen.

La compresión y la gestión de ésta es dada a las cámaras digitales que, equipadas con una CPU, tienen la capacidad de cálculo suficiente para esta operación.

Existe una gran selección de algoritmos de compresión:

5.2.1. M-JPEG

El Motion JPEG o M-JPEG es tal vez el más usado entre los algoritmos de compresión de vídeo. Las cámaras digitales efectúan adquisiciones de cada fotograma y su compresión en formato

JPEG. Terminada la compresión, la cámara genera una trasmisión en flujo continuo de max. 30 imágenes por segundo (30 fps). En el caso de una trasmisión superior a los 16 fps las imágenes se perciben con el ojo humano como un movimiento fluido. Este algoritmo de compresión toma el nombre de Motion JPEG porque de hecho se transmiten tantas imágenes completas con el mismo nivel de compresión y calidad en el formato JPEG.

Una de las ventajas del estándar Motion JPEG está en el hecho de que varias imágenes de una secuencia vídeo pueden tener la misma calidad, que varía según el nivel de compresión elegido por la cámara de redes o por el codificador de vídeo. Mientras más grande sea el nivel de compresión, menor es la calidad de las imágenes y la dimensión del archivo. En algunas condiciones, por ejemplo de poca iluminación o cuando la toma se vuelve compleja, las dimensiones del archivo de la imagen pueden volverse aún más grandes y gastar más ancho de banda y más espacio de memorización. Para impedir el aumento del ancho de banda y del espacio de memorización gastados, los productos con tecnología de vídeo de red Axis permiten al usuario imponer un límite máximo de dimensión del archivo para un fotograma de la imagen.

Como no existen lazos entre los fotogramas en el formato Motion JPEG, el vídeo Motion JPEG es sólido en el sentido de que si durante la transmisión se pierde un fotograma, el resto del vídeo no se verá afectado.

El formato Motion JPEG es un estándar que no prevé la adquisición de ninguna licencia. Su característica es una amplia compatibilidad y se difunde en aplicaciones donde se necesitan fotogramas individuales de una secuencia vídeo (por ejemplo, para el análisis) y en donde se utilizan velocidades de transmisión reducidas, normalmente 5 fotogramas por segundo o menos. El estándar Motion JPEG puede ser útil también para aplicaciones que requieren la integración con sistemas que apoyan sólo Motion JPEG.

La desventaja principal del estándar Motion JPEG es el hecho de que no utiliza técnicas de compresión de vídeo para reducir los datos ya que consiste de una serie de imágenes fijas y completas. El resultado es una velocidad de transmisión en bit relativamente alta o una

relación de compresión baja para la calidad ofrecida respecto a los estándares de compresión de vídeo MPEG-4 y H.264

5.1.2. MPEG y MPEG-4

El MPEG es muy usado en el streaming audio/vídeo, a diferencia del M-JPEG este algoritmo se basa en la confrontación entre imágenes únicas adquiridas de las cámaras digitales transmitiendo una sola imagen completa y compresa y sucesivamente trasmitiendo sólo las diferencias con la imagen indicada.

Este algoritmo de compresión lleva a una gran reducción de los datos para transmitir. El MPEG ha sido creado a finales de los años 80 y al paso de los años ha tenido mejorías pasando de MPEG-1 a MPEG-2 y actualmente a MPEG-4 que puede superar los límites de los 25/30 fps de las primeras versiones manteniendo un bit rate relativamente bajo.

Cuando se habla de estándar MPEG-4 en aplicaciones de video vigilancia, a menudo se refiere al estándar MPEG-4 parte 2, conocido también como MPEG-4 Visual. Como a todos los estándares MPEG se lo puede adquirir con licencia, o sea, los usuarios tienen que pagar una tarifa asociada a la licencia para cada una de las estaciones de vigilancia. El estándar MPEG-4 apoya aplicaciones con ancho de bando limitado y aplicaciones que requieren imágenes de alta calidad, sin límites de velocidad de transmisión y con ancho de banda virtualmente ilimitado.

5.2.3. H.264

El H.264 forma parte de una nueva generación de algoritmos de compresión en vías de desarrollo cuyo fin es obtener una elevada compresión de datos pero manteniendo una alta calidad de las imágenes y teniendo también un bit rate inferior a los estándares anteriores. El estándar H.264, conocido también como MPEG-4 Parte 10/AVC, donde AVC es la sigla de Advanced Video Coding, es el estándar MPEG más reciente para la codificación de vídeo. Seguramente es destinado a llegar a ser el estándar de vídeo más difundido en el futuro. Un codificador que apoya el estándar H.264 es capaz de reducir las dimensiones de los archivos de

vídeo digitales de más del 80% respecto al formato Motion JPEG y hasta el 50% respecto al estándar MPEG-4, sin compromisos en términos de calidad de las imágenes. Lo que significa que para la gestión de los archivos de vídeo es necesario menos espacio de memorización y ancho de banda, o que es posible obtener imágenes de calidad más elevada con la misma velocidad de trasmisión en bit.

El estándar H.264 es el fruto del trabajo conjunto de las organizaciones responsables de la definición de estándar para los sectores de las telecomunicaciones (Video Coding Experts Group de ITU-T) e IT (Moving Picture Experts Group de ISO/IEC) y es destinado a tener una difusión aún más amplia respecto a los estándares anteriores. En el sector de video vigilancia, es muy probable que el estándar de compresión H.264 venga rápidamente aprobado para las aplicaciones que requieren resoluciones y velocidad de transmisión elevadas, por ejemplo para la vigilancia de autopistas, aeropuertos y casinos, donde el uso de 30/25 fotogramas (NTSC/PAL) por segundo representa la norma. Estos últimos son de hecho ámbitos en los que la reducción del ancho de banda y del espacio de memorización necesarios puede ofrecer las ventajas más significativas.

El estándar H.264 es probablemente destinado también a acelerar la difusión de las cámaras de red con resolución mega píxel porque esta tecnología de compresión ultra-eficiente es capaz de reducir las dimensiones de los archivos grandes y la velocidad de transmisión in bit sin comprometer la calidad de las imágenes. El nuevo estándar presenta también alguna desventaja. Aunque ofrece ventajas significativas en términos de ancho de banda y espacio de memorización, este estándar requiere la aplicación de las cámaras de red y estaciones de vigilancia de altas prestaciones.

5.3. Protocolos de comunicación

El **nivel de aplicación** o **capa de aplicación** es el séptimo nivel del modelo OSI.

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 protocolos de transferencia de archivos (FTP)

En esta capa aparecen diferentes protocolos:

- FTP (*File Transfer Protocol* - Protocolo de transferencia de archivos) para transferencia de archivos.
- DDNS (Dynamic *Domain Name System* - Sistema Dinámico de Nombres de Dominio).
- DHCP (*Dynamic Host Configuration P*rotocol - Protocolo de configuración dinámica de anfitrión).
- SMTP (*Simple Mail Transport Protocol*).
- UDP (User Datagram Protocol)
- TCP/IP (Protocolo de control de transmisión/Protocolo de Internet)
- UPnP (Universal Plug and Play)
- GPRS (General packet radio service)

FTP (*File Transfer Protocol* - Protocolo de transferencia de archivos) es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.

El servicio FTP es ofrecido por la capa de aplicación del modelo de capas de red TCP/IP al usuario, utilizando normalmente el puerto de red 20 y el 21. Un problema básico de FTP es que está pensado para ofrecer la máxima velocidad en la conexión, pero no la máxima seguridad, ya

que todo el intercambio de información, desde el login y password del usuario en el servidor hasta la transferencia de cualquier archivo, se realiza en texto plano sin ningún tipo de cifrado, con lo que un posible atacante puede capturar este tráfico, acceder al servidor y/o apropiarse de los archivos transferidos.

DDNS. (Dynamic Domain Name System) Es una herramienta muy útil cuando nuestra línea ADSL tiene un direccionamiento dinámico, es decir, nuestro proveedor de internet nos asigna una IP pública diferente cada vez que nos conectamos.

Si nuestra intención es configurar un servidor web, ftp, montar una VPN, etc. necesitamos tener localizado nuestro router en internet para poder tener acceso. Esto lo conseguimos mediante la función DDNS.

Dicha función permite configurar el router para asociarlo, mediante un nombre de dominio, a una dirección IP. Esto lo lleva a cabo un servidor que proporciona soporte para DNS con IP dinámica.

DHCP (**Dynamic Host Configuration Protocol** - **Protocolo de configuración dinámica de *host***) es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

- El protocolo DHCP incluye tres métodos de asignación de direcciones IP:

Asignación manual o estática: Asigna una dirección IP a una máquina determinada. Se suele utilizar cuando se quiere controlar la asignación de dirección IP a cada cliente, y evitar, también, que se conecten clientes no identificados.

Asignación automática: Asigna una dirección IP de forma permanente a una máquina cliente la primera vez que hace la solicitud al servidor DHCP y hasta que el cliente la libera. Se suele utilizar cuando el número de clientes no varía demasiado.

Asignación dinámica: el único método que permite la reutilización dinámica de las direcciones IP. El administrador de la red determina un rango de direcciones IP y cada dispositivo conectado a la red está configurado para solicitar su dirección IP al servidor cuando la tarjeta de interfaz de red se inicializa. El procedimiento usa un concepto muy simple en un intervalo de tiempo controlable.

SMTP (Simple Mail Transfer Protocol) Protocolo Simple de Transferencia de Correo, es un protocolo de la capa de aplicación. Protocolo de red basado en textos utilizados para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos (PDA's, teléfonos móviles, etc.). Está definido en el RFC 2821 y es un estándar oficial de Internet.

SMTP se basa en el modelo cliente-servidor, donde un cliente envía un mensaje a uno o varios receptores. La comunicación entre el cliente y el servidor consiste enteramente en líneas de texto compuestas por caracteres ASCII. El tamaño máximo permitido para estas líneas es de 1000 caracteres.

Las respuestas del servidor constan de un código numérico de tres dígitos, seguido de un texto explicativo. El número va dirigido a un procesado automático de la respuesta por autómata, mientras que el texto permite que un humano interprete la respuesta. En el protocolo SMTP todas las órdenes, réplicas o datos son líneas de texto, delimitadas por el carácter <CRLF>. Todas las réplicas tienen un código numérico al comienzo de la línea.

(**UDP**) **User Datagram Protocol** es un protocolo del nivel de transporte basado en el intercambio de datagramas (Encapsulado de capa 4 Modelo OSI). Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Tampoco tiene confirmación ni control de flujo, por lo que los paquetes pueden adelantarse

unos a otros; y tampoco se sabe si ha llegado correctamente, ya que no hay confirmación de entrega o recepción. Su uso principal es para protocolos como DHCP, BOOTP, DNS y demás protocolos en los que el intercambio de paquetes de la conexión/desconexión son mayores, o no son rentables con respecto a la información transmitida, así como para la transmisión de audio y vídeo en tiempo real, donde no es posible realizar retransmisiones por los estrictos requisitos de retardo que se tiene en estos casos.

TCP/IP (Protocolo de control de transmisión/Protocolo de Internet) es un conjunto de protocolos de red en los que se basa Internet y que permiten la transmisión de datos entre computadoras. En ocasiones se le denomina *conjunto de protocolos **TCP/IP***, en referencia a los dos protocolos más importantes que la componen: Protocolo de Control de Transmisión (TCP) y Protocolo de Internet (IP), que fueron dos de los primeros en definirse, y que son los más utilizados de la familia. Existen tantos protocolos en este conjunto que llegan a ser más de 100 diferentes, entre ellos se encuentra el popular HTTP (HyperText Transfer Protocol), que es el que se utiliza para acceder a las páginas web, además de otros como el ARP (Address Resolution Protocol) para la resolución de direcciones, el FTP (File Transfer Protocol) para transferencia de archivos, y el SMTP (Simple Mail Transfer Protocol) y el POP (Post Office Protocol) para correo electrónico, TELNET para acceder a equipos remotos, entre otros.

El TCP/IP es la base de Internet, y sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo PC, minicomputadoras y computadoras centrales sobre redes de área local (LAN) y área extensa (WAN).

(UPnP) Universal Plug and Play Conectar y Usar Universal, es una arquitectura software abierta y distribuida que de forma independiente al fabricante, sistema operativo, lenguaje de programación, etc. permite el intercambio de información y datos a los dispositivos conectados a una red. Según el Foro UPnP:

UPnP define protocolos y procedimientos comunes para garantizar la interoperatividad sobre PC permitidos por red, aplicaciones y dispositivos inalámbricos.

La arquitectura UPnP soporta el trabajo de una red sin configurar y automáticamente detecta cualquier dispositivo que puede ser incorporado a ésta, obtiene su dirección IP, un nombre lógico, informando a los demás de sus funciones y capacidad de procesamiento, y le informa, a su vez, de las funciones y prestaciones de los demás. Los servidores DNS y DHCP son opcionales y son usados solamente si están disponibles en la red de trabajo.

UPnP se construye sobre protocolos y formatos existentes utilizándose juntos para definir un marco que permita la definición, muestra en la red, y control de los dispositivos de ésta.

GPRS (General packet radio service) es un paquete orientado al servicio de datos móviles en el 2G y 3G de la comunicación celular del sistema de sistema global para comunicaciones móviles (GSM). GPRS fue originalmente estandarizado por el Instituto Europeo de Normas de Telecomunicación (ETSI) en respuesta a la anterior CDPD y el i-mode de conmutación de paquetes de tecnologías celulares. Ahora es mantenido por el 3rd Generación Partnership Project (3GPP).

El uso de GPRS es típicamente cobran en base a volumen de datos. Esto contrasta con conmutación de circuitos de datos, que normalmente se facturan por minuto de tiempo de conexión, independientemente de si el usuario transfiere los datos durante ese período.

5.4. Redes Inalámbricas

Las redes inalámbricas de área local se diferencian de las redes de área local tradicionales en que los terminales no están interconectados físicamente mediante un cable, sino que se utilizan ondas de radio para este fin. Esto es posible, en gran parte, a que los organismos internacionales que establecen el reparto de las frecuencias han dejado libres varias franjas para uso personal o privado. Estas frecuencias son usadas, por ejemplo, por teléfonos fijos inalámbricos, walkie-talkies etc. En cambio y en contra de lo que se piensa comúnmente, los aficionados a la radio-afición cuentan con unas frecuencias

Existe una nueva tecnología que hace uso de las frecuencias libres de licencia las redes de área local inalámbricas o redes wireless. Las LAN inalámbricas utilizan básicamente longitudes de

onda correspondientes a las microondas (2,4 GHz y 5 GHz) y permiten tener anchos de banda apreciables (desde 1 MB/s en las primeras versiones hasta llegar a los 54 MB/s de los últimos estándares). La banda alrededor de los 5 GHz es abierta, el ancho de banda que se puede ocupar depende de la situación particular que haya impuesto cada legislador. Es por ello que en Europa se pueden utilizar hasta 455 MHz, mientras que en Norteamérica el ancho de banda se restringe a 300 MHz en Japón a 100 MHz.

5.4.1. Componentes y Topologías de una Red Inalámbrica

Una red local 802.11 está basada en una arquitectura donde el sistema está dividido en células, denominadas conjunto de Servicios Básicos (BSS), y cada una de estas células está controlada por una estación.

Aunque una red wireless puede estar formada por una única célula (incluso sin utilizar un punto de acceso), normalmente se utilizan varias células, donde los puntos de accesos estarán conectados a través de un sistema de distribución (DS), generalmente Ethernet y en algunos casos sin usar cables.

La red wireless completa incluyendo las diferentes células sus puntos de acceso y sistema de distribución, puede verse en las capas superiores del modelo OSI como una red 802 clásica, y es denominada en el estándar como conjunto extendido de Servicios (ESS). La siguiente figura 2 muestra una red 802.11 clásica, con los componentes descritos previamente:

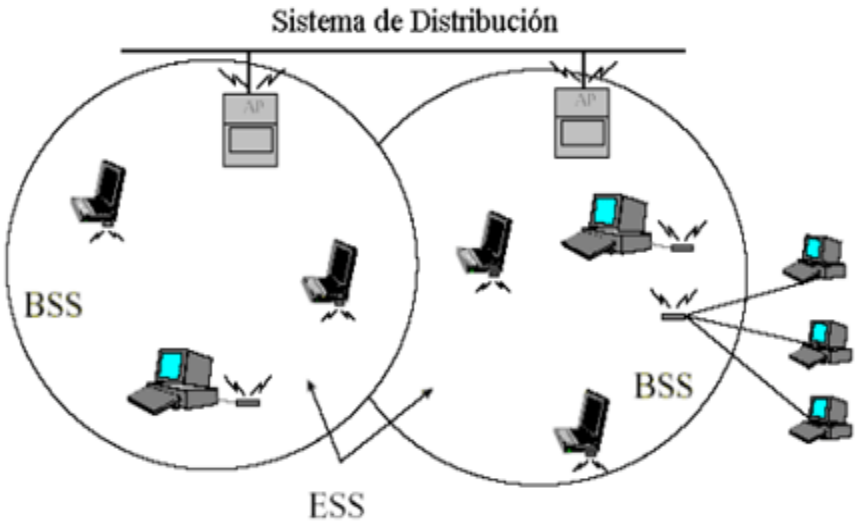


Fig. 2 muestra una red 802.11 clásica

En muchos sitios, las redes Ethernet de cable tradicional han sido ampliadas con la implantación de este tipo de redes inalámbricas. La interconexión de varias redes locales (como por ejemplo en el caso de redes inalámbricas que se extienden en todo el campus universitario) ha propiciado que algunos visionarios hayan visto la posibilidad de crear una red metropolitana con gran ancho de banda y con la posibilidad de acceso a Internet, de forma que se pudiera acceder a cualquier servicio de los que comúnmente se utilizan en Internet (correo, web, ftp, etc.) desde cualquier lugar dentro del ámbito metropolitano.

5.5. Topología

Existen dos modos diferentes de operación para los dispositivos 802.11: Ad Hoc (Juego de Servicios Independientes Básicos-Set, IBSS) o Infraestructura (Juego de Servicios Extendidos) Una red Ad Hoc es usualmente aquella que existe por un tiempo limitado entre dos o más dispositivos inalámbricos que no están conectados a través de un punto de acceso (Access Point - AP) a una red cableada. Por ejemplo, dos usuarios de laptop que deseen compartir archivos podrían poner una red ad hoc usando NICs compatibles con 802.11 y compartir archivos a través del medio inalámbrico (WM) sin la necesidad de usar medios externos(por ejemplo discos floppy, tarjetas flash).

Fig. 3 Red Ad Hoc

El modo de Infraestructura asume la presidencia de uno o más APs puenteando el medio inalámbrico al medio cableado. El AP maneja la autentificación de la estación y la asociación con la red inalámbrica. Múltiples APs conectados por un sistema de distribución (DS) puede extender el alcance de la red inalámbrica a un área mucho mayor de la que puede ser cubierta por un solo AP. En instalaciones típicas, el DS es simplemente la infraestructura de la red IP existente. Para propósitos de seguridad, LANs virtuales (VLANs) son usadas con frecuencia para segregar el tráfico inalámbrico de otro tráfico en el DS. Aunque 802.11 permite que las estaciones inalámbricas conmuten de forma dinámica la asociación de un punto de acceso a otro (tal sería el caso de un usuario de un PDA caminando a través de un campus), no gobierna como esto deberá ser logrado. Como resultado de esto, las implementaciones de los diferentes vendedores son incompatibles en este sentido

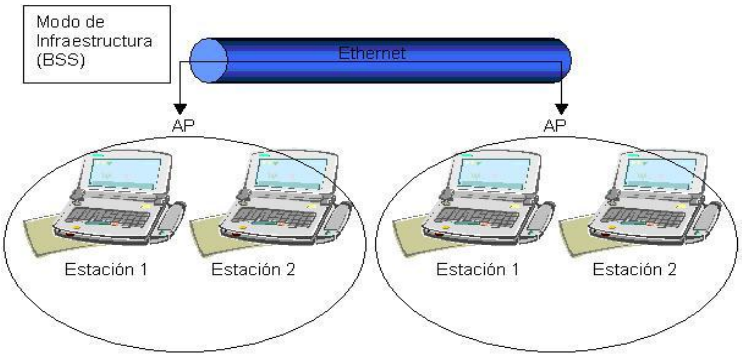


Fig. 4 Modo de infraestructura

Dentro de los Pas (actualmente ya se puede comenzar a aplicar también a los TRs) se puede modificar enormemente la capacidad de TX/RX gracias al uso de antenas especiales. Estas antenas se pueden dividir en:

- Direccionales
- Omnidireccionales

Las antenas direccionales envían la información a una cierta zona de cobertura, a un ángulo determinado, por lo cual su alcance es mayor, sin embargo fuera de la zona de cobertura no se escucha nada, no se puede establecer comunicación entre los interlocutores. Las antenas Omnidireccionales envían la información teóricamente a los 360 grados por lo que es posible establecer comunicación independientemente del punto en el que se esté En contrapartida el alcance de estas antenas es menor que el de las antenas direccionales.

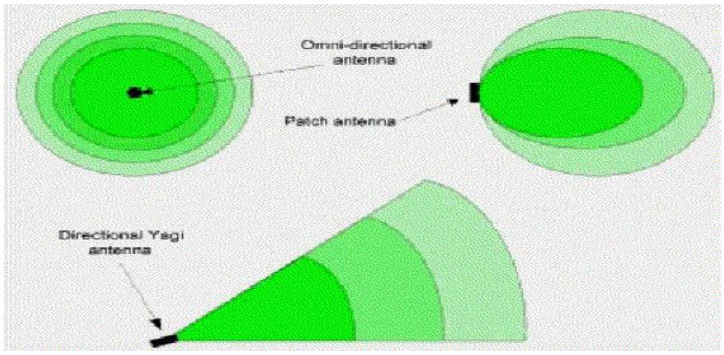


Fig. 5 TX/RX antenas

5.6. IEEE 802.11 - Wireless Networking

El protocolo IEEE 802.11 o WI-FI es un estándar de protocolo de comunicaciones de la IEEE que define el uso de los dos niveles más bajos de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN. En general, los protocolos de la rama 802.x definen la tecnología de redes de área local.

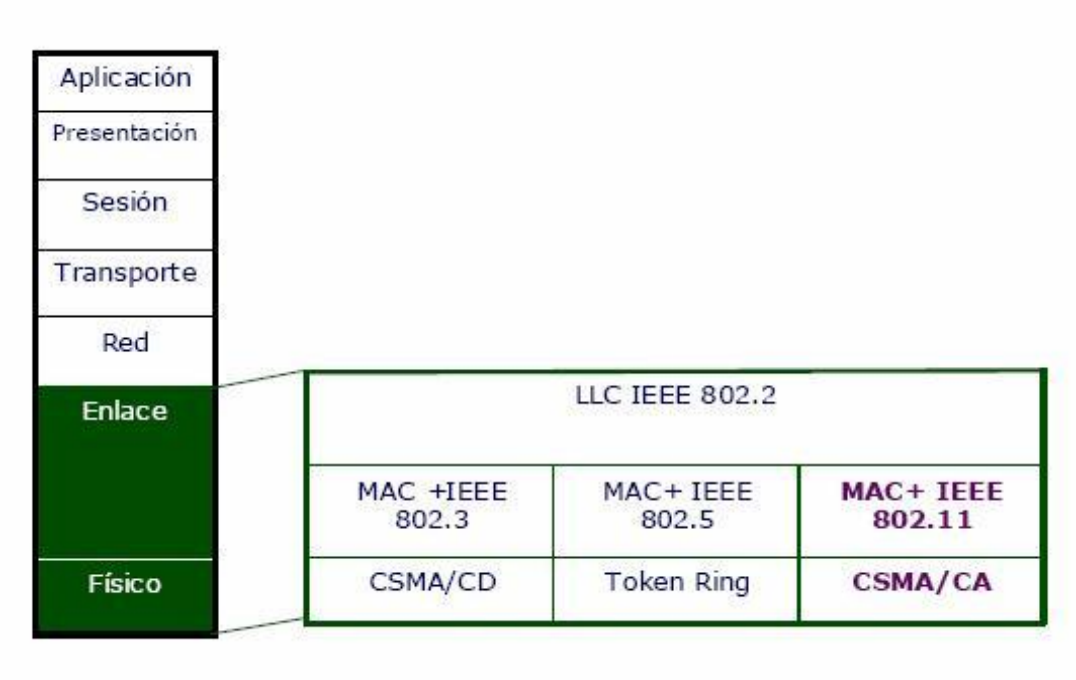


Fig.6 IEEE 802.11

La familia 802.11 actualmente incluye seis técnicas de transmisión por modulación que utilizan todos los mismos protocolos. El estándar original de este protocolo data de 1997, era el IEEE 802.11, tenía velocidades de 1 hasta 2 Mbps y trabajaba en la banda de frecuencia de 2,4 GHz En la actualidad no se fabrican productos sobre este estándar. El término IEEE 802.11 se utiliza también para referirse a este protocolo al que ahora se conoce como "802.11legacy." La siguiente modificación apareció en 1999 y es designada como IEEE 802.11b, esta especificación tenía velocidades de 5 hasta 11 Mbps, también trabajaba en la frecuencia de 2,4 GHz También se realizó una especificación sobre una frecuencia de 5 GHz que alcanzaba los 54 Mbps, era la 802.11a y resultaba incompatible con los productos de la b y por motivos técnicos casi no se desarrollaron productos. Posteriormente se incorporó un estándar a esa velocidad y compatible con el b que recibiría el nombre de 802.11g. En la actualidad la mayoría de productos son de la especificación b y de la g (Actualmente se está desarrollando la 802.11n, que se espera que alcance los 500 Mbps). La seguridad forma parte del protocolo desde el principio y fue mejorada en la revisión 802.11i. Otros estándares de esta familia (c–f, h–j, n) son mejoras de servicio y extensiones o correcciones a especificaciones anteriores. El primer

estándar de esta familia que tuvo una amplia aceptación fue el 802.11b. En 2005, la mayoría de los productos que se comercializan siguen el estándar 802.11g con compatibilidad hacia el 802.11b.

5.7. Principales Estándares 802.11

5.7.1. 802.11 Legacy

La versión original del estándar IEEE 802.11 publicada en 1997 especifica dos velocidades de transmisión de 1 y 2 Mbit/s que se transmiten por señales infrarrojas en la banda a 2,4 GHz. El estándar original también define el protocolo CSMA/CA (Múltiple acceso por detección de portadora evitando colisiones) como método de acceso. Una parte importante de la velocidad de transmisión teórica se utiliza en las necesidades de esta codificación para mejorar la calidad de la transmisión bajo condiciones ambientales diversas, lo cual se tradujo en dificultades de interoperabilidad entre equipos de diferentes marcas. Estas y otras debilidades fueron corregidas en el estándar 802.11b, que fue el primero. (CSMA/CA: Es un protocolo de control de redes utilizado para evitar colisiones entre los paquetes de datos (comúnmente en redes inalámbricas, ya que estas no cuenta con un modo práctico para transmitir y recibir simultáneamente).

5.7.2. 802.11ª

La revisión 802.11a al estándar original fue ratificada en 1999. El estándar 802.11a utiliza el mismo juego de protocolos de base que el estándar original, opera en la banda de 5 GHz y utiliza 52 subportadoras orthogonal frequency-division multiplexing (OFDM) con una velocidad máxima de 54 Mbit/s, lo que lo hace un estándar práctico para redes inalámbricas con velocidades reales de aproximadamente 20 Mbit/s. La velocidad de datos se reduce a 48, 36, 24, 18, 12, 9 o 6 Mbit/s en caso necesario. 802.11a tiene 12 canales no solapados, 8 para red inalámbrica y 4 para conexiones punto a punto.

Dado que la banda de 2.4 GHz tiene gran uso (pues es la misma banda usada por los teléfonos inalámbricos y los hornos de microondas, entre otros aparatos), el utilizar la banda de 5 GHz

representa una ventaja del estándar 802.11a, dado que se presentan menos interferencias. Sin embargo, la utilización de esta banda también tiene sus desventajas, dado que restringe el uso de los equipos 802.11a a únicamente puntos en línea de vista, con lo que se hace necesario la instalación de un mayor número de puntos de acceso; Esto significa también que los equipos que trabajan con este estándar no pueden penetrar tan lejos como los del estándar 802.11b dado que sus ondas absorbidas.

(OFDM: Es una técnica de modulación FDM que permite transmitir grandes cantidades de datos digitales sobre una onda de radio. OFDM divide la señal de radio en muchas sub-señales que son transmitidas simultáneamente hacia el receptor en diferentes frecuencias. OFDM reduce la diafonía (efecto de cruce de líneas) durante la transmisión de la señal).

5.7.3. 802.11b

La revisión 802.11b del estándar original fue ratificada en 1999. 802.11b tiene una velocidad máxima de transmisión de 11 Mbit/s y utiliza el mismo método de acceso CSMA/CA definido en el estándar original. El estándar 802.11b funciona en la banda de 2.4 GHz debido al espacio ocupado por la codificación del protocolo CSMA/CA, la velocidad máxima de transmisión es de aproximadamente 5.9 Mbit/s.

Los productos 802.11b aparecieron en el mercado muy rápido debido a que la 802.11b es una extensión directa de la técnica de modulación DSSS definida en el estándar original. Por lo tanto los chips y productos fueron fácilmente actualizados para soportar las mejoras del 802.11b. El dramático incremento en el uso del 802.11b junto con sustanciales reducciones de precios causó una rápida aceptación.

La tarjetas de 802.11b pueden operar a 11 Mbit/s pero pueden reducirse hasta 5.5, 2 o 1 Mbit/s en el caso de que la calidad de la señal se convierta en un problema. Dado que las tasas bajas de transferencia de información usan algoritmos menos complejos y más redundantes para proteger los datos son menos susceptibles a la corrupción debido a la atenuación o interferencia de la señal. Sean han hecho extensiones del protocolo 802.11b para incrementar

su velocidad a 22, 33, 44 Mbit/s pero estas no han sido ratificadas por la EEE. Estas extensiones han sido ampliamente obviadas por los desarrolladores del 802.11g I que tiene tasas de transferencia a 54 Mbit/s y es compatible con 802.11b (DSSS: Es uno de los métodos de modulación en espectro ensanchado para transmisión de señales digitales sobre ondas radiofónicas que más se utilizan).

5.7.4. 802.11g

En Junio de 2003, se ratificó un tercer estándar de modulación: 802.11g. Este utiliza la banda de 2.4 GHz (al igual que el estándar 802.11b) pero opera a una velocidad teórica máxima de 54 Mbit/s, o cerca de 24.7 Mbit/s de velocidad real de transferencia, similar a la del estándar 802.11a. Es compatible con el estándar b y utiliza las mismas frecuencias. Buena parte del proceso de diseño del estándar lo tomó el hacer compatibles los dos estándares. Sin embargo, en redes bajo el estándar g la presencia de nodos bajo el estándar b reduce significativamente la velocidad de transmisión. El mayor rango de los dispositivos 802.11g es ligeramente mayor que en los del 802.11b pero el rango que el cliente puede alcanzar 54 Mbit/s es mucho más corto que en el caso de802.11b.

Los equipos que trabajan bajo el estándar 802.11g llegaron al mercado muy rápidamente, incluso antes de su ratificación. Esto se debió en parte a que para construir equipos bajo este nuevo estándar se podían adaptar los ya diseñados para el estándar b. Muchos de los productos de banda dual 802.11a/b se convirtieron de banda dual a modo triple soportando a (a, b y g) en un solo adaptador móvil o AP. A pesar de su mayor aceptación 802.11g sufre de la misma interferencia de 802.11b en el rango ya saturado de 2.4 GHz.

5.7.5. 802.11n

En enero de 2004, la IEEE anunció la formación de un grupo de trabajo 802.11 para desarrollar una nueva revisión del estándar 802.11 la velocidad real de transmisión podría llegar a los 500 Mbps (lo que significa que las velocidades teóricas de transmisión serían aún mayores), y debería ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g, y

cerca de 40 veces más rápida que una red bajo el estándar 802.11b. También se espera que el alcance de operación de las redes sea mayor con este nuevo estándar. Existen también otras propuestas alternativas que podrán ser consideradas y se espera que el estándar que debía ser completado hacia finales de 2006, se implante hacia 2008, puesto que no es hasta principios de 2007 que no se acabe el segundo boceto. No obstante ya hay dispositivos que se han adelantado al protocolo y ofrecen de forma no oficial éste estándar con la promesa de actualizaciones para cumplir el estándar.

Protocol	Release Date	Op. Frequency	Data Rate (Typ)	Data Rate (Max)	Range (Indoor)
Legacy	1997	2.4 -2.5 GHz	1 Mbit/s	2 Mbit/s	?
802.11a	1999	5.15-5.35/5.47-5.725/5.725-5.875 GHz	25 Mbit/s	54 Mbit/s	~30 meters (~100 feet)
802.11b	1999	2.4-2.5 GHz	6.5 Mbit/s	11 Mbit/s	~30 meters (~100 feet)
802.11g	2003	2.4-2.5 GHz	25 Mbit/s	54 Mbit/s	~30 meters (~100 feet)
802.11n	2008 (projected)	2.4 GHz or 5 GHz bands	200 Mbit/s	540 Mbit/s	~50 meters (~160 ft)

Tabla 1. Comparativa entre los principales estándares IEEE 802.11

5.8. Router

Un router es un dispositivo de interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.

La estación de trabajo envía la solicitud al router más cercano, es decir, a la pasarela predeterminada de la red en la que se encuentra. Este router determinará así el siguiente equipo al que se le enviarán los datos para poder escoger la mejor ruta posible. Para hacerlo, el router cuenta con tablas de enrutamiento actualizadas, que son verdaderos mapas de los itinerarios que pueden seguirse para llegar a la dirección de destino. Existen numerosos protocolos dedicados a esta tarea.

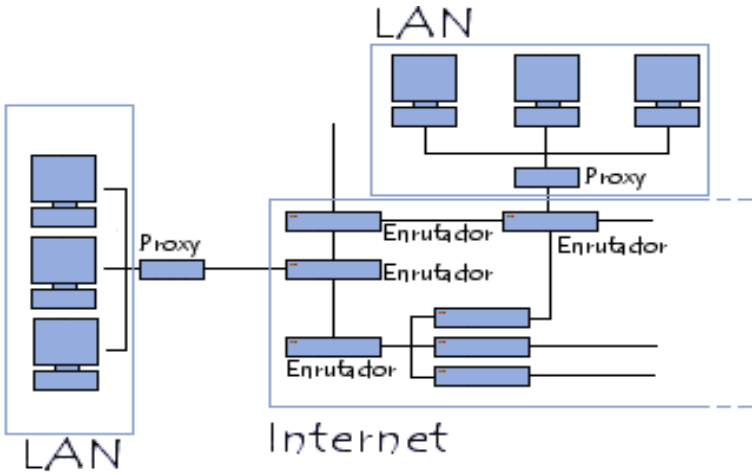


Fig. 7 Enrutamiento

Además de su función de enrutar, los routers también se utilizan para manipular los datos que circulan en forma de datagramas, para que puedan pasar de un tipo de red a otra. Como no todas las redes pueden manejar el mismo tamaño de paquetes de datos, los routers deben fragmentar los paquetes de datos para que puedan viajar libremente.

5.7.1. Diseño físico de los routers

Los primeros routers eran simplemente equipos con diversas tarjetas de red, cada una conectada a una red diferente. La mayoría de los routers actuales son hardware dedicados a la tarea de enrutamiento y que se presentan generalmente como servidores 1U.

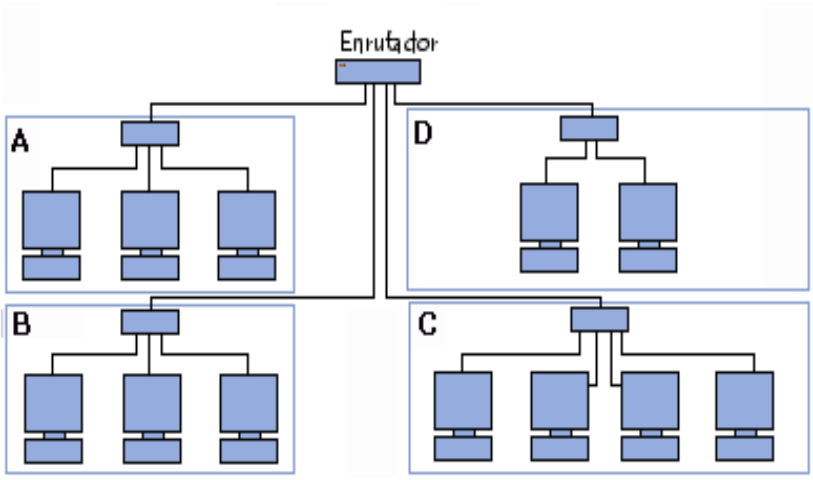


Fig. 8 Diseño físico del router

Un router cuenta con diversas interfaces de red, cada una conectada a una red diferente. Por lo tanto, posee tantas direcciones IP como redes conectadas.

5.7.2. Router inalámbrico

Un router inalámbrico comparte el mismo principio que un router tradicional. La diferencia es que aquél permite la conexión de dispositivos inalámbricos (como estaciones WiFi) a las redes a las que el router está conectado mediante conexiones por cable (generalmente Ethernet). Existen dos tipos de algoritmos de enrutamiento principales:

- Los routers del tipo vector de distancias generan una tabla de enrutamiento que calcula el "costo" de cada ruta y después envían esta tabla a los routers cercanos. Para cada solicitud de conexión el router elige la ruta menos costosa.
- Los routers del tipo estado de enlace escuchan continuamente la red para poder identificar los diferentes elementos que la rodean. Con esta información, cada router calcula la ruta más corta (en tiempo) a los routers cercanos y envía esta información en forma de paquetes de actualización.

5.8. Ups (sistema de alimentación ininterrumpida)

Un sistema de alimentación ininterrumpida, es un dispositivo que gracias a sus baterías, puede proporcionar energía eléctrica tras un apagón a todos los dispositivos que tenga conectados. Otra de las funciones de los UPS es la de mejorar la calidad de la energía eléctrica que llega a las cargas, filtrando subidas y bajadas de tensión y eliminando armónicos de la red en el caso de usar corriente alterna.

Los UPS dan energía eléctrica a equipos llamados cargas críticas, como pueden ser aparatos médicos, industriales o informáticos que, como se ha mencionado anteriormente, requieren tener siempre alimentación y que ésta sea de calidad, debido a la necesidad de estar en todo momento operativos y sin fallos (picos o caídas de tensión).

Los UPS son necesarios para el correcto funcionamiento del circuito cerrado ya que este debe trabajar continuamente para brindar una cobertura total de seguridad ya sea con la presencia y ausencia de energía eléctrica.

Los requerimientos que el UPS debe cumplir:

- El UPS debe brindar respaldo a los equipos durante la ausencia de energía eléctrica.
- El UPS debe cumplir los requerimientos de potencia de circuito cerrado de televisión con su respectiva potencia en watts o en VA.
- El UPS debe brindar protección para prevenir daños causados por transitorios y que posea alta eficiencia de conversión de la batería hacia la salida para obtener mayores rendimientos del sistema.

5.9. Servidores

En informática, un servidor es una computadora que, formando parte de una red, provee servicios a otras computadoras denominadas clientes.

También se suele denominar con la palabra servidor a:

- Una aplicación informática o programa que realiza algunas tareas en beneficio de otras aplicaciones llamadas clientes. Algunos servicios habituales son los servicios de archivos, que permiten a los usuarios almacenar y acceder a los archivos de una computadora y los servicios de aplicaciones, que realizan tareas en beneficio directo del usuario final. Este es

el significado original del término. Es posible que un ordenador cumpla simultáneamente las funciones de cliente y de servidor.

- Una computadora en la que se ejecuta un programa que realiza alguna tarea en beneficio de otras aplicaciones llamadas clientes, tanto si se trata de un ordenador central (mainframe), un miniordenador, una computadora personal, una PDA o un sistema embebido; sin embargo, hay computadoras destinadas únicamente a proveer los servicios de estos programas: estos son los servidores por antonomasia.

- Un servidor no es necesariamente una máquina de última generación de grandes proporciones, no es necesariamente un superordenador; un servidor puede ser desde una computadora vieja, hasta una máquina sumamente potente (ej.: servidores web, bases de datos grandes, etc. Procesadores especiales y hasta varios terabytes de memoria). Todo esto depende del uso que se le dé al servidor. Si usted lo desea, puede convertir al equipo desde el cual usted está leyendo esto en un servidor instalando un programa que trabaje por la red y a la que los usuarios de su red ingresen a través de un programa de servidor web como Apache.

Por lo cual podemos llegar a la conclusión de que un servidor también puede ser un proceso que entrega información o sirve a otro proceso. El modelo Cliente-servidor no necesariamente implica tener dos ordenadores, ya que un proceso cliente puede solicitar algo como una impresión a un proceso servidor en un mismo ordenador.

5.9.1. Tipos de servidores

En la siguiente lista hay algunos tipos comunes de servidores:

- **Servidor de archivo**: es el que almacena varios tipos de archivos y los distribuye a otros clientes en la red.

- **Servidor de impresiones**: controla una o más impresoras y acepta trabajos de impresión de otros clientes de la red, poniendo en cola los trabajos de impresión (aunque también puede cambiar la prioridad de las diferentes impresiones), y realizando la mayoría o todas las otras funciones que en un sitio de trabajo se realizaría para lograr una tarea de impresión si la impresora fuera conectada directamente con el puerto de impresora del sitio de trabajo. Muchas impresoras son capaces de actuar como parte de una red de ordenadores sin ningún otro dispositivo, tal como un "print server" (servidor de impresión), a actuar como intermediario entre la impresora y el dispositivo que está solicitando que se termine un trabajo de impresión.

- **Servidor de correo**: almacena, envía, recibe, enruta y realiza otras operaciones relacionadas con email para los clientes de la red.

- **Servidor de fax**: almacena, envía, recibe, enruta y realiza otras funciones necesarias para la transmisión, la recepción y la distribución apropiadas de los fax.

- **Servidor de la telefonía**: realiza funciones relacionadas con la telefonía, como es la de contestador automático, realizando las funciones de un sistema interactivo para la respuesta de la voz, almacenando los mensajes de voz, encaminando las llamadas y controlando también la red o el Internet, p. ej., la entrada excesiva de la voz sobre IP (VoIP), etc.

- **Servidor del acceso remoto (RAS)**: controla las líneas de módem de los monitores u otros canales de comunicación de la red para que las peticiones conecten con la red de una posición remota, responde llamadas telefónicas entrantes o reconoce la petición de la red y realiza la autentificación necesaria y otros procedimientos necesarios para registrar a un usuario en la red.

- **Servidor de uso**: realiza la parte lógica de la informática o del negocio de un uso del cliente, aceptando las instrucciones para que se realicen las operaciones de un sitio de trabajo y sirviendo los resultados a su vez al sitio de trabajo, mientras que el sitio de

trabajo realiza la interfaz operadora o la porción del GUI del proceso (es decir, la lógica de la presentación) que se requiere para trabajar correctamente.

- **Servidor web**: almacena documentos HTML, imágenes, archivos de texto, escrituras, y demás material Web compuesto por datos (conocidos colectivamente como contenido), y distribuye este contenido a clientes que la piden en la red.

- **Servidor de base de datos**: provee servicios de base de datos a otros programas u otras computadoras, como es definido por el modelo cliente-servidor. También puede hacer referencia a aquellas computadoras (servidores) dedicadas a ejecutar esos programas, prestando el servicio.

- **Servidor no dedicado:** son aquellos que no dedican toda su potencia a los clientes, sino también pueden jugar el rol de estaciones de trabajo al procesar solicitudes de un usuario local

5.10. Linux

Es un sistema operativo descendiente de UNIX. Unix es un sistema operativo robusto, estable, multiusuario, multitarea, multiplataforma y con gran capacidad para gestión de redes, Linux fue creado siguiendo estas características. En la década de los ochenta apareció un nuevo sistema, era una versión básica y reducida de Unix llamada Minix, su autor fue Andrew Tanenbaum, el objetivo era crear un acceso a este sistema sin tener que pagar licencias, basados en este sistema el señor Linus B. Torvalds, a mediados de 1991 empezó a trabajar en un proyecto para mejorar las deficiencias de Minix, Torvalds creó la primera versión de Linux (Contracción de Linus y Unix) numerada como versión 0.01. Esta versión solo contenía un Kernel muy rudimentario y para poder realizar cualquier operación se requería que la máquina tuviera instalado Minix. El 5 de Octubre de 1991 fue creada y publicada la versión 0.02 cuando Torvalds logro ejecutar programas como el Bash y el Gcc, después de esta publicación se distribuyó en forma gratuita el código de Linux e invito a todo aquel que pudiera aportar ideas nuevas y

mejorar el código vía Internet, gracias a estos aportes Linux evoluciono rápidamente a las versiones 0.03, 0.10, 0.11 y 0.12. En Marzo de 1992 fue creada la versión 0.95

LINUX es un sistema operativo, compatible Unix. Dos características muy peculiares lo diferencian del resto de los sistemas que podemos encontrar en el mercado, la primera, es que es libre, esto significa que no tenemos que pagar ningún tipo de licencia a ninguna casa desarrolladora de software por el uso del mismo, la segunda, es que el sistema viene acompañado del código fuente. El sistema lo forman el núcleo del sistema (kernel) más un gran número de programas / librerías que hacen posible su utilización.

LINUX se distribuye bajo la GNU Public License: por lo tanto, el código fuente tiene que estar siempre accesible.

El sistema ha sido diseñado y programado por multitud de programadores alrededor del mundo. El núcleo del sistema sigue en continuo desarrollo bajo la coordinación de Linus Torvalds, la persona de la que partió la idea de este proyecto, a principios de la década de los noventa. Día a día, más y más programas / aplicaciones están disponibles para este sistema, y la calidad de los mismos aumenta de versión a versión. La gran mayoría de los mismos vienen acompañados del código fuente y se distribuyen gratuitamente bajo los términos de licencia de la GNU Public License. En los últimos tiempos, ciertas casas de software comercial han empezado a distribuir sus productos para Linux y la presencia del mismo en empresas aumenta rápidamente por la excelente relación calidad-precio que se consigue con Linux.

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

5.10.1. Características de Linux

- Multitarea: varios programas (realmente procesos) ejecutándose al mismo tiempo.
- Multiusuario: varios usuarios en la misma máquina al mismo tiempo (y sin licencias para todos).
- Multiplataforma: corre en muchas CPUs distintas, no sólo Intel.
- Funciona en modo protegido 386.
- Tiene protección de la memoria entre procesos, de manera que uno de ellos no pueda colgar el sistema.
- Carga de ejecutables por demanda: Linux sólo lee de disco aquellas partes de un programa que están siendo usadas actualmente.
- Política de copia en escritura para la compartición de páginas entre ejecutables: esto significa que varios procesos pueden usar la misma zona de memoria para ejecutarse. Cuando alguno intenta escribir en esa memoria, la página (4Kb de memoria) se copia a otro lugar. Esta política de copia en escritura tiene dos beneficios: aumenta la velocidad y reduce el uso de memoria.
- Memoria virtual usando paginación (sin intercambio de procesos completos) a disco: una partición o un archivo en el sistema de archivos, o ambos, con la posibilidad de añadir más áreas de intercambio sobre la marcha (se sigue denominando intercambio, es en realidad un intercambio de páginas). Un total de 16 zonas de intercambio de 128Mb de tamaño máximo pueden ser usadas en un momento dado con un límite teórico de 2Gb para intercambio.
- La memoria se gestiona como un recurso unificado para los programas de usuario y para el caché de disco, de tal forma que toda la memoria libre puede ser usada para caché y éste puede a su vez ser reducido cuando se ejecuten grandes programas.
- Librerías compartidas de carga dinámica (DLL's) y librerías estáticas también, por supuesto.
- Se realizan volcados de estado (core dumps) para posibilitar los análisis post-mortem, permitiendo el uso de depuradores sobre los programas no sólo en ejecución sino también tras abortar éstos por cualquier motivo.

- Casi totalmente compatible con POSIX, System V y BSD a nivel fuente.
- Mediante un módulo de emulación de iBCS2, casi completamente compatible con SCO, SVR3 y SVR4 a nivel binario.
- Todo el código fuente está disponible, incluyendo el núcleo completo y todos los drivers, las herramientas de desarrollo y todos los programas de usuario; además todo ello se puede distribuir libremente. Hay algunos programas comerciales que están siendo ofrecidos para Linux actualmente sin código fuente, pero todo lo que ha sido gratuito sigue siendo gratuito.
- Control de tareas POSIX.
- Pseudo-terminales (pty's).
- Emulación de 387 en el núcleo, de tal forma que los programas no tengan que hacer su propia emulación matemática. Cualquier máquina que ejecute Linux parecerá dotada de coprocesador matemático. Por supuesto, si tu ordenador ya tiene una FPU (unidad de coma flotante), será usada en lugar de la emulación, pudiendo incluso compilar tu propio kernel sin la emulación matemática y conseguir un pequeño ahorro de memoria.
- Soporte para muchos teclados nacionales o adaptados y es bastante fácil añadir nuevos dinámicamente.
- Consolas virtuales múltiples: varias sesiones de login a través de la consola entre las que se puede cambiar con las combinaciones adecuadas de teclas (totalmente independiente del hardware de video). Se crean dinámicamente y puedes tener hasta 64.
- Soporte para varios sistemas de archivo comunes, incluyendo minix-1, Xenix y todos los sistemas de archivo típicos de System V, y tiene un avanzado sistema de archivos propiocon una capacidad de hasta 4 Tb y nombres de archivos de hasta 255 caracteres de longitud.
- Acceso transparente a particiones MS-DOS (o a particiones OS/2 FAT) mediante un sistema de archivos especial: no necesitas ningún comando especial para usar la partición MS-DOS, parece un sistema de archivos normal de Unix (excepto por algunas graciosas restricciones en los nombres de archivo, permisos, y esas cosas). Las particiones comprimidas de MS-DOS 6 no son accesibles en este momento, y no se espera que lo sean en el futuro. El

soporte para VFAT (WNT, Windows 95) ha sido añadido al núcleo de desarrollo y estará en la próxima versión estable.

- Un sistema de archivos especial llamado UMSDOS que permite que Linux sea instalado en un sistema de archivos DOS.
- Soporte en sólo lectura de HPFS-2 del OS/2 2.1
- Sistema de archivos de CD-ROM que lee todos los formatos estándar de CD-ROM.
- TCP/IP, incluyendo ftp, telnet, NFS, etc.
- Appletalk disponible en el actual núcleo de desarrollo.
- Software cliente y servidor Netware disponible en los núcleos de desarrollo

5.10. Debian

Debían o Proyecto Debían es una comunidad conformada por desarrolladores y usuarios, que mantiene un sistema operativo GNU basado en software libre. El sistema se encuentra pre compilado, empaquetado y en un formato deb para múltiples arquitecturas de computador y para varios núcleos

Nació como una apuesta por separar en sus versiones el software libre del software no libre. El modelo de desarrollo del proyecto es ajeno a motivos empresariales o comerciales, siendo llevado adelante por los propios usuarios, aunque cuenta con el apoyo de varias empresas en forma de infraestructuras. Debían no vende directamente su software, lo pone a disposición de cualquiera en Internet, aunque sí permite a personas o empresas distribuirlo comercialmente mientras se respete su licencia, La comunidad de desarrolladores del proyecto cuenta con la representación de Software in the Public Interest, una organización sin ánimo de lucro que da cobertura legal a varios proyectos de software libre.

La primera adaptación del *sistema Debían*, siendo también la más desarrollada, es Debían GNU/Linux, basada en el núcleo Linux, y como siempre utilizando herramientas de GNU

5.11. ZoneMinder

ZoneMinder es un conjunto integrado de aplicaciones que proporcionan una solución completa de vigilancia que permite la captura, análisis, registro y monitoreo de cualquier circuito cerrado de televisión o cámaras de seguridad conectado a una máquina basada en Linux. Está diseñado para funcionar en distribuciones que apoyan el vídeo para Linux (V4L) y la interfaz ha sido probado con cámaras de video para tarjetas de BTTV, varias cámaras USB y también es compatible con la mayoría de las cámaras de red IP. ZoneMinder también requiere MySQL y PHP, y se ve reforzada por un servidor web como Apache.

Zoneminder es una aplicación Open Source que permite adicionar varias cámaras de video, pudiendo así ver un circuito cerrado de televisión CCTV o apenas una simple cámara para vigilar a los animales domésticos.

Esta aplicación posee además un sistema de detección de movimiento con grabación de imágenes, pudiendo así mejorar la seguridad de diversas instalaciones.

ZoneMinder está compuesto por varios componentes que hace posible la captura de imagen real y el análisis, es sencillo interfaz web que le permite controlar tanto la situación actual y ver y organizar eventos históricos que han tenido lugar. La interfaz web le permite comprobar y controlar su instalación ZoneMinder de otros ordenadores en su casa o desde cualquier parte del mundo. ZoneMinder no requiere en absoluto la interfaz web para las funciones del día a día. También hay una interfaz simple que permite HTML de básico monitoreo asimismo permite pausar, rebobinar e incluso Zoom digital tanto de video en vivo e histórico.

5.11.1. Características del software ZoneMinder

A continuación se describe un conjunto de características específicas del software ZoneMinder.Trabaja sobre cualquier distribución de Linux que soporte la interfaz “Video para Linux”.

- Soporta cámaras de video, cámaras USB y cámaras IP.
- Soporta cámaras PTZ (*Pan Tilt Zoom*).
- Construido sobre las herramientas estándar C++, PERL y PHP.
- Usa bases de datos basados en MySQL.
- Múltiples Zonas (Regiones de Interés) pueden ser definidas por cada cámara; cada una puede trabajar con diferente sensibilidad.

Gran número de opciones de configuración, que permiten el máximo rendimiento en cualquier hardware, Interfaz web amigable para el usuario.
Soporta cámaras que trabajan con diferentes compresiones de video, tales como MJPEG, MPEG4, H.264 entre otras, Filtros definidos por el usuario que permiten la selección de cualquier número de eventos, por combinación de características en cualquier orden.
Notificación de eventos por correo electrónico, SMS o por teléfono analógico, celular o IP. Carga automática de eventos a un servidor de almacenamiento FTP (*File Transfer Protocol – Protocolo de Transferencia de Archivos*).

Incluye X.10 bi-direccional permitiendo la integración de señales de control X.10 cuando el video es capturado así como para disparar dispositivos X.10 cuando exista detección de movimiento, Múltiples usuarios y niveles de acceso, Soporte multilenguaje.

Soporte de activación externa de dispositivos y aplicaciones desarrollados por terceros.
Acceso por teléfono celular xHTML (*eXtensible Hypertext Markup Language – Lenguaje. Extensible de Marcado de Hipertexto*) permitiendo el acceso a funciones comunes.

5.11.2. Requerimientos del software ZoneMinder.

5.11.2.1. **Requerimientos en software.**

ZoneMinder necesita de varios requisitos en software detallados a continuación.

Sistema Operativo Linux que soporte la interfaz “Video para Linux”.

Sistema de gestión de base de datos MySQL.

Librerías libjpeg (Librerías JPEG).

FFmpeg.

Librerías PHP.

Compilador PERL.

Módulos de PERL.

Aplicación Java Cambazola (Aplicación para Internet Explorer).

Servidor web APACHE.

5.11.2.2. **Requerimientos en hardware.**

ZoneMinder es un software que trata de consumir la menor cantidad de recursos posibles gracias a la cooperación directa con los demonios del sistema, por lo que sus requerimientos en hardware son relativamente bajos comparados a sus alternativas pagadas; a continuación se presenta un conjunto de requerimientos en hardware.

VI. Desarrollo

a. Estudio de factibilidad

6.1.1. Requerimientos funcionales

- Monitorear el área interna y externa en el área de Tesorería de la UNAN-Managua
- Brindar el servicio de vigilancia las 24 horas
- Garantizar el acceso remoto y seguro al mismo a través de la red
- Registrar eventos en específico en el área de Tesorería de la UNAN-Managua
- Envíos de notificación por medio de correo electrónico

6.1.2. Requerimientos no funcionales

- Notificaciones SMS
- Implementación de una vlan para vigilancias
- Sistemas de alarmas integrados al sistema de vigilancia

b. Alternativas

1. Sistemas de vigilancias CCTV y desarrollo de software para su administración, adaptado a los requerimientos
2. Sistema de vigilancias remoto a través de un servidor web open soucer (debían, Apache, Zoneminder) y cámaras IP

c. Requerimientos técnicos

Alternativa 1

1. sistema de vigilancia CCTV
2. servidor
   a. Procesador Pentium IV 3GHz o superior
   b. 3GB de memoria RAM o superior
   c. Interfaz de red de 1000 Mb/s
   d. Disco Duro de 500 GB o superior

3. Equipos clientes del sistema
    a. Procesador Pentium II 3GHz o superior
    b. 1GB de memoria RAM o superior
    c. Interfaz de red de 100 Mb/s
    d. Disco Duro de 80 GB o superior
    e. Sistema operativo Windows server

Alternativa 2

1. Cámaras IP
2. Servidor
    a. Procesador Pentium IV 3GHz o superior
    b. 3GB de memoria RAM o superior
    c. Interfaz de red de 1000 Mb/s
    d. Disco Duro de 500 GB o superior
    e. Sistema operativo Linux Debían
3. Equipos clientes del sistema
    a. procesador Pentium IV 3GHz o superior
    b. 1GB de memoria RAM o superior
    c. Interfaz de red de 100 Mb/s
    d. Disco Duro de 80 GB o superior

d. Factibilidad técnica

Actualmente la UNAN-Managua no cuenta con equipos de hardware ni cámaras IP necesaria para llevar a cabo el funcionamiento del proyecto, también es necesario utilizar una máquina que será el servidor para el monitoreo del área de Tesorería de la UNAN-Managua, el centro cuenta con las instalaciones físicas adecuadas para la ubicación y distribución de los equipos

Alternativa 1

Equipo	Características	Estado
Solución CCTV	6 cámaras de vigilancia tipo domo, cables, conectores, alimentadores	No presente
Monitor adicional CCTV	Marca: vi.com	No presente

Tabla 2. Factibilidad técnica CCTV

Alternativa 2

Equipo	Características	Estado
Servidor de Vigilancia	• Procesador Pentium IV 3GHz o superior • 3GB de memoria RAM o superior • Interfaz de red de 1000 Mb/s • Disco Duro de 500 GB o superior • Sistema operativo Linux Debían	Presente en la institución
Equipos clientes del sistema	• procesador Pentium II 3GHz o superior • 1GB de memoria RAM o superior • Interfaz de red de 100 Mb/s • Disco Duro de 80 GB o superior	Presente en la institución
Cámaras IP	Cámaras de video con conectividad a intranet	No presente en la institución
Infraestructura de red	Cableado estructurado, Smith, Router, etc.	Presente en la Institución

Tabla 3. Factibilidad técnica cámaras IP

e. Factibilidad económica

Costos de equipos a adquirir

Alternativa 1		Alternativa 2	
Solución ctv.	$800,00	6 Cámaras IP	$780,00
Monitor adicional CCTV	$200,00		
Total	**$1.000,00**	**Total**	**$780,00**

Tabla 4. Factibilidad económica

*Esto incluye los equipos que no están presentes en la institución y deben adquirirse (ver Factibilidad técnica)

Costo de instalación

Alternativa 1	**$300,00**	**Alternativa 2**	**$200,00**

Tabla 5. Costo de instalación

Costo totales:

Alternativa 1		**Alternativa 2**	
Costos de equipos	$1.000,00	Costos de equipos	$780,00
Costos de instalación	$300,00	Costos de instalación	$200,00
Total	**$1.300,00**	**Total**	**$980,00**

Tabla 6. Costos totales

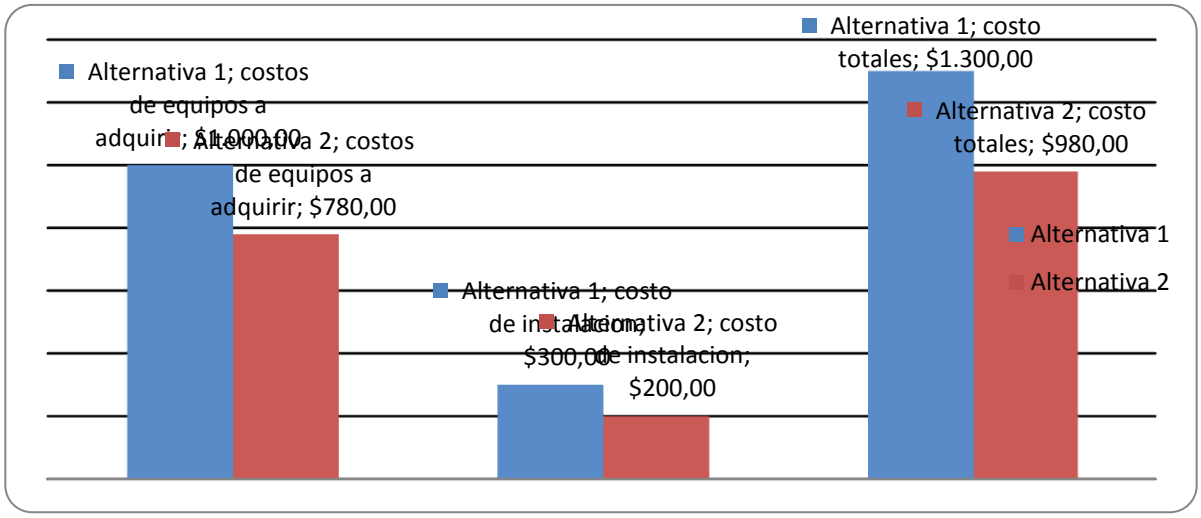


Fig 9 grafica comparativa

Conclusión: la alternativa 2 resulta ser más factible que la alternativa 1, por tener $ 320 menos en sus costos.

f. Factibilidad operativa

En base de una entrevista (A) al señor José Santos Martínez Jefe de Seguridad de la UNAN-Managua. Se conoció que todos los CPF cuentan con conocimientos de informática suficientes para utilizar las herramientas ofrecidas en la alternativa 2 de vigilancia (sitio web de vigilancias). Ninguno de los posibles operadores del sistema de vigilancia ha tenido experiencia con sistema de vigilancia CCTV

Tanto en la alternativa 1 como en la alternativa 2 se cumplen los siguientes requerimientos funcionales:

- Monitorear el área interna y externa en el área de Tesorería de la UNAN-Managua
- Garantizar el acceso remoto y seguro al mismo a través de la red
- Registrar eventos en específico en el área de tesorería
- Envíos de notificación por medio de correo electrónico

6.2. Cantidad de cámaras necesarias

Se obtuve mediante el algoritmo "guardas de museo" que la cantidad de cámaras necesarias para el polígono descrito por el área de Tesorería de la UNAN-Managua es de 6 cámara en el área interna y una en el área externa como mínimo.

6.2.1 Posicionamiento de cámaras de vigilancia

Para realizar el posicionamiento de las cámaras de seguridad y encontrar los puntos exactos donde se pueda obtener mayor visibilidad, conservar la estética y que cubran todos los sitios importantes que deben ser vigilados dentro del área donde se va implementar el proyecto, que en este caso es en el área de Tesorería de la UNAN-Managua (véase la fig.5), se realizó por medio del algoritmo de la galería de arte.

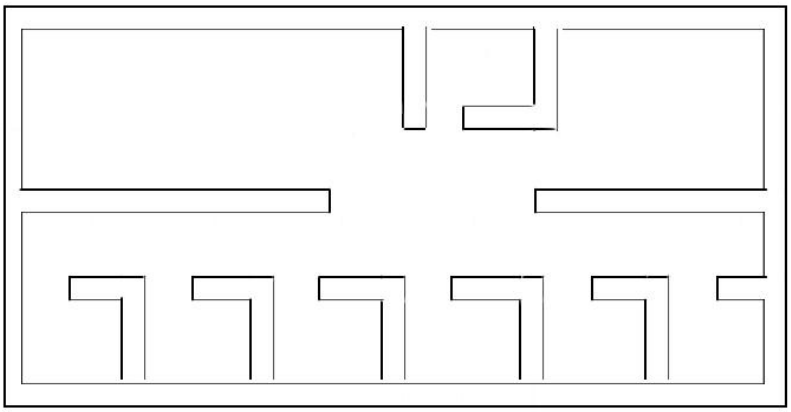


Fig.10 Área de Tesorería de la UNAN-Managua

Dicho algoritmo no indica el número de cámaras de seguridad necesarias para vigilar toda el área de Tesorería del recinto UNAN-Managua, estará delimitada por el número de "**n"** vértices del polígono, n/3 cámaras colocadas en determinadas vértices del polígono, que serán suficientes y necesarias para vigilar el interior de polígono simple de "**n**" lados.

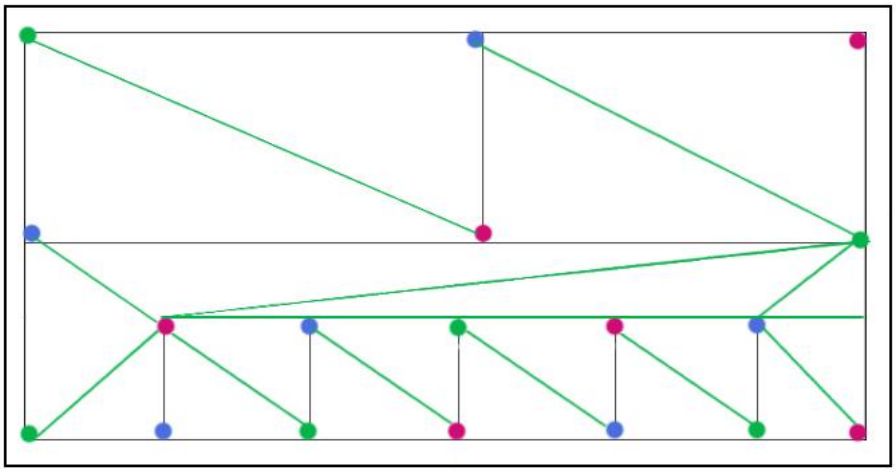


Fig. 11 Triangulación del algoritmo

La demostración se realiza en pocos pasos:

1. Triangular el polígono con sus diagonales.

2. Mostrar que para dicha triangulación, sus vértices pueden colorearse con sólo tres colores, de modo que cada triángulo tenga todos los colores.

3. Escoger los vértices del polígono con el color menos frecuente

Cada punto indica posibles lugares de donde colocar las cámaras de vigilancia, en este caso el número de puntos es el mismo para cada color se toma cualquier color (véase en la fig. 10)

Al realizar el cálculo, éste no refleja que el número de cámaras esta dado en seis, se toman los puntos en los que se visualicen o se tenga mayor ángulo de vigilancia para este caso se toman los puntos de color rojo ya que estos poseen mayor visualización de vigilancia (véase en la fig.11)

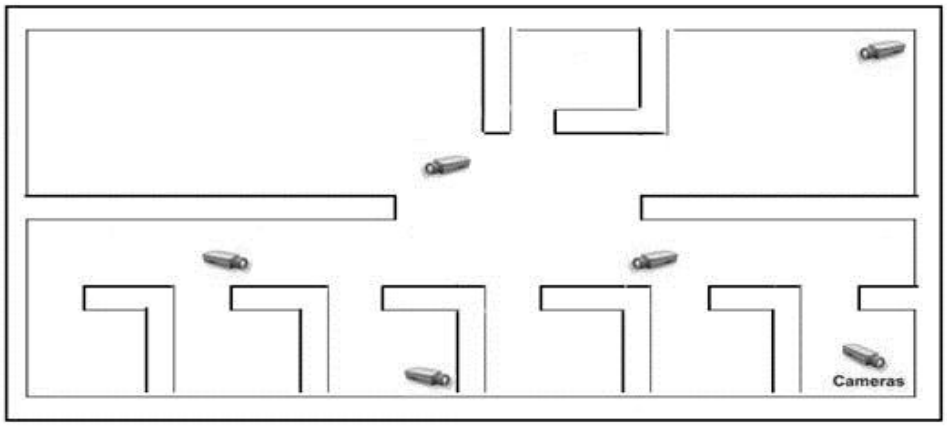


Fig. 12 Posicionamiento de las cámaras de vigilancia

A como se muestra en la figura estos son los posibles lugares que pueden estar ubicadas las cámaras IP para la vigilancia.

7.1. Desarrollo de topología necesaria

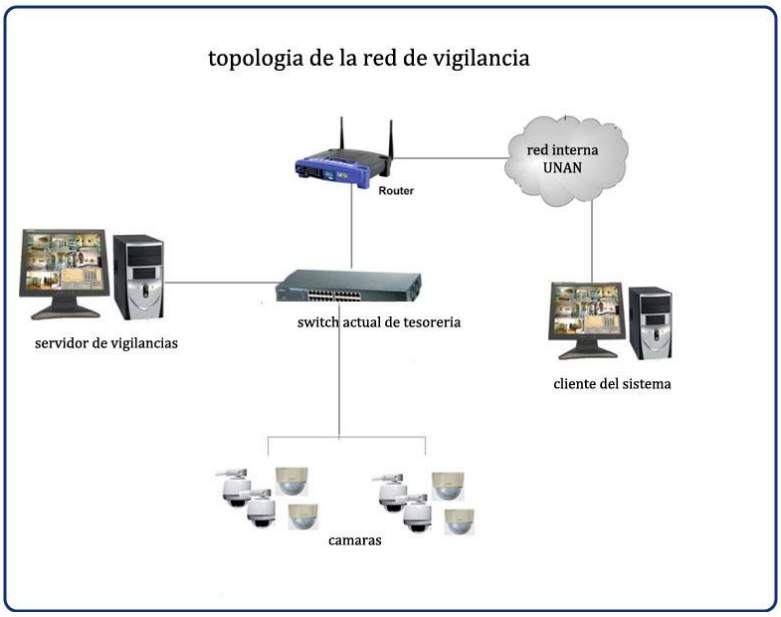


Fig. 13 Topología de la red de vigilancia

La topología de la red de vigilancia se especifica como la cadena de comunicación usada por los nodos que conforman la red para comunicarse. Un ejemplo claro de esto es la topología que se muestra en la fig. 9 la cual nos indica cómo estará distribuida la red de vigilancia en la área de Tesorería de la UNAN-Managua, en este caso la red debe estar de esta forma: las cámaras grabarían los eventos ocurridos, luego estos datos son enviados por medio del switch al servidor de vigilancia, este a su vez envía los datos al switch por otra línea hacia un router que está conectado a la red interna de la UNAN-Managua y este envía la información a los hosts (estaciones de trabajo) o clientes del sistema, el resultado de esto es una red con apariencia de árbol porque desde el switch que se tiene se ramifica la distribución de la información captadas por las cámaras dando lugar a la creación de una nueva subred interna .

8.1. Configuración de servidor en ambiente de prueba

7.1.1. Configuración de parámetros del S.O.

Para poder configurar la tarjeta de red de un servidor se tiene que utilizar la configuración de IP estática:

```
Auto eth1
iface eth1 inet static

    Address 10.x.x.x
    netmask 255.x.x.x
Network 10.x.x.x
    Broadcast 10.x.x.x
    Gateway 10.x.x.x
Dns-nameservers 8.8.8.8
```

Como se puede observar posee la misma estructura, en este caso utilizamos la interfaz eth1, la cual se configura para que se levante con el sistema (**auto eth1**) y pasar a definir mediante iface todos los parámetros de red, que en este caso comprenden la IP asignada a la interfaz (10.x.x.x), su máscara de red (255.x.x.x), la red en la que se encuentra (10.x.x.x), la IP asignada para Broadcast en la red (10.x.x.x), la puerta de enlace o router (10.x.x.x) y los servidores DNS (8.8.8.8).

- **El fichero /etc/network/interfaces**

Fichero de configuración /etc/network/interfaces. Dicho fichero para la configuración equivalente a :

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
        address 10.x.x.x
       netmask 255.x.x.x
gateway 10.x.x.x
```

- **Configuración del DNS**

Modifica el archivo /etc/resolv.conf o puede crearse, si no existe, con la siguiente información:

```
### Comentarios varios
```

domain inf-cr.uclm.es
nameserver 10.x.x.x

nameserver 10.x.x.x

para acceder a una máquina por medio de un nombre que no está en el DNS, se puede editar el archivo /etc/hosts e incluir en él una línea del tipo:

10.x.x.x arco.inf-cr.uclm.es arco

8.1. Instalación de sistema de monitoreo

ZoneMinder es un sistema de vigilancia de vídeo completo y de distribución gratuita para plataforma Linux. Es un sistema de detección de movimientos lo cual permite reducir la cantidad de datos de vídeo que deben enviarse por la red, ya que el envío de información solo se produce cuando se detecta un cambio en el patrón de la escena que pudiese significar una alteración en la seguridad de la zona que se está monitoreando.

ZoneMinder está basado completamente en Web lo cual permite administrar y monitorear todos los sistemas de seguridad que se implementen mediante este sistema ya sea por la intranet corporativa o incluso desde internet.

Linux origina que se deban realizar ciertas modificaciones antes de realizar los pasos descritos en la documentación del software para una correcta instalación

- Instalación del dispositivo de captura de video.

Antes de realizar la instalación de Zoneminder es necesario realizar la instalación de nuestros dispositivos de captura de video y asegurarnos que estos funcionen ya que no es posible iniciar el dominio de ZoneMinder sin tener la cámara reconocida

En anexo se encuentra los pasos para la instalación del sistema o programa de monitoreo

9.1. Calculo del ancho de banda (BW)

El ancho de banda aproximado y necesario para una cámara IP depende de varios parámetros tal y como se indica en la figura 10.

Fig. 14 Parámetros para el cálculo del ancho de banda

Para determinar el ancho de banda según los parámetros necesitamos saber las características de la cámara FOSCAM FI8909W.

Sensor de imagen	Sensor	1/4" Sensor CMOS a color
	Resolución	640 x 480 Pixels (300k Pixels)
	Iluminación	0.5 Lux mínimo
	Controles	Control de brillo, contraste y frecuencia de luz. Automáticos y manuales
Lentes	lentes	Cristal; Lentes IR-infrarrojas de visión nocturna; rosca estándar S-Mount para intercambio de objetivos f: 3.6 mm, 67º ángulo de visión
Audio	Entrada	Micrófono incorporado
	Salida	Altavoz incorporado
	Compresión audio	ADPCM
Video	Compresión vídeo	MJPEG
	Imágenes/seg.	15 fps (VGA), 30 fps (QVGA)
	Resolución	• 640 x 480 (VGA), 320 x 240 (QVGA)
	Volteo imagen	Vertical / Horizontal
	Frecuencia luz	50Hz, 60Hz o Exterior

	Ajustes vídeo	Brillo, Contraste
Comunicación	Red Ethernet	10/100 Mbps RJ-45
	Protocolos	HTTP, FTP, TCP/IP, UDP, SMTP, DHCP, PPPoE, DDNS, UPnP, GPRS
	WiFi	IEEE 802.11b/g
	Velocidad datos	802.11b: 11Mbps (Max.), 802.11g: 54Mbps (Max.)
	Seguridad WiFi	Encriptación WEP, WPA, WPA2
Datos físicos	Luz infrarroja	11 IR LEDs, Alcance nocturno hasta 8 m
	Dimensiones	En mm.: 110 (La) x 100 (An) x 108 (Al)
	Peso	418 gr (accesorios incluidos)
Alimentación	Alimentación	Adaptador DC 5V/2.0A
	Consumo	5 W máximo
Entorno	Temperatura	0° ~ 55°C (operativa) -10°C ~ 60°(almacenamiento)
	Humedad	20% ~ 85% sin condensación (operativa) 0% ~ 90% sin condensación (almacenamiento)

Tabla 7. Especificaciones técnicas de la cámara IP FOSCAM FI8909W

9.1.1. Sobrecarga generada por el encapsulamiento de datos

Debido a que este proyecto se enfoca en las comunicaciones inalámbricas, se escoge el estándar IEEE 802.11g para él envió de los datos de información.

IEEE 802.11g este estándar ofrece velocidades de 54 Mbps en la banda de 2.4 GHZ asegurando la compatibilidad con los equipos WI-FI preexistentes de 11 Mbps, posee los siguientes elementos obligatorios opcionales:

El método OFDM (Multiplicación por división de frecuencias ortogonales) es obligatorio y permite alcanzar altas velocidades en la banda de 2.4 GHZ.

Los sistemas deben de ser totalmente compatibles con el IEEE 802.11g.

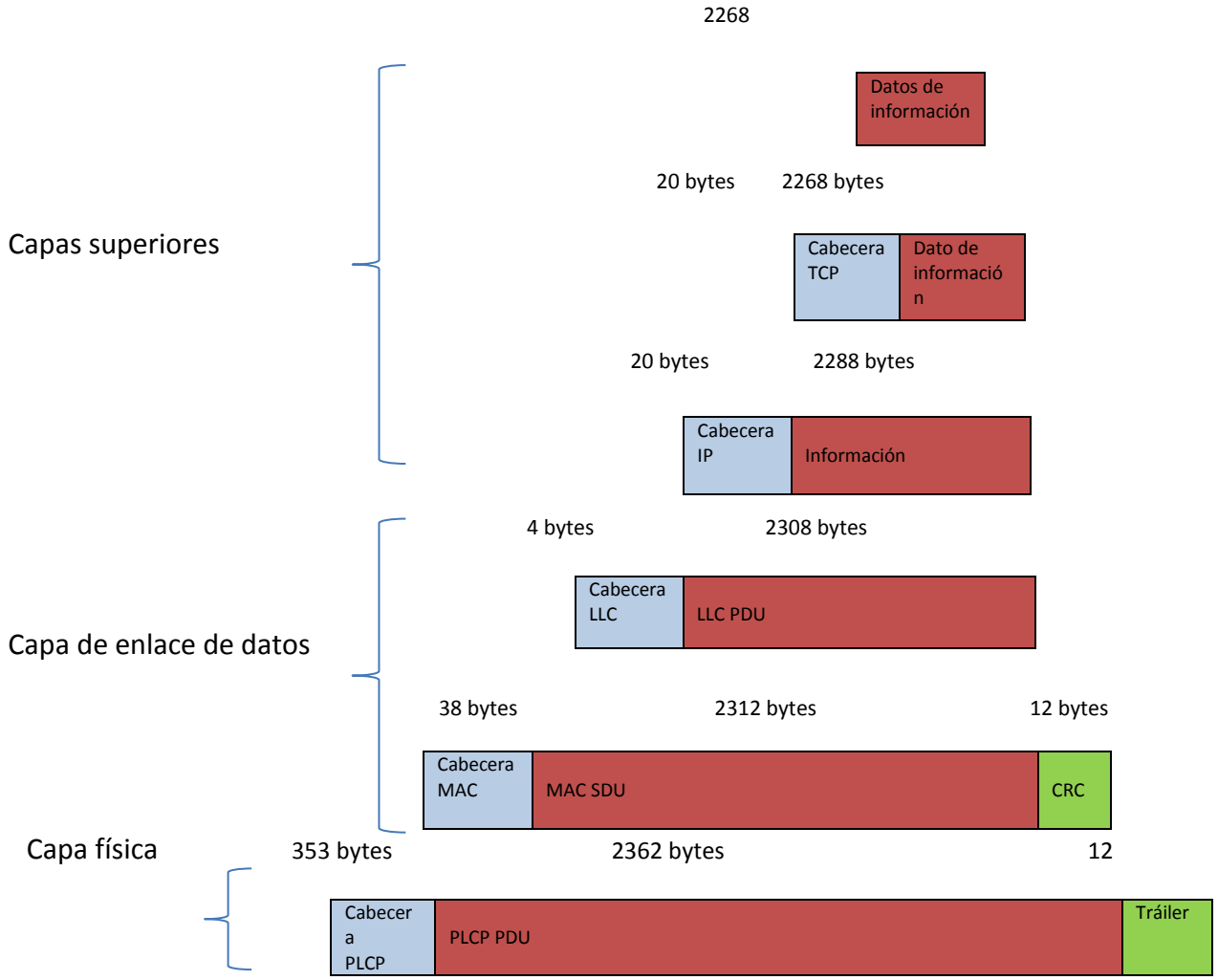


Fig. 15 Proceso de encapsulamiento de datos de información

Se observa que los datos de información tienen un valor máximo de 2268 bytes o 18144 bits es decir por cada trama 802.11g enviada únicamente 18144 bits corresponden a información, estos datos se encapsulan capa por capa convirtiéndose en la PDU de la capa anterior hasta llegar a la capa física, para luego ser enviados por el medio de transmisión.

En la capa física al sumar la cabecera PLCP, PLCP PDU y el tráiler se obtiene 21732 bits, este valor es el total de datos que se envían por el medio físico.

9.1.2. Calculando sobrecarga por encapsulamiento

Sobrecarga por encapsulamiento= Bits totales - Bits de información

Sobrecarga por encapsulamiento= 21732 bits – 18144 bits

Sobrecarga por encapsulamiento= 3588 bits

Se establece que en cada proceso de encapsulamiento se genera 3588 bits o 448.5 bytes estos datos no corresponden a bits de información por lo que esta sobrecarga genera un incremento en el ancho de banda.

Siguiendo el orden de los parámetros necesarios para calcular el ancho de banda aproximado de la cámara IP FOSCAM FI8909W según sus características:

9.1.3. Resolución y método de compresión parámetros MJPEG

Los parámetros de resolución y de compresión de video permiten obtener un nuevo parámetro llamando tamaño de cuadro el cual es medido en kilobytes.

Se indican los valores de tamaño del cuadro según las características de la cámara FOSCAM FI8909W en función de la resolución y de la compresión MJPEG

COMPRESION DE VIDEO

RESOLUCION	MJPEG-1O	MJPEG-20	MJPEG-30	MJPEG-40	MJPEG-50	MJPEG-90
320x340(QVGA)	12 KB	9KB	8KB	7KB	6KB	4KB
352x240(CIF NTSC)	13 KB	10KB	9KB	8KB	7KB	4KB
352X288 (CIF PAL)	15 KB	12KB	11KB	9KB	8KB	5KB
480X360	26 KB	21KB	18KB	16KB	14KB	9KB
640X480 (VGA)	46 KB	38KB	32KB	28KB	25KB	16KB
704X240(2CIF NTSC)	26 KB	21KB	18KB	16KB	14KB	9KB
704X288(2 CIF PAL)	31 KB	25KB	21KB	19KB	17KB	10KB
704X480(4 CIF NTSC)	51 KB	41KB	36KB	31KB	28KB	17KB
704X576(4 CIF PAL)	61KB	50KB	43KB	38KB	33KB	21KB
800X600(SVGA)	73KB	59KB	50KB	44KB	40KB	24KB
1280X720(HD)	139KB	113KB	97KB	85KB	76KB	47KB
1280X960(1.22MP)	186KB	150KB	129KB	114KB	101KB	62KB

Tabla 8. Compresión de video MJPEG

9.1.4. **Cálculo aproximado de ancho de banda usando la cámara IP FOSCAM FI8909W**

Se obtiene las condiciones con las que se genere mayor ancho de banda.

Estas condiciones son:

Resolución máxima= 640x480 (VGA)

Número máximo de cuadros por segundo= 15

El tamaño del cuadro se obtiene de la tabla con una compresión de video MJPEG -10 y una resolución de 640x480 (VGA) = 46 Kbytes

Con estos valores se puede determinar el número aproximado de tramas del IEEE 802.11g que se necesita para transmitir un cuadro completo, la siguiente operación matemática consiste en efectuar una división entre el tamaño de un cuadro y la cantidad de datos de información antes del proceso de encapsulamiento.

$$\#\ \text{De tramas} = \frac{\text{Tamaño de un cuadro [KBytes]}}{\text{Datos de información antes del proceso de encapsulamiento [Bytes]}}.$$

$$\#\ \text{De tramas} = \frac{46\ \text{KBytes}}{2268\ \text{Bytes}} \times \frac{1024\ \text{Bytes}}{1\ \text{KBytes}} = 20.77\ \text{Tramas}$$

De tramas= 21 Tramas

Ahora se calcula aproximadamente la sobrecarga total, la misma que es igual al producto entre el número de tramas y la sobrecarga generada por encapsulamiento.

Sobrecarga total = 21 Tramas x 448.5 Bytes

$$\text{Sobrecarga total} = 9418.5\ \text{Bytes} \times \frac{1\ \text{Kbyte}}{1024\ \text{Byte}} = 9.19\ \text{Kbyte}$$

Sobrecarga total = 9.19 Kbyte

Ahora se procede a calcular el tamaño real aproximado de un cuadro transmitido, empleado en el estándar 802.11g

Tamaño real de un cuadro [Bytes] = 46 Kbytes + 9.19 Kbytes = 55.2 Kbytes

Tamaño real de un cuadro en [Bits] = 55.2 Kbytes x 8 bits = 441.58 Kbits

Ahora se obtiene el ancho de banda aproximado que consume una cámara IP, para encontrar este valor se realiza el producto entre el tamaño real de un cuadro y el número de cuadros enviados en un segundo

$$\text{Ancho de banda Mbps} = 441.58\ \frac{\text{kbits}}{\text{Cuadro}} \times 15\ \frac{\text{cuadros}}{\text{segundos}} \times \frac{1\ \text{Mbit}}{1024\ \text{Kbits}} = 6.47\ \text{Mbps}$$

6.47 Mbps consume de ancho de banda una cámara IP, con una resolución máxima de 640x480 (VGA) a 15 fps (cuadros por segundo), bajo el estándar 802.11g una cámara FOSCM FI8909W es la condición en que se genera mayor ancho de banda de consumo.

La cámara FOSCAM FI8909W trabaja con resoluciones 640x480 (VGA) y 320X240 (QVGA), hasta el momento se calculó el valor máximo aproximado del ancho de banda con la resolución más alta y en las peores condiciones para que exista un mayor consumo, por lo que es conveniente calcular con la resolución más baja, a fin de tener una idea cuantitativa entre una resolución y otra.

Se procede a calcular el ancho de banda aproximado con una resolución de 320x240 (QVGA) con una compresión MJPEG-90 estas serían las condiciones para que se dé el mínimo consumo de ancho de banda.

Resolución mínima = 320x240 (QVGA)
Numero de cuadros por segundo = 15
El tamaño del cuadro se obtiene de la tabla con una compresión de video MJPEG -90 y una resolución de 320x240 (QVGA) = 4 Kbytes

Con estas condiciones se procede determinar el número aproximado de tramas del IEEE 802.11g que se necesita para transmitir un cuadro completo.

$$\#\ \text{De tramas} = \frac{\text{Tamaño de un cuadro [KBytes]}}{\text{Datos de información antes del proceso de encapsulamiento [Bytes]}}.$$

$$\#\ \text{De tramas} = \frac{4\ \text{KBytes}}{2268\ \text{Bytes}} \times \frac{1024\ \text{Bytes}}{1\ \text{KBytes}} = 1.80\ \text{Tramas}$$

De tramas= 2 Tramas

Ahora se procede a calcular un aproximado de la sobrecarga total.

Sobrecarga total = 2 Tramas x 448.5 Bytes= 897 bytes

$$\text{Sobrecarga total} = 897 \text{ Bytes} \times \frac{1 \text{ Kbyte}}{1024 \text{ Byte}} = 0.87 \text{ Kbyte}$$

Ahora se procede a calcular el tamaño real aproximado de un cuadro transmitido, empleado en el estándar 802.11g.

Tamaño real de un cuadro [Bytes] = 4 Kbytes + 0.87 Kbytes = 4.87 Kbytes

Tamaño real de un cuadro en [Bits] = 4.87 Kbytes x 8 bits = 39 Kbits

Ahora se obtiene el ancho de banda aproximado que consume una cámara IP FOSCAM FI8909W con las condiciones para el mínimo consumo de ancho de banda

$$\text{Ancho de banda Mbps} = \frac{39 \text{ kbits}}{\text{Cuadro}} \times \frac{15 \text{ cuadros}}{\text{segundos}} \times \frac{1 \text{ Mbit}}{1024 \text{Kbits}} = 0.57 \text{ Mbps}$$

9.1.5. Ancho de banda que consume el total de cámaras IP

Con el ancho de banda que consume una cámara IP se procede a calcular el ancho de banda aproximado que consume el total de cámaras IP.

Para calcular el ancho de banda total aproximado se debe multiplicar el número total de cámaras por el ancho de banda que consume cada una de ellas.

Ancho de Banda total [Mbps] = Ancho de banda por cada cámara [Mbps] X # de cámaras

Ancho de Banda total [Mbps] = 0.57 Mbps x 6 = 3.42 Mbps

4.11.6. Calculo de la capacidad aproximada de almacenamiento del disco duro para el servidor en una semana.

La cantidad de información almacenada en un disco duro depende de la cantidad de datos que se guarden en un tiempo determinado. Conociendo el ancho de banda aproximado que genera el total de cámaras y considerando que los eventos se eliminarían cada semana se puede obtener un cálculo aproximado de la cantidad de información que debe ser almacenada en el disco duro.

Ahora se procede a realizar un cálculo de datos que se guardarían en una semana en el disco duro

Almacenamiento [Gbyte] = AB total x segundos x semana

$$\text{Almacenamiento [Gbyte]} = 3.42\text{Mbps} \times 604800 \frac{\text{[segundos]}}{\text{[Semana]}} \times \frac{1 \text{ [Gbits]}}{1024 \text{ [Mbits]}} \times \frac{1 \text{ [byte]}}{8 \text{ [bits]}}$$

Almacenamiento [Gbyte] = 252.4 Gbytes

VII. Conclusión

a. Conclusión

En la Implementación de un sistema de vigilancia y control de eventos con acceso a través de red, en el área de Tesorería de la UNAN – Managua, se auditaron todos los eventos ocurridos en dicha área, mediante la vigilancia con cámaras ip tanto en las zonas externas como internas del área de Tesorería.

También se realizaron los cálculos necesarios para conocer los bits de información que se generan y el ancho de banda necesario que genera la red inalámbrica de la UNAN-Managua.

Se Implementa un sistema de vigilancia accesible a través de la red donde el usuario puede manipular el programa de monitoreo sin ninguna dificultad conforme con lo que necesite para su cometido.

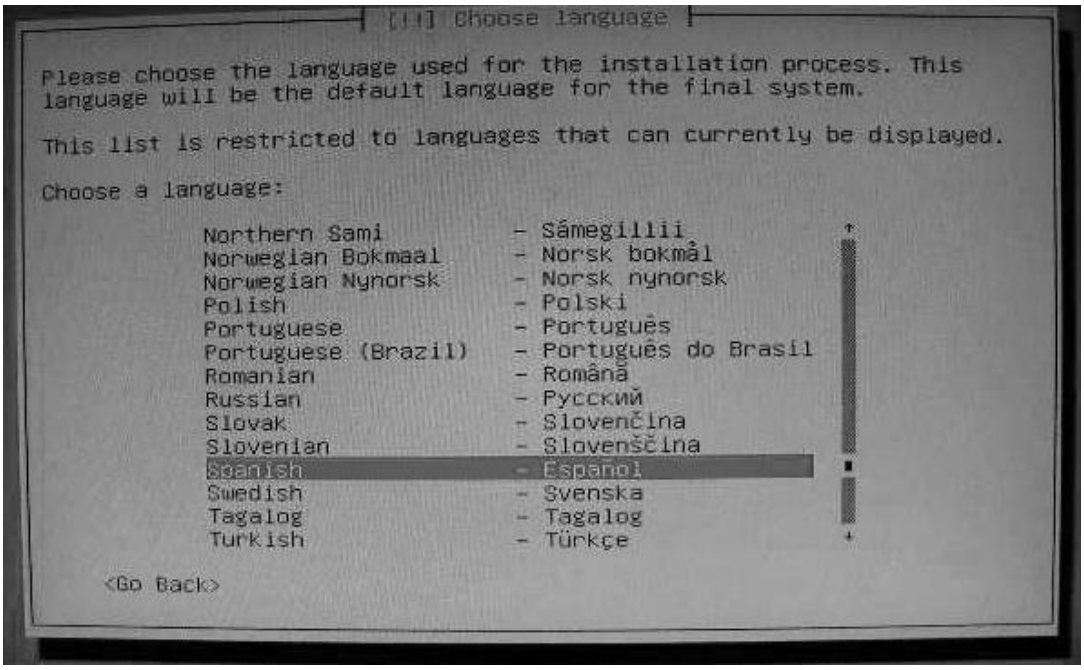
Además se monitorearon los eventos que transcurrieron en el área de Tesorería en el sistema de vigilancia instalado.

También se realizó un estudio de factibilidad que dio como resultado que la Alternativa 2 es la más factible tanto técnica, económica como operativa. Esto fue debido a que en la UNAN-Managua se cuenta con la mayoría de los requerimientos técnicos para su implementación.

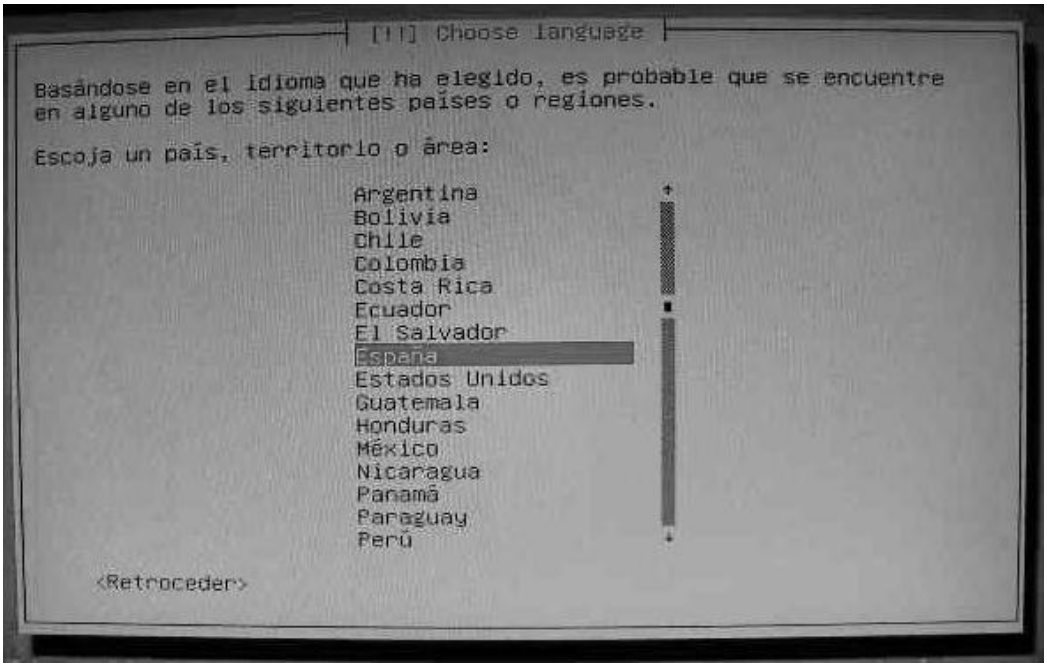
VIII. Anexos

a. Pasos para la instalación de Linux debían:

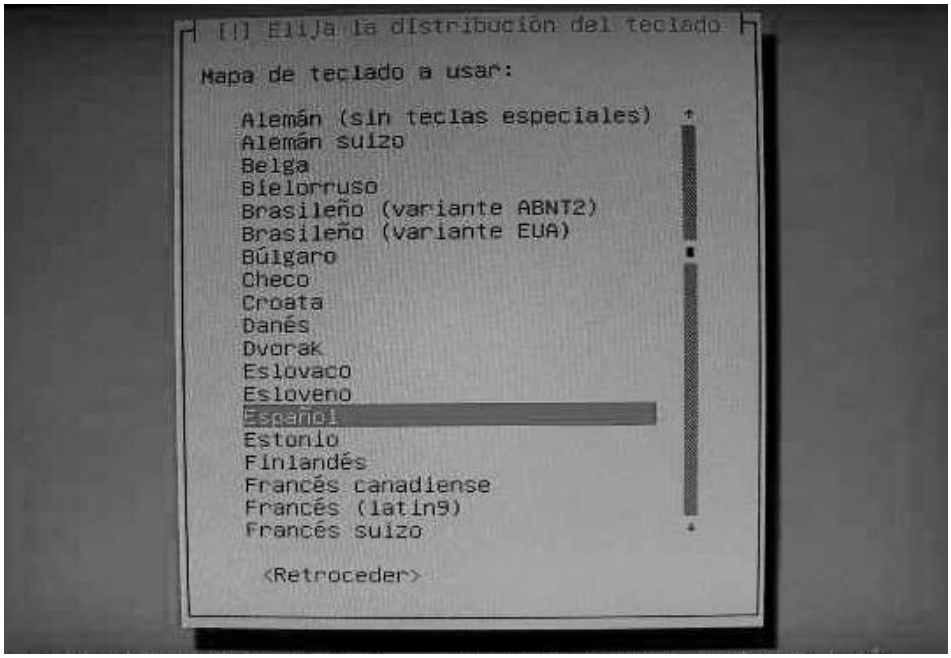
- Se selecciona el lenguaje del que se quiere la instalación



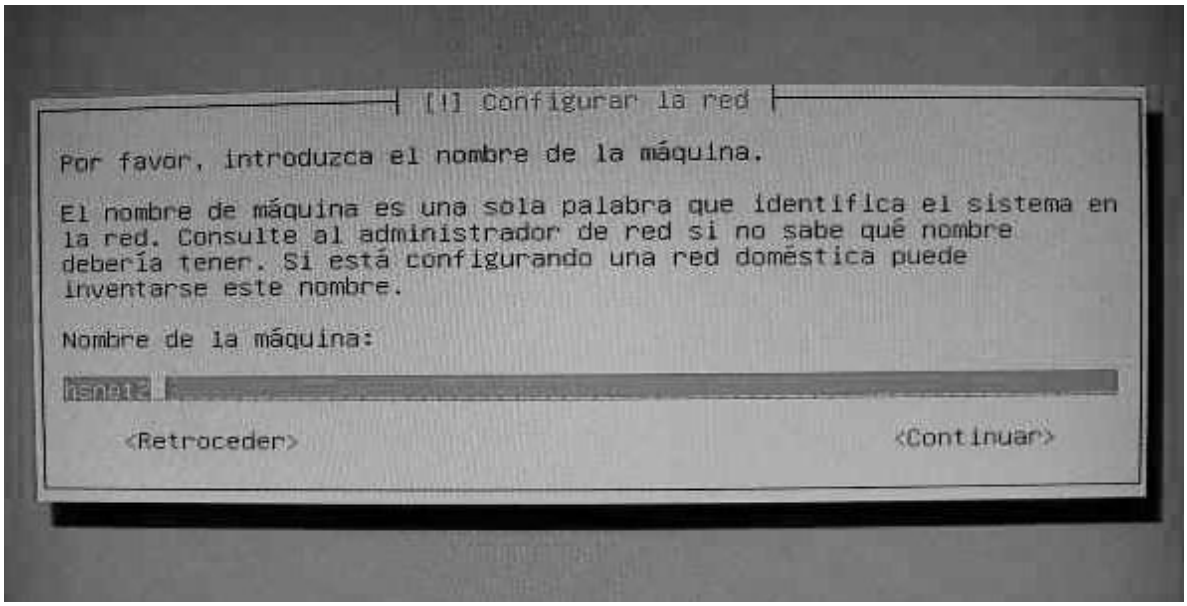
- Se escoge el país



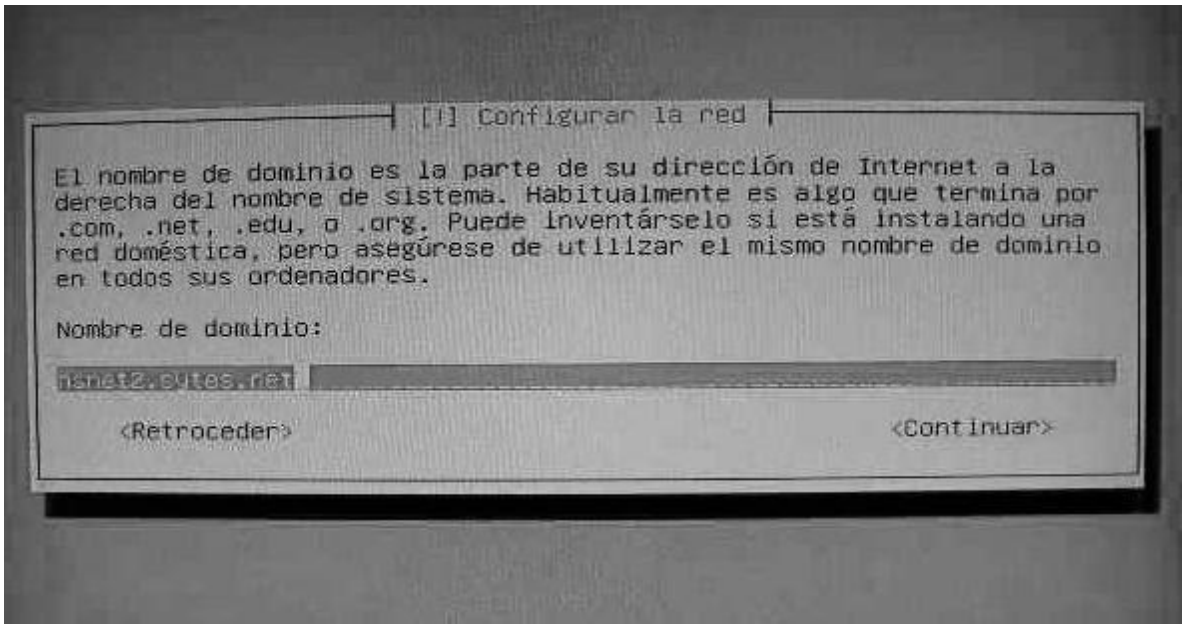
- Se elije la distribución del teclado (español).



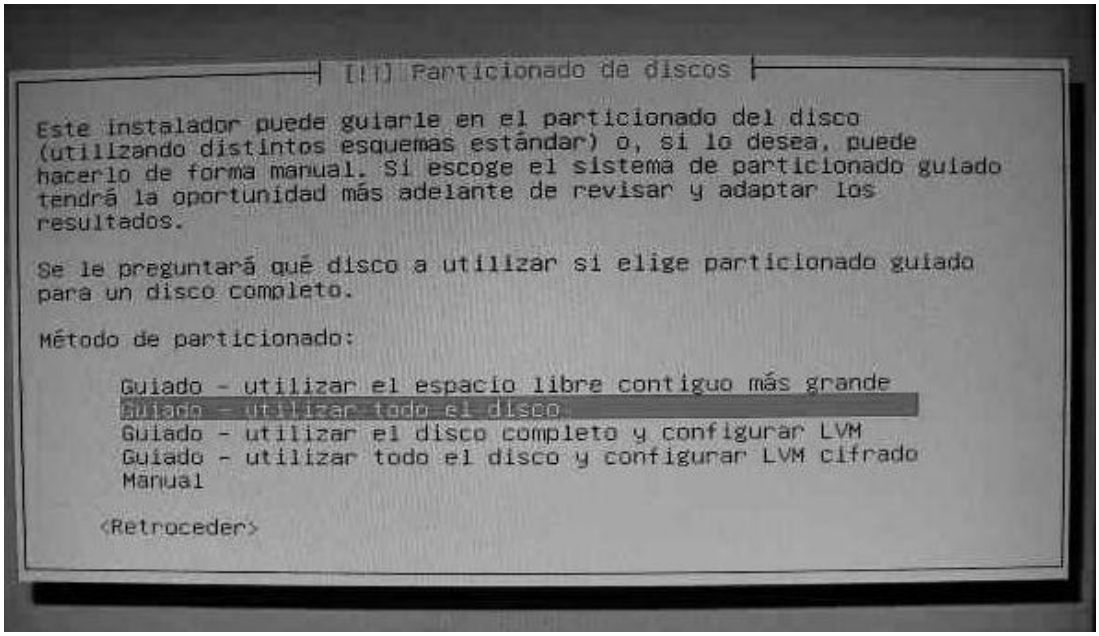
- Se introduce el nombre del sistema o de la máquina



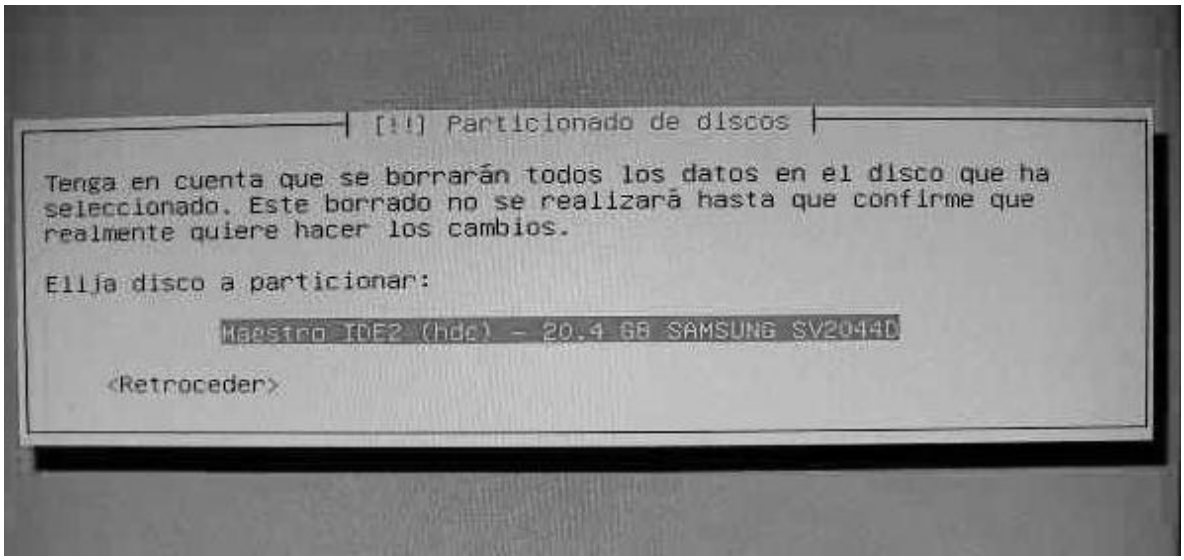
- Se configura el nombre de domino



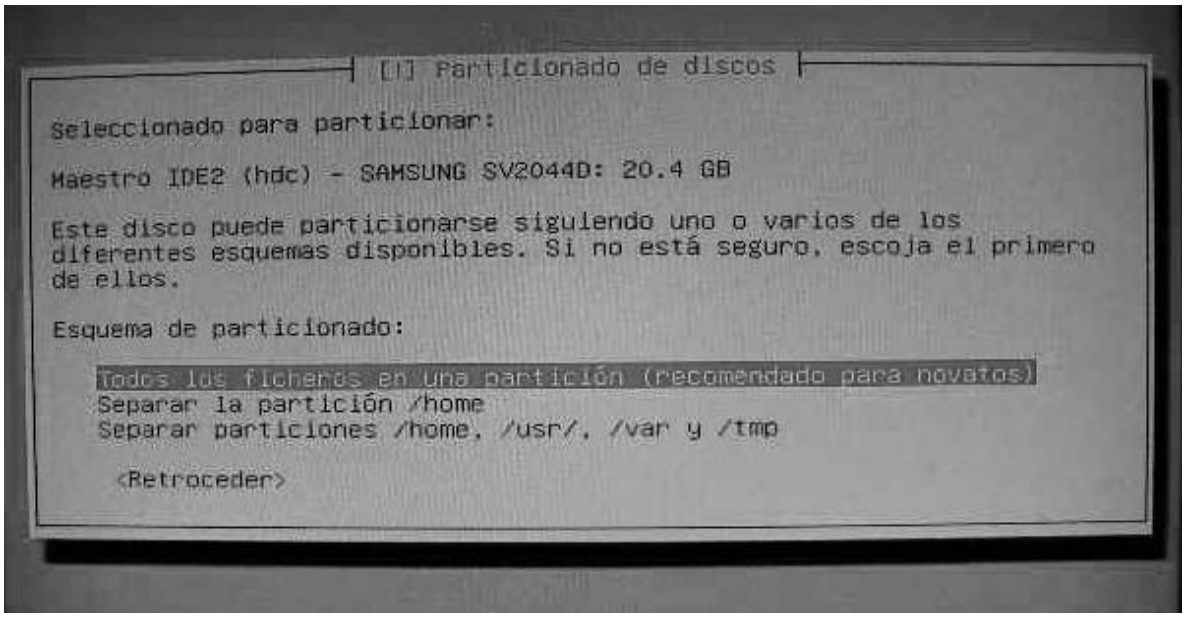
- Luego el proceso pide particionar el disco. Como vamos a usar la instalación de **Linux Debían** como servidor no se compartirá el disco duro. Por lo que se selecciona (**Guiado – utilizar todo el disco**).



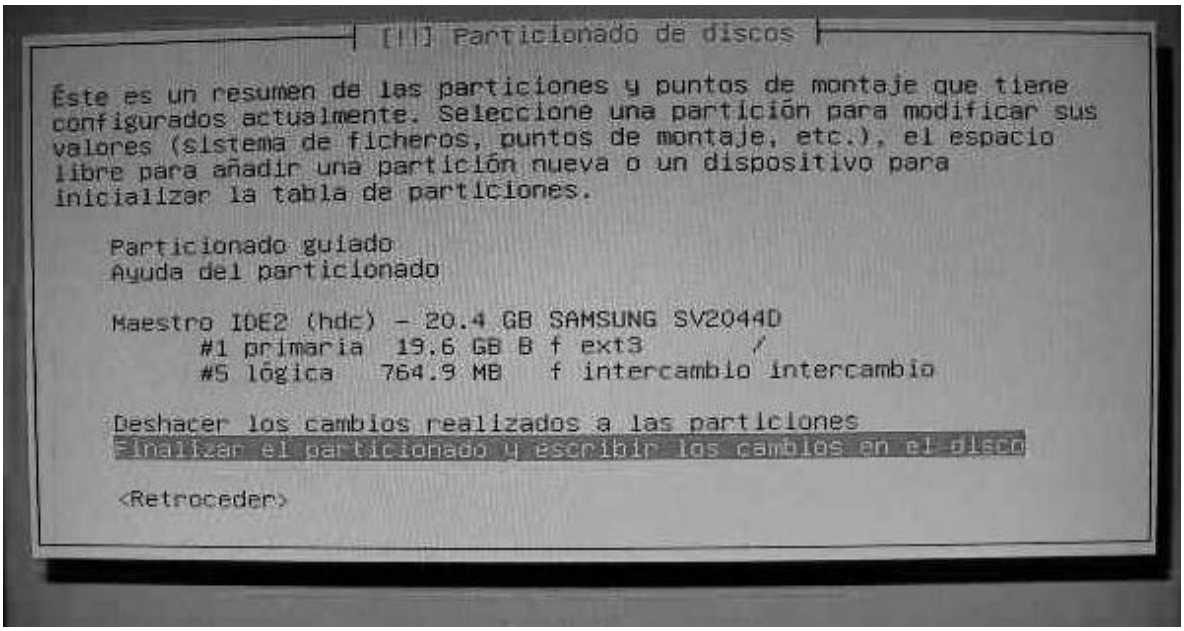
- Se elije el disco donde se desea particionar



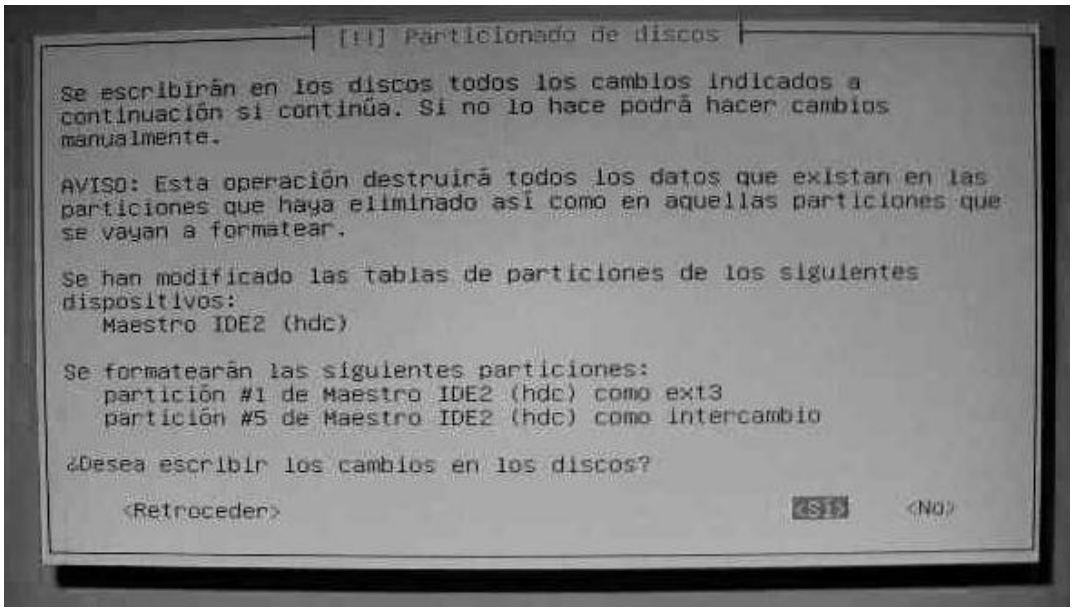
- Ahora nos deja elegir entre tres opciones, para simplificar un poco las cosas podemos seleccionar el modo (recomendado *para novatos)* que tan solo nos creará una partición **raíz /** y una **swap**. Se separara la partición **/home /** y se instalan todos los ficheros en la partición ya antes seleccionada



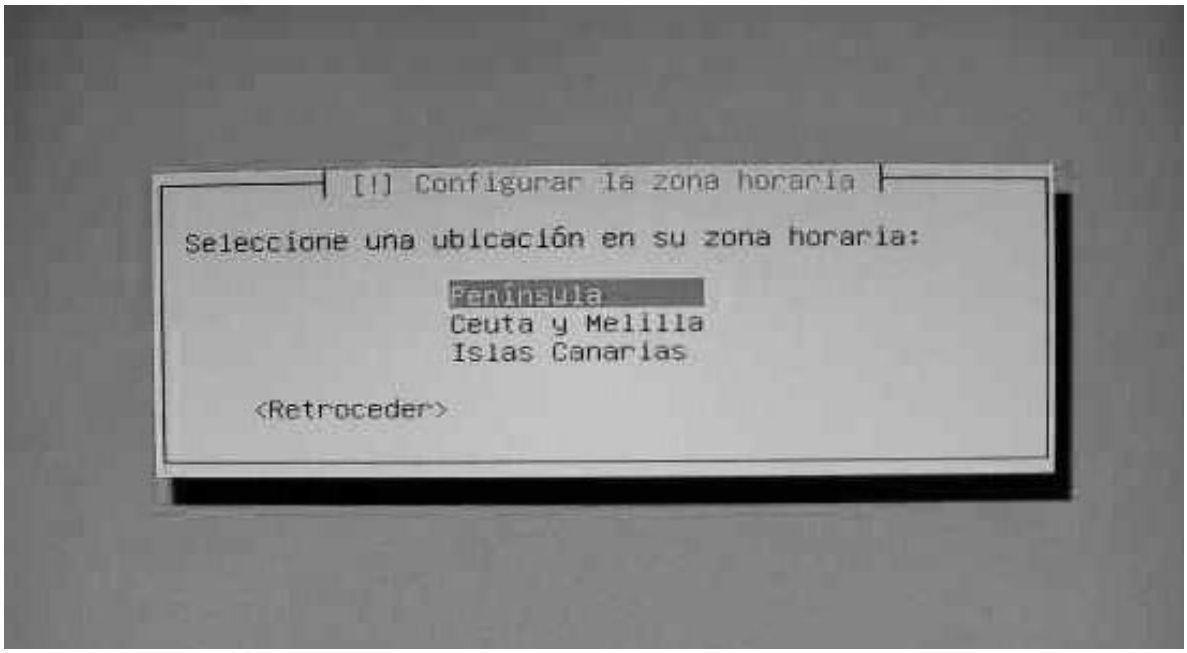
- Se finalizar el proceso de particionado y se procede a escribir los cambios en el disco



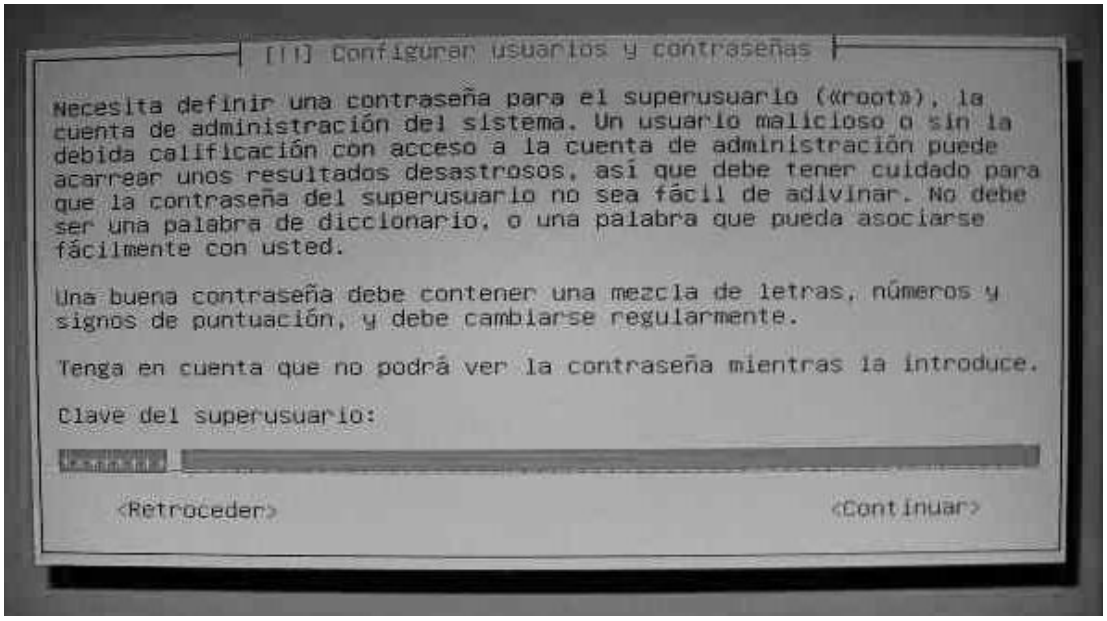
- El proceso de estación pide que se escriba en el disco todos los cambios hechos a la hora de particionar el disco



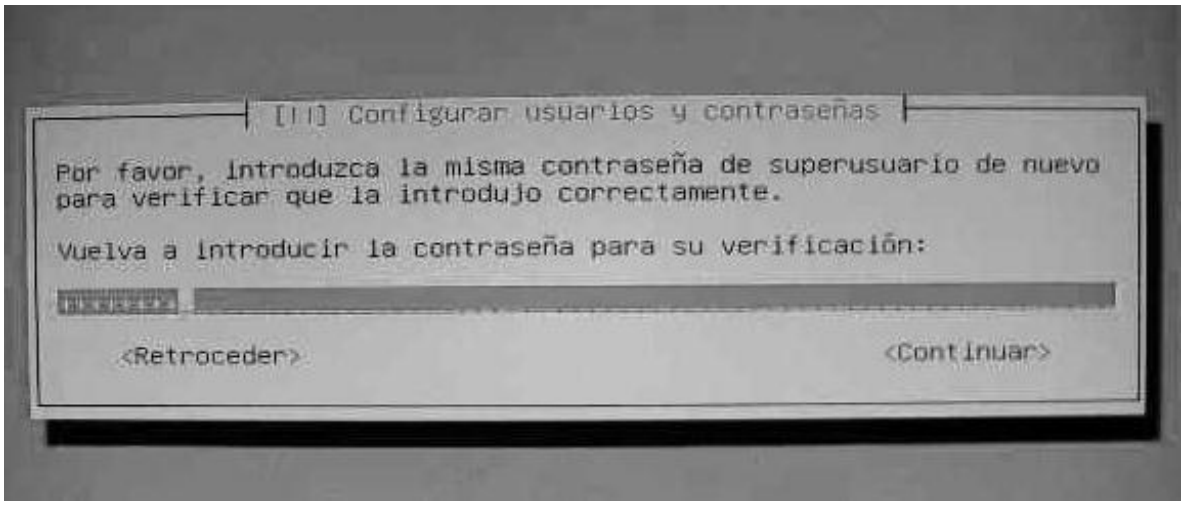
- Se selecciona la zona horaria



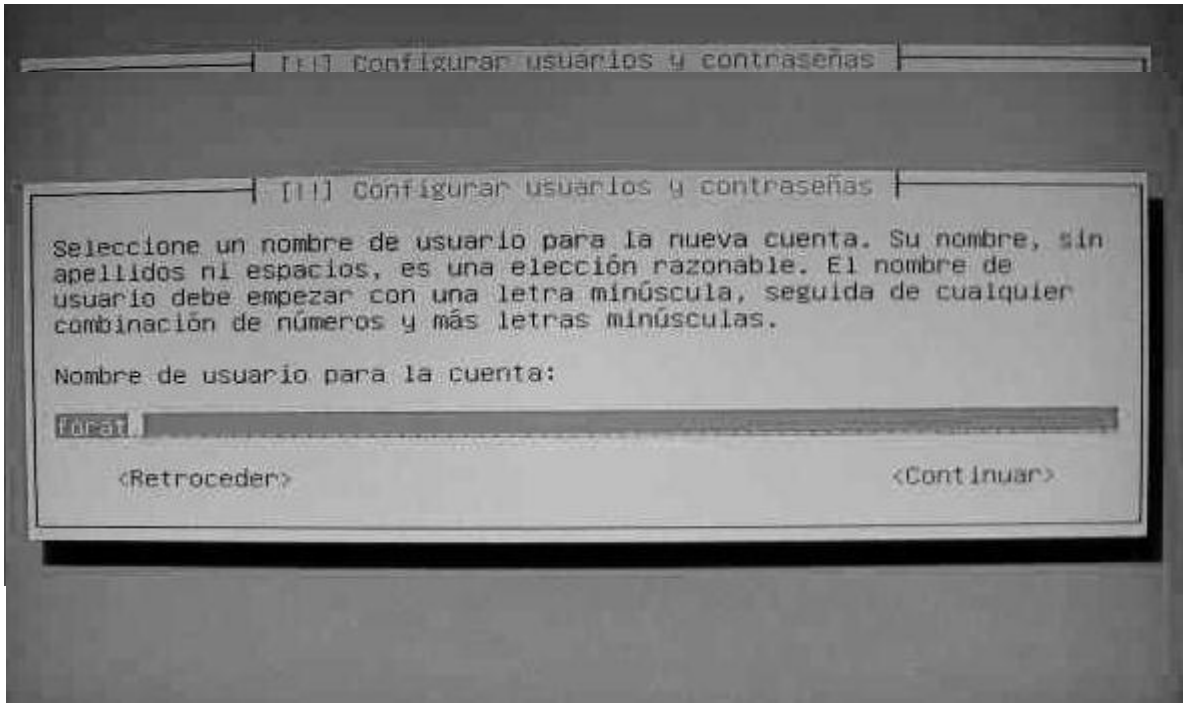
- Se definirá una contraseña para el súper usuario (root)



- Rescriba la misma contraseña de súper usuario para verificar que la introdujo correctamente

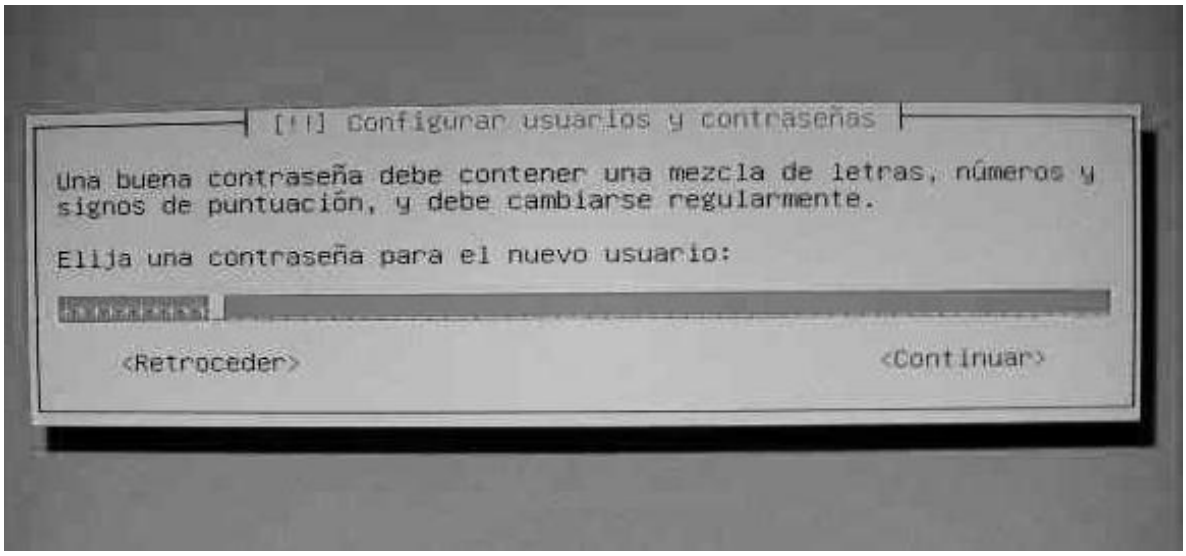


- se creará una cuenta de usuario para que se use en vez de la cuenta de súper usuario en las tareas que no sean administrativas.

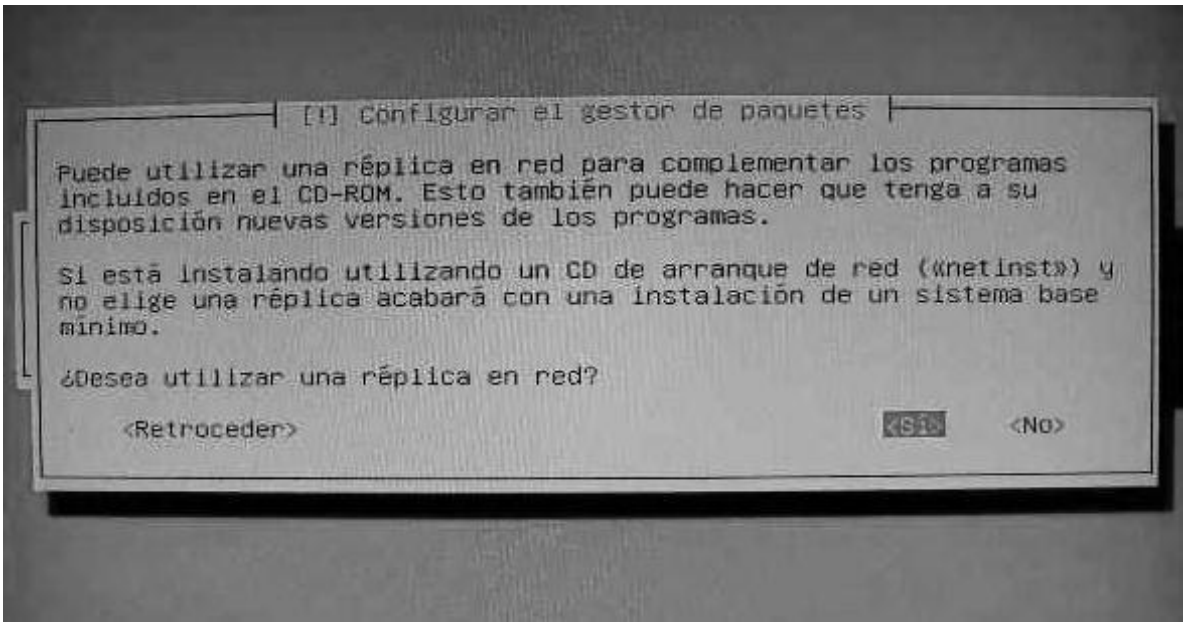


- Se escribe un nombre de usuario para la nueva cuenta

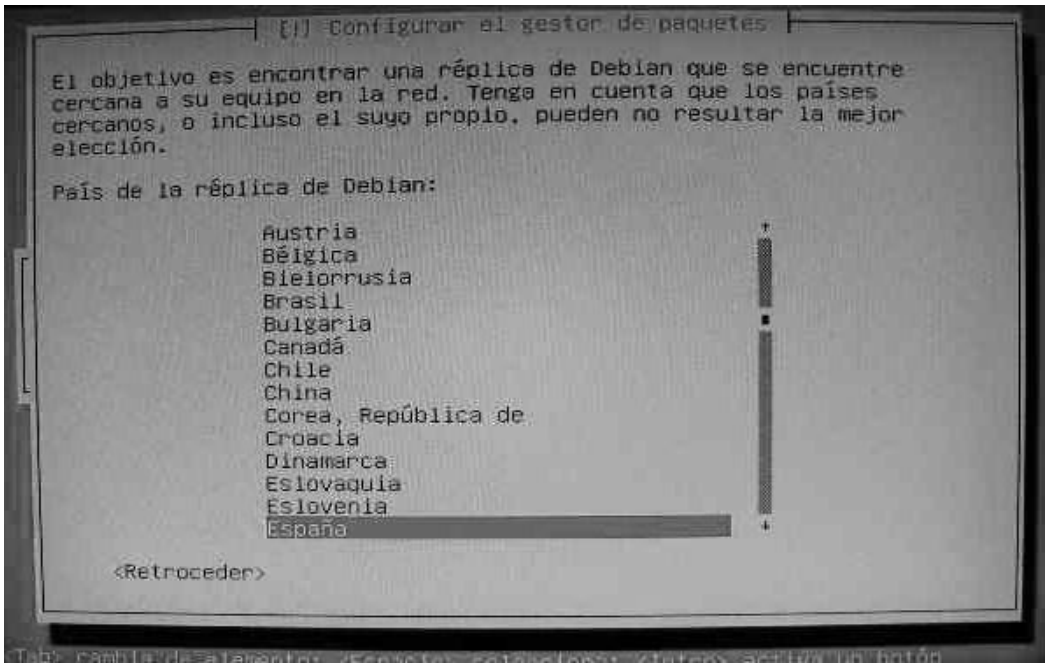
- Introduzca una contraseña para el usuario ya creado



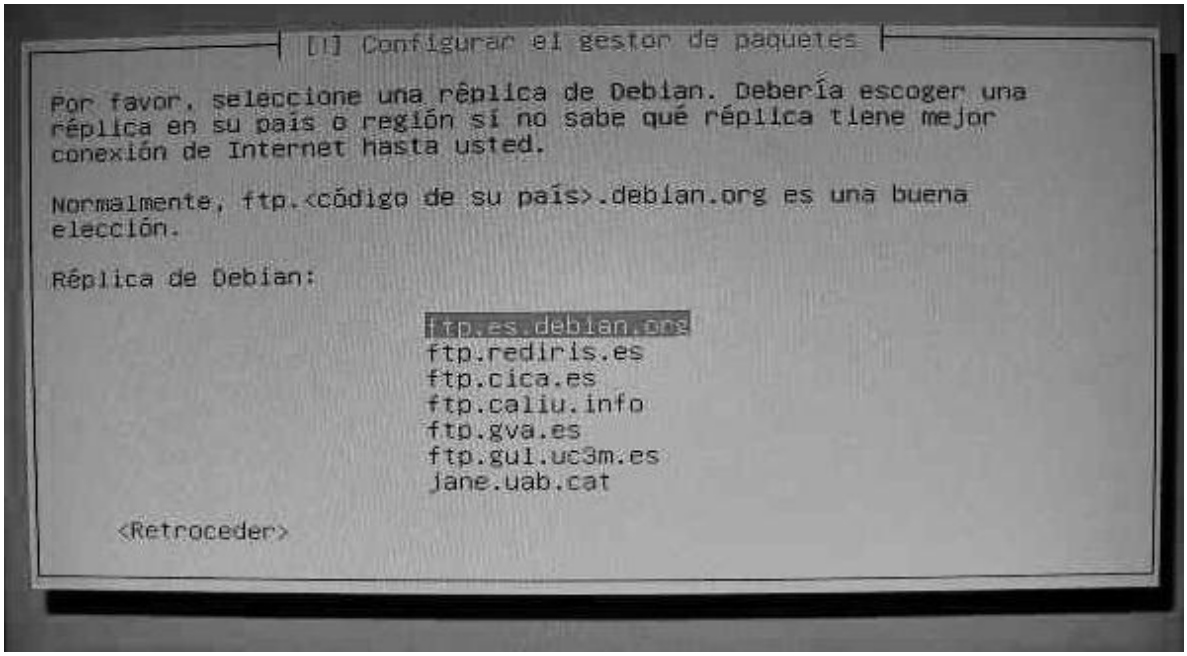
- se utiliza una réplica de red para complementar los programas



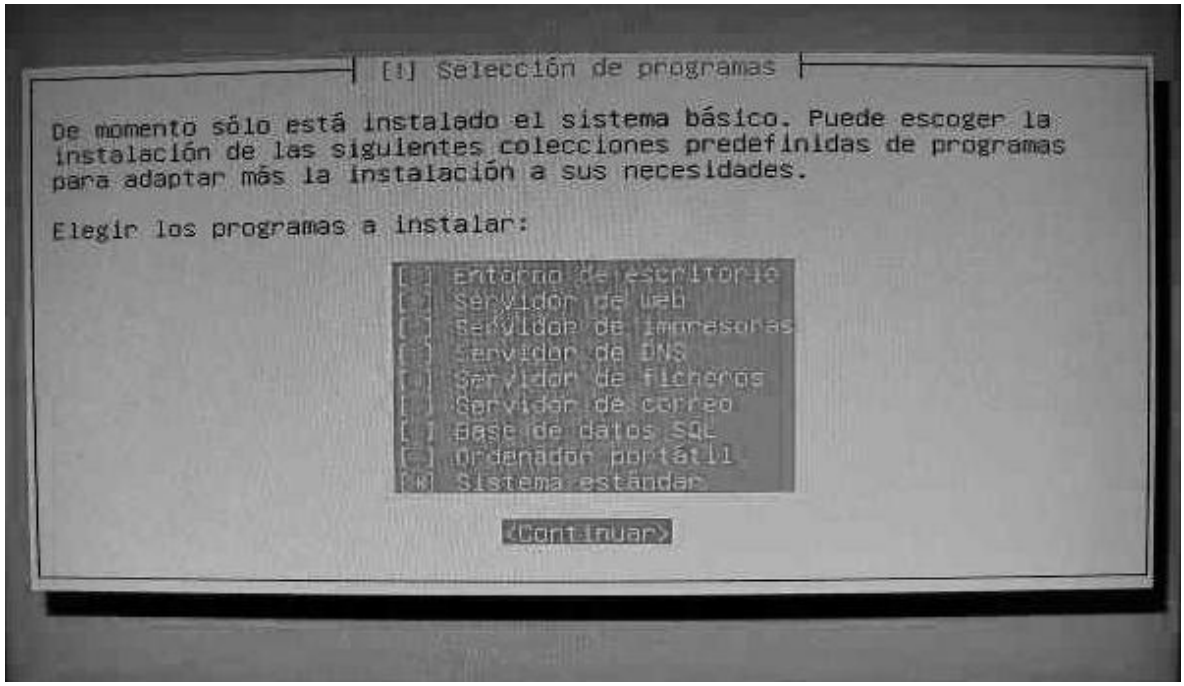
- Se elige un país el cual se pueda utilizar como replica



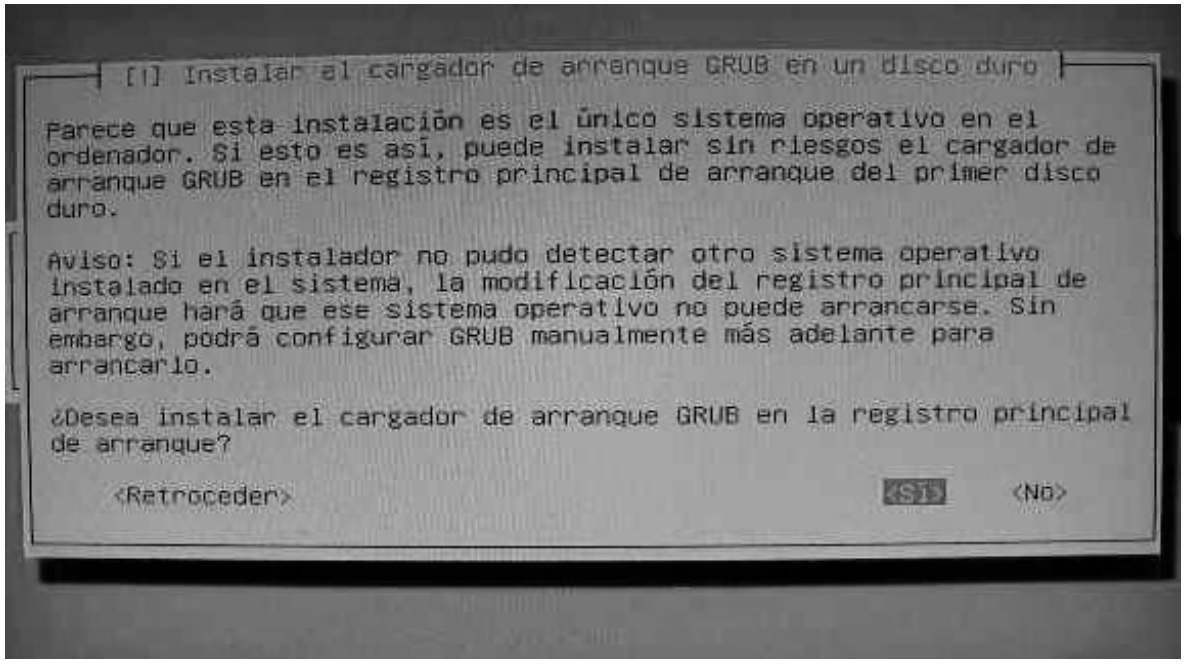
- Elegimos la replica



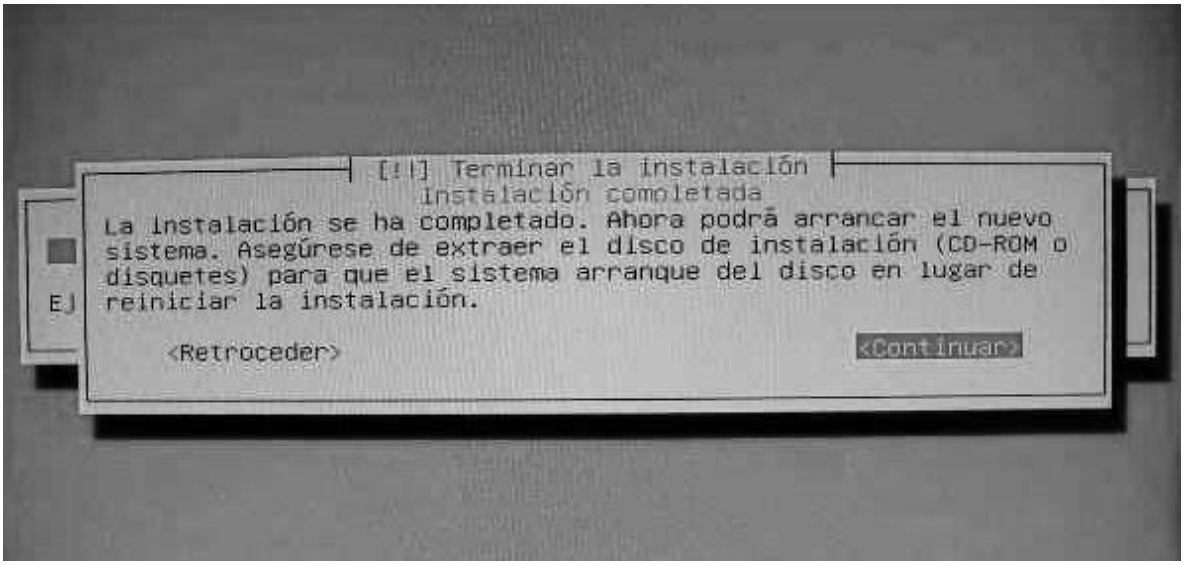
- Se selecciona el sistema estándar ya que se instaló el sistema básico



- En este momento la instalación nos pide instalar el archivo GRUB en el disco duro



Se finaliza la instalación con éxito



b. Pasos para la instalación de software de vigilancia ZoneMinder

1) Descargar la última versión disponible de ZoneMinder en el sitio Web oficial en:

http://www.zoneminder.com

En este caso se descarga el paquete de nombre 'zm-0.9.8.tar.gz'.

2) Ingresar al directorio donde se descarga y ejecutar el siguiente comando:

'#tar -xvzf zm-0.9.8.tar.gz'

Tal como se a mencionado este comando descomprimirá el paquete y creara un directorio de nombre 'zm-0.9.8'.

3) Descargar la versión más reciente del paquete 'TermReadKey' desde el sitio oficial en:

http://search.cpan.org/author/JSTOWE/TermReadKey-2.21/

En este caso se descarga el paquete de nombre 'TermReadKey-2.21.tar.gz'.

4) Entrar en el directorio donde se descarga y ejecutar el siguiente comando:

'#tar -xvzf TermReadKey-21.21.tar.gz'

Esta instrucción creara un directorio de nombre 'TermReadKey-2.21'.

5) Ingresar dentro de este directorio y ejecutar los siguientes comandos:

'#make'

'#make install'

Estos comandos compilan e instalan los módulos de lectura de teclado para el compilador del lenguaje Perl. Esto es necesario ya que ZonMinder lo requiere

6) Ingresar en el directorio 'src' de la carpeta 'zm-0.9.8' y editar el archivo de nombre 'zm.h' y comentar la línea (utilizar // al comienzo de la línea) double round(double); esta linea es alrededor de la numero 46 dentro del archivo.

7) Entrar en el directorio de nombre 'zm-0.9.8' y ejecutar el siguiente comando:

'./configure –with-mysql=/usr –with-webdir=/var/www/html/zm –with-cgidir=/var/www/cgi-bin'

Esta instrucción enviara algunos parámetros de ubicación de archivos al archivo de compilación de la aplicación. La ruta '/usr' corresponde al directorio raíz de archivos de sistema utilizables por usuarios, a esa ruta ZoneMinder le agrega la ruta 'lib/mysql' por lo cual el archivo 'libmysqlclient.a' debe encontrarse en la ruta completa '/usr/lib/mysql/'. De no ser así deberán modificarse los parámetros enviados o crear links simbólicos a la carpeta de origen.

Los otros dos parámetros le dicen la ubicación de instalación (preferiblemente dentro del directorio Web) y la ubicación de la carpeta de gráficos y binarios del servidor Web que en este caso es '/var/www/cgi-bin'.

8) Crear el directorio 'zm' dentro de '/var/www/html'.

9) Dentro del directorio 'zm-0.9.8' ejecutar el siguiente comando (como usuario root):

'#chmod +x zmconfig.pl'

Esto le dará permisos de ejecución al archivo.

10) En el mismo directorio ejecutar el comando:

'#./zmconfig.pl'

Esto iniciara la ejecución del script, escrito en lenguaje Perl, 'zmconfig.pl', el cual preguntara una serie de información que por lo general deberá ser ingresada con los valores desplegados por defecto.

En el caso de la pregunta que hace mención respecto al nombre del servidor este debe ser localhost ya que es en la misma maquina donde se ejecutaran MySQL y ZoneMinder.

Respecto a la pregunta del applet para imagenes 'cambozoal.jar' se escribe solo el mismo nombre del archivo, este sirve para crear imágenes en miniatura a partir de originales mayores para hacer más rápida la carga de una serie de imanes y se copea posteriormente.

Además se nos preguntará por dos nombres de usuarios MySQL y sus respectivas contraseñas, el primero con atributos totales dentro de la base de datos que se creara 'zm' y otro con permisos de consulta dentro de la base de datos 'zm' en MySQL, esto usuarios se podrán crear más tarde pero para fines de prueba se ingresa los dos usuarios como 'root' y con su contraseña para MySQL.

El resto de las preguntas hacen referencia sobre parámetros de distintas configuraciones de anchos de banda y sobre transmisión a dispositivos movibles, todo esto se puede ingresar con los valores por defecto

11) Descargar la última versión disponible del applet para imágenes 'cambozola' desde:

http://www.charliemouse.com/code/cambozola/

En nuestro caso se descarga el paquete de nombre 'cambozola-latest.tar.gz'

12) Descomprimir tal como se ha realizado anteriormente con el comando 'tar -xvzf'.

13) Esto creará varios directorios y archivos, copiar el contenido del directorio 'dist' dentro de /var/WWW/html/zm'.

14) Crear una base de datos con el esquema 'zmschema.sql' que se encuentra dentro de la carpeta 'db' dentro del directorio 'zm-0.9.8', esto se realiza estando dentro del directorio 'db' y ejecutando el siguiente comando:

'#mysql < zmschema.sql -p'

Se nos consultara por la password del 'root' en MySQL. Luego dentro de 'PhpMyAdmin' podremos darles todos los permisos dentro de la base de datos 'zm' a otros usuarios.

16) Editar el archivo '/etc/php.ini' y verificar que la linea 49 este de la siguiente manera:

short_open_tag = On

17) Ejecutar los siguientes comandos dentro del directorio 'zm-0.9.8':

'#make'

'#make install'

Antes de usar la aplicacion se debe modificar el archivo zmactions.php ya que recientemente se detectó un error en este. En la linea 69 se encontrara lo siguiente:

```
stopDaemon("zma",$mid);
zmaControl( $mid );
```

Se debe borrar la primera y modificar la segunda para que quede de la siguiente forma:

```
zmaControl( $mid, true );
```

18) Luego de esto y si no se generaron mensajes de error la aplicación ZoneMinde debiera estar correctamente instalada, ahora para probarla solo basta ingresar dentro del directorio 'scripts' y ejecutar los siguientes comandos:

'#chmod +x zm'

'#./zm start'

Esto ejecutara manualmente el demonio de la aplicación 'ZoneMinde' el cual puede luego hacerse que inicie automaticamente al encenderse la computadora colocando una referencia a la última instrucción en el archivo '/etc/rc.d/rc.local'.

Luego solo habrá que escribir la siguiente dirección en un browser tanto de Windows como de Linux.

http://operaciones3/zm/zm.php o http://192.168.45.157/zm/zm.php

La utilización de la aplicación esta descrita en un archivo de nombre 'README.txt' en el directorio 'zm-0.9.8', además en este archivo hay ciertas sugerencia y pasos adicionales que es conveniente revisar sobre todo en el caso de encontrarse con algún error durante el proceso

c. Guía de usuario para la configuración de ZoneMinder

1.1. Parámetros de configuración ZoneMinder

Concluida la instalación de ZoneMinder, hay que ejecutar ciertos pasos para configurar y monitorear cada una de las cámaras instaladas, considerando si son cámaras Web, IP o video cámara. En la figura 1, se indica la página principal de ZoneMinder.

Figura 1.1 Página Principal de ZoneMinder.

1.2. Monitores

Un monitor es la representación del streaming de video en una página web creada usando PHP. Un monitor debe ser configurado previamente antes de funcionar.

La ventana de configuración se muestra en la figura 1.2.

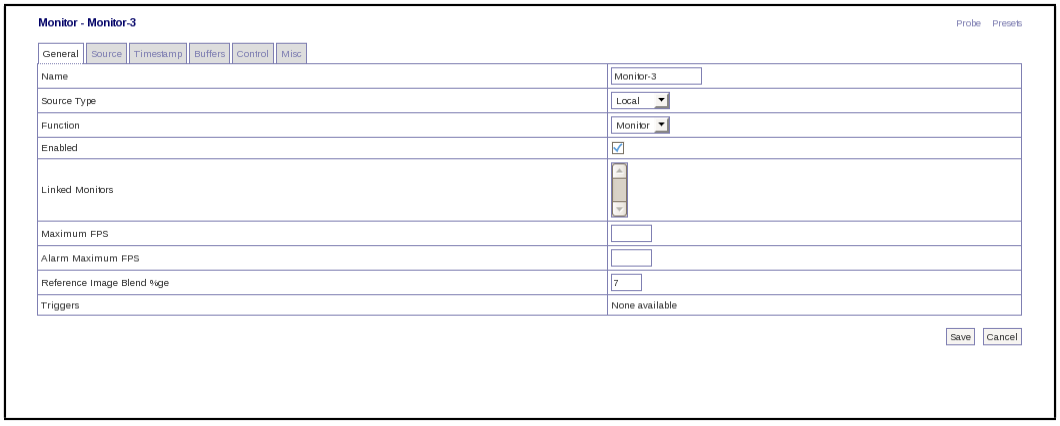


Figura 1.2. Ventana de configuración para un nuevo monitor

Las opciones de configuración de la pestaña monitor son:

- Pestaña General.
- Pestaña Fuente.

- Pestaña Marca de Tiempo.
- Pestaña Búfer.
- Pestaña Control.
- Pestaña Miscelánea.

A continuación se describe cada una de las opciones de configuración.

1.3. Pestaña General.

Campo Nombre. Aquí se indica el nombre para el monitor. Debe ser un nombre que contenga únicamente caracteres alfanuméricos, guiones (-) y guiones bajos (_), el espacio en blanco no está permitido

Campo Tipo Fuente (*Source Tipe Field*). Se define qué tipo de cámara se va a utilizar, siendo estas:

Tipo Local. Este tipo se refiere a cámaras de video y cámaras web.

Tipo Remoto. Este tipo se refiere a cámaras IP.

Campo Función (*Function Field*). Esencialmente define la función del monitor. Puede ser alguna de las siguientes opciones.

None.- Deshabilita temporalmente al monitor.

Monitor.- El monitor solo recibe el streaming de video pero no se realiza ningún tipo de análisis de video.

Modect.- Permite la detección de movimiento. Todas las imágenes capturadas será analizadas y generará eventos cuando exista movimiento.

Record.- Permite grabación continua, en esta opción la detección de movimiento está deshabilitada.

Mocord.- Es un híbrido entre Modect y Record, que permite grabación continua y detección de movimiento.

Nodect.- Está designado para ser usado con dispositivos externos, lo que significa que si un dispositivo externo se activa, este inicia la grabación de video.

Campo Habilitado (*Enabled Field*). Este campo permite activar la generación de eventos en respuesta a la detección de movimientos o por activación de dispositivos externos

Campo Monitores Vinculados (*Linked Monitors Field*). Este campo permite enlazar otros monitores que activarán este monitor en caso de que se detecte movimiento.

Campo Máximo FPS (*FPS Maximum Field*). Este campo permite aligerar la carga del servidor en caso de que se tengan varias cámaras, permitiéndonos, Limitar FPS a un valor específico y reducir el procesamiento. En caso de ser cámaras IP se debe configurar en el servidor interno del mismo.

Campo Máxima Alerta FPS (*AlarmMaximum FPS Field*). Este campo permite generar una alarma cuando se recibe un número superior de FPS, debido a movimientos inusuales de algún lugar monitoreado. En caso de no utilizar esta opción se debe dejar este campo en cero.

Campo de Mezcla de Imágenes Referenciada (*Reference ImageBlend Field*). Este campo permite determinar el grado de composición de una imagen. Cada imagen analizada en ZoneMinder es una composición de imágenes anteriores y está formada aplicando la imagen actual y un cierto porcentaje de la imagen anterior. Para establecer este valor se debe iniciar con un valor de 10, el mismo que es un valor por defecto y luego ir reduciendo hasta obtener la imagen deseada.

1.4. Pestaña Fuente (*Source*).

Las opciones de configuración de la pestaña "*Source*" varían dependiendo del parámetro "Tipo de Fuente" que se escogió previamente. En la figura 1.3, se indica la ventana generada por la pestaña Fuente cuando se utiliza cámaras Web o cámaras de video analógicas.

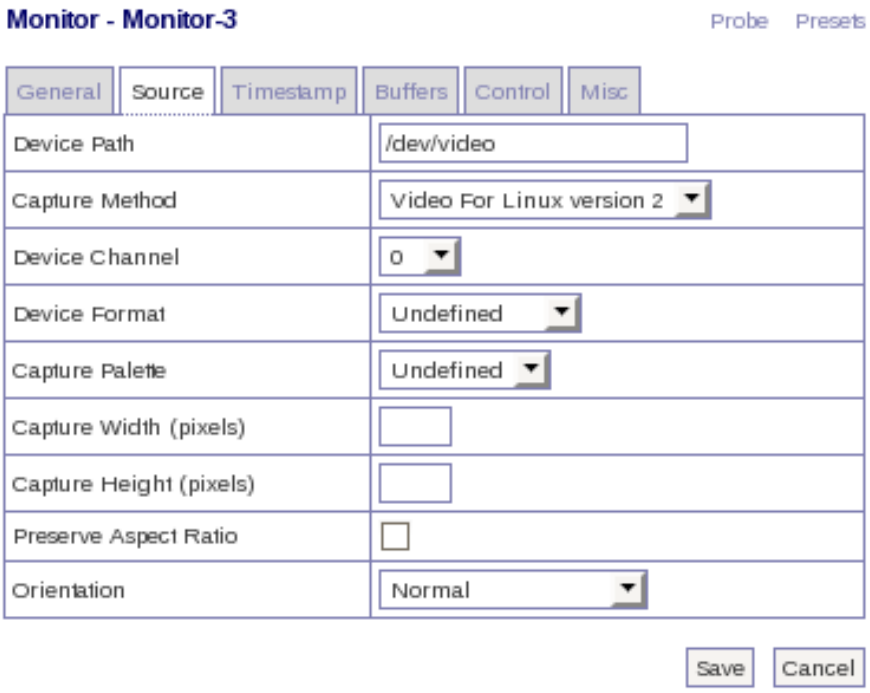


Figura 1.3. Ventana de configuración pestaña Fuente para dispositivos local

En la figura 1.4, se indica la ventana de configuración cuando se utiliza cámaras IP

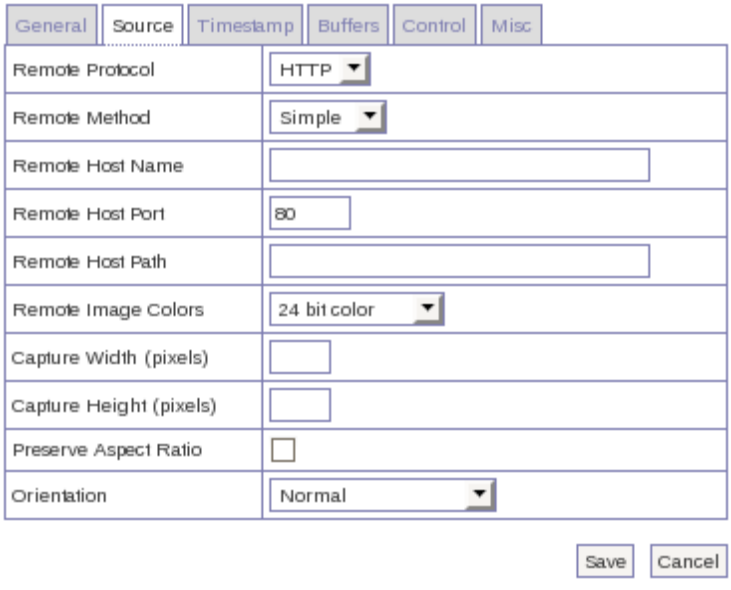


Figura 1. 4. Ventana de configuración pestaña fuente para dispositivos remotos

Campo de Protocolo Remoto (*Remote Protocol Field*). Este campo indica el protocolo con el cual se va a conectar una cámara IP. Los protocolos soportados por ZoneMinder son HTTP (*HyperText Transfer Protocol - Protocolo de Transferencia de Hipertexto*) y RTSP (*Real Time Streaming Protocol – Protocolo de Flujo de Datos en Tiempo Real*).

Campo Método Remoto (*Remote Method Field*). Este campo Indica en que formato va a ser enviado la URL (*Uniform Resource Locator - Localizador de Recurso Uniforme*). Puede ser simple o regexp.

Campo Nombre de Host Remoto (*Remote Host Name Field*). Este campo indica el dominio o la dirección IP de la cámara de donde se obtiene el streaming de video.

Campo Path Remoto (*Remote Path Field*). Este campo indica la URL correspondiente al streaming de video.

Campo Colores de Imágenes Remotos (*Remote Image Colors Field*). Este campo permite indicar la cantidad de colores para el video. Este valor puede ser 24 bits u 8 bits.

Campo Ancho de la Captura (*Capture Width Field*). Este campo permite escoger el ancho de la imagen del streaming de video, provisto por el dispositivo de video.

Campo Alto de la Captura (*Field Capture Height*). Este campo permite escoger el alto de la imagen del streaming de video, provisto por el dispositivo de video.

Campo Radio de Aspecto (*Keepaspect ratio Field*). Este campo permite calcular automáticamente el ancho o el alto del streaming de video enviado por un dispositivo de video. Este proceso se lo realiza teniendo en cuenta la relación de aspecto que por defecto en ZoneMinder es 4:3.

Campo Orientación (Orientation Field). Este campo permite adaptar la rotación de video en caso de que esta cámara se encuentre cabeza abajo o de lado, no es muy recomendable activarlo, debido a que requiere procesamiento adicional.

1.5. Pestaña Marca de Tiempo (Timestamp).

Las opciones de configuración para esta pestaña permiten etiquetar el video capturado ingresando el formato de los ejes, hora y fecha. En la figura 5, se indica la ventana de configuración Marca de Tiempo.

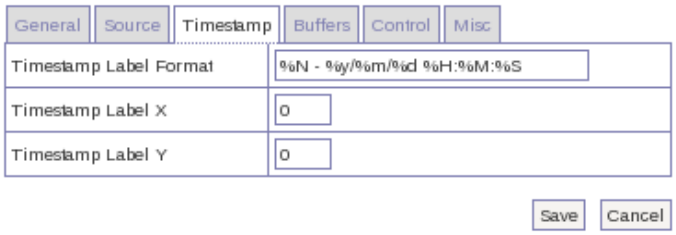


Figura 1.5. Ventana de configuración de Marca de Tiempo.

Campo Formato Etiqueta de la Pestaña de Tiempo (*Timestamp Label Format*). Este campo permite adaptar el formato de hora y fecha a cada frame de video. El formato a ingresar para obtener fecha, hora, minuto, segundo y centésima de segundo es: %y/%m-%H:%M:%S.%f. En caso de que se requiera identificar el nombre del monitor se debe agregar %N.

Campo de Etiqueta X/Y para la pestaña de Tiempo (*Timestamp Label X/Y*). Este campo permite indicar el lugar donde se mostrará el campo Timestamp Label Format.

1.6. Pestaña Búfer.

Las opciones de configuración para esta pestaña permiten determinar y analizar los cuadros enviados por las cámaras para determinar alarmas. En la figura 1.6, se indica la pestaña Búfer.

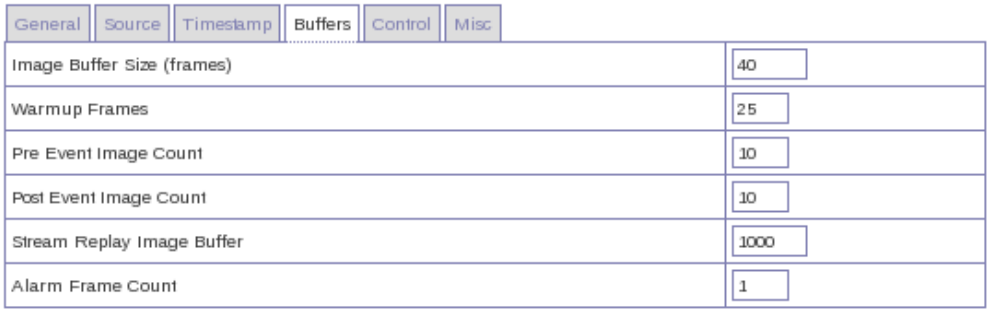


Figura 1. 6. Ventana de configuración de Búfer

Campo Tamaño de Búfer (*Buffer Size Field*). Este campo permite determinar cuántos cuadros se procesan en un "anillo de búfer" en un momento dado. El anillo de búfer es el espacio de almacenamiento donde las últimas "n" imágenes son almacenadas, para ser restauradas en caso de alarma o simplemente si se van a aguardar para posteriormente ser analizadas. El

valor promedio y por defecto es de 50, se puede aumentar este valor pero requiere mayor cantidad de memoria.

Campo *Warm-up Frames*. Este campo permite especificar cuantos cuadros debe procesar el demonio "análisis". El valor promedio y por defecto es de

25 cuadros, si el valor es muy alto retrasa el inicio del demonio análisis y si el valor es muy bajo se generarán falsas alarmas.

Campo de Imagen Pre/Post Evento (*Pre/Post Event Image Buffer Field*). Este campo permite determinar cuántos cuadros se debe mantener antes y después de un evento. El valor promedio y por defecto es 10.

Campo Cuenta de Frames de Alarma (*Alarm Frame Count Field*). Este campo permite especificar cuantos cuadros alarmas consecutivos deben ocurrir antes de que se genere una alarma. El valor por defecto es 1, haciéndolo muy sensible, por lo que este valor no es óptimo.

1.7. Pestaña Control.

Las opciones de configuración para esta pestaña permiten determinar controles para manipular remotamente cámaras PTZ. En la figura 1.7, se indica la pestaña control.

Figura 1.7. Ventana de configuración Control

Campo Controlable (*Controllable Field*). Este campo permite indicar que la cámara a trabajar es controlable, es decir es PT o PTZ.

Campo Tipo de Control (*Control Type Field*). Este campo permite escoger el modelo de la cámara a ser controlada. Por defecto cinco modelos de cámaras están configuradas, si la cámara a trabajar no se encuentra listada, se debe modificar un script existente de alguno de los cinco modelos; este script está escrito en lenguaje PERL.

Campo Dispositivos de Control (*Control Device Field*). Este campo permite indicar el tipo de interfaz para controlar la cámara. En cámaras IP este campo no se toma en cuenta, debido a que la interfaz que controla el movimiento de la cámara es la tarjeta de red.

Campo Control de Dirección (*Control Address Field*). Este campo permite indicar la dirección IP que ocupa la cámara.

Campo Tiempo de Espera de Parada Automática (*Auto Stop Timeout Field*). Este campo permite detener el movimiento de una cámara PT dentro de un tiempo. Los valores pueden variar desde centésimas de segundos a segundos.

Campo Seguimiento de Movimiento (*Track Motion Field*). Este campo permite usar el módulo de rastreo de movimiento. Este módulo no es propio de todas las cámaras.

Campo Retardo de Seguimiento (*Track Delay Field*). Este campo permite indicar el número de segundos que se va suspender el rastreo de movimiento para después continuarlo.

Campo Sitio de Regreso (*Return Location Field*). Este campo permite regresar la cámara al sitio antes de iniciar el rastreo de movimiento.

Campo Retardo de Regreso (*Return Delay Field*). Este campo permite especificar el retardo en segundos que la cámara se demora en volver a su posición original después de terminar el rastreo de movimiento

1.8. Pestaña Miscelánea (Misc Tab).

Las opciones de configuración para esta pestaña permiten configurar ciertos aspectos relacionados a los eventos. En la figura 1.8, se indica la pestaña Miscelánea.

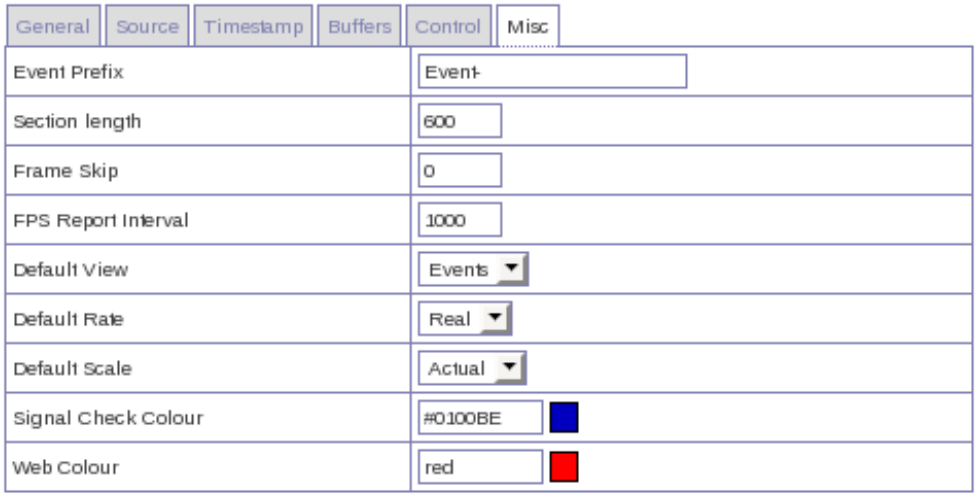


Figura 1. 8. Pestaña de configuración Miscelánea.

Campo Prefijo de Evento (Event Prefix Field). Este campo permite asignar un nombre a un evento.

Campo Longitud de Seción (Section Length Field). Este campo permite especificar la duración en segundos de los eventos generados únicamente en modo Record o Mocord. El rango de valores recomendados para no hacer difícil el análisis de los eventos es entre 300 y 900 segundos debido a que se debe realizar un análisis cuadro a cuadro.

Campo Salto de Cuadros (Frame Skip Field). Este campo permite especificar cuantos cuadros deberían ser omitidos, cuando se trabaja únicamente en modo Record y Mocord. El valor de 1 en este campo indica que por cada cuadro guardado va a omitir uno, de esta manera se reduce el espacio almacenado en el disco.

Campo de Escala por Defecto (Default Scale Field). Este campo permite ingresar la escala de la imagen a mostrar en la interfaz web.

Campo Color de la Web (Web Colour Field). Este campo permite especificar el color que identificará a cada uno de los monitores.

9.2. Usuarios y niveles de acceso.

La administración de Zoneminder es realizado por varios tipos de usuarios, los mismos que tienen diferentes niveles de acceso. El administrador posee los permisos necesarios para realizar cambios en el streaming recibido como en el almacenado, cambios en las zonas de vigilancia, idioma, etc. El resto de usuarios, así como sus permisos son asignados por el administrador.

La pestaña de usuarios tiene por defecto al usuario administrador, el mismo que posee los permisos para una administración total.

En la figura 2.1, se indica la Pestaña usuarios.

Figura 2.1 Pestaña Usuarios.

Para crear y administrar nuevas cuentas se debe abrir la ventana añadir nuevo usuario (*Add New User)*. La interfaz que permite crear y/o modificar nuevas cuentas de usuario se indica en la figura 2.2.

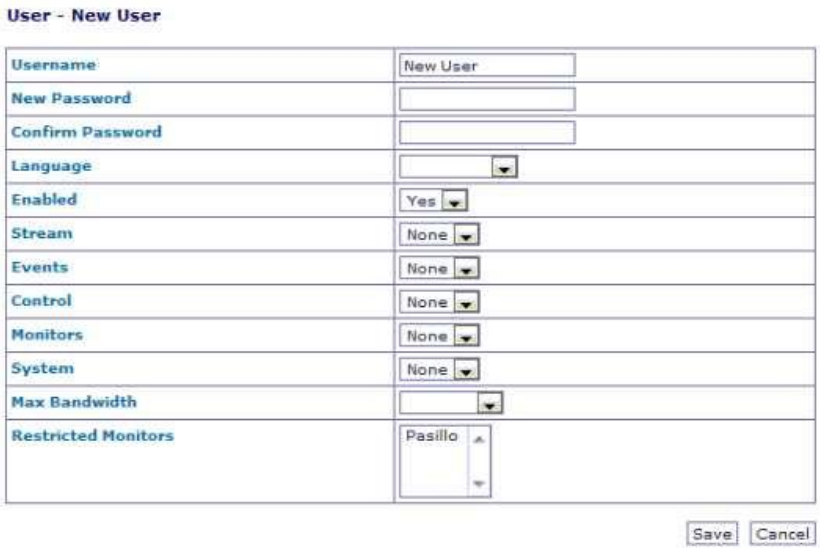


Figura 2.2 Ventana Usuario Nuevo (*Add New User*).

La ventana Añadir Nuevo Usuario permite crear una infinidad de usuarios, asignándoles diferentes niveles de acceso definidos por cada uno de los campos presentados a continuación.

Lenguaje (Language). El campo “Lenguaje” permite escoger el idioma de la interfaz web.

Habilitado (Enabled). El campo "Habilitado" permite o niega habilitar dicha cuenta.

Stream. El campo "Stream" permite o niega la visualización del video.

Eventos (Events). El campo "Eventos" permite o niega el acceso a los eventos guardados.

Control. El campo "Control" permite o niega acceder al movimiento de las cámaras PTZ.

Monitores (Monitors). El campo "Monitores" permite o niega la edición de Monitores.

Sistema (System). El campo "Sistema" permite o niega el ingreso a configuraciones avanzadas de ZoneMinder.

Máximo Ancho de Banda (Max Bandwidth). El campo "Ancho de Banda" permite asignar el ancho de banda con el que se conectarán los usuarios remotos.

Monitores Restringidos (Restricted Monitors). El campo "Monitores Restringidos" niega la visualización de los monitores seleccionados.

3.1. Zonas de vigilancia.

ZoneMinder se caracteriza por ser un software muy potente en el momento de analizar el streaming de video, permitiendo analizar un cuadro por sectores y asignarle varias zonas de vigilancia para que tome una acción diferente por cada una de ellas.

Cuando se crea un monitor y éste está asociado a una cámara, automáticamente se crea una zona denominada activa, que analizará todo el cuadro cuando se habilite el modo Modect o Mocord.

Los campos de configuración de zonas de vigilancia se realizan en la ventana agregar o editar una zona de vigilancia.

En la figura 3.1, se indican los campos de configuración de Zonas de Vigilancia.

Figura 3.1 Ventana agregar/editar/eliminar Zona de Vigilancia.

Al agregar o editar una zona de vigilancia se obtendrá lo que se indica en la figura 3.2.

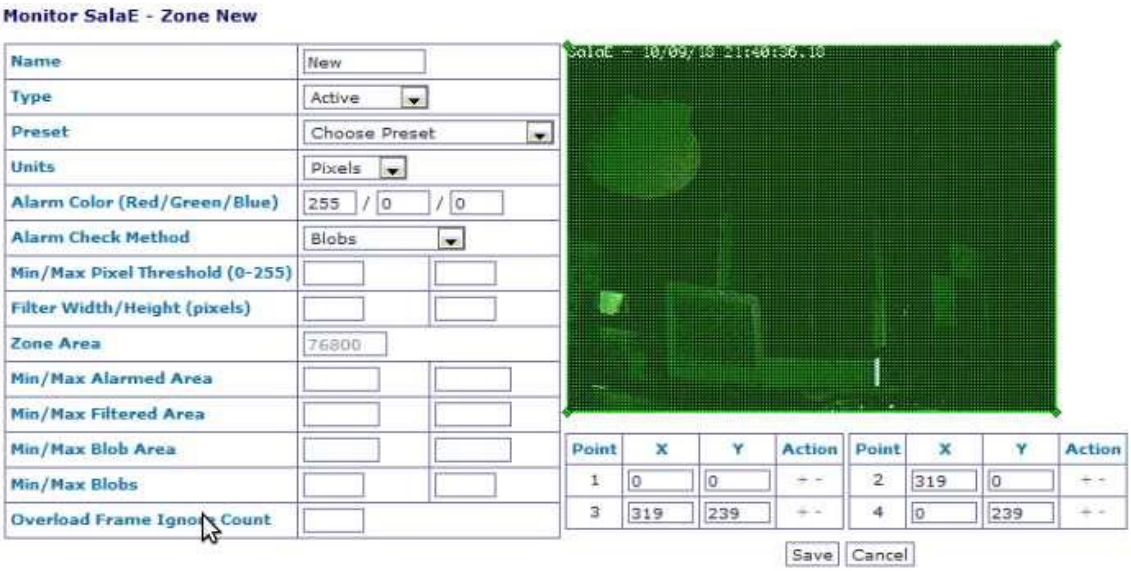


Figura 3.2. Ventana agregar/editar/eliminar Zona de Vigilancia.

A continuación, se analiza cada uno de los campos de configuración.

Campo Nombre (Name Field). Este campo permite identificar con un nombre a la zona de vigilancia

Campo Tipo (Type Field). Este campo permite indicar la función que va a desempeñar la zona de vigilancia, convirtiéndose en uno de los campos más importantes. A continuación se analiza cada uno de los tipos de zonas de vigilancia.

Activa (Active). Esta zona de vigilancia es la más usada y es la zona que se activa automáticamente cuando se crea un monitor. La función de esta zona es activar una alarma que creará un evento cuando se presente movimiento en esta zona.

Inclusiva (Inclusive). Esta zona de vigilancia es usada para zonas que se desea que genere alarmas únicamente si una zona activa ha generado una alarma.

Exclusiva (Exclusive). Esta zona de vigilancia es usada para generar alarmas de prioridad baja, es decir, que genera una alarma cuando existe movimiento dentro de ella, pero no es tan relevante como la alarma que se pueda generar en una zona de vigilancia activa. Esta alarma se activa independientemente de otras alamas.

Pre Exclusiva (Pre Exclusive). Esta zona de vigilancia es usada para impedir que se activen alarmas debido a cambios de luz, sombras, polvo, entre otras. El principal uso de esta zona es para prevenir falsas alarmas.

Inactiva (Inactive). Esta zona de vigilancia es usada para anular la activación de alarmas generadas por cualquier tipo de movimientos o cambios de luz

Campo Peseteados (Presets Field). Este campo permite seleccionar varias configuraciones predefinidas de sensibilidad. Al escoger una configuración predefinida los campos siguientes se autocompletan.

Campo Unidades (Units Field). Este campo permite escoger en que formato se mostrarán las opciones a configurar. Permite escoger entre pixeles o porcentajes. El porcentaje se refiere al espacio de la imagen.

Campo Color de Alarma (Alarm Colour Field). Este campo permite escoger el color que va a identificar a cada una de las zonas. Este color se superpone al color de las imágenes en forma de malla, sin obstruir la visión de la imagen.

Campo Método de Chequeo de Alarma (Alarm Check Method Field). Este campo permite especificar la naturaleza de la alarma, determinando que pudo haberla activado y si esta representa una alarma verdadera para que genere un evento. Este campo contiene tres métodos de comprobación

Pixeles de Alarma (Alarm Pixels). Esta opción indica que únicamente el conjunto de pixeles que generaron una alarma van a ser usados para determinar el estado de la imagen.

Pixeles de Filtrado (Filtered Pixels). Esta opción indica que pixeles deben ser filtrados para eliminar pixeles aislados.

Blobs.Esta opción permite utilizar un análisis más sofisticado para agregar pixeles de alarma. Esta opción requiere más procesamiento por parte del computador.

Campo Umbral Mín/Máximo de Pixeles (Min/Maxium Pixel Threshold Field). Este campo permite definir los límites para diferenciar con un valor a un pixel con otro, en una imagen de referencia**.**

Campo Ancho/Alto de Filtrado (Filter Width/Height Field). Este campo permite mejorar la detección de eventos válidos. ZoneMinder aplica otras funciones para complementar este campo y distinguir eventos de interés de otros que no tienen trascendencia.

Campo Zona de Área (Zone Area Field). Representa el área medida en pixeles definida por la zona de monitoreo. Este campo no puede ser modificado numéricamente, ya que se realiza automáticamente cuando se define un área.

Campo Área Mínima/Máxima de Alarma (Min/Maximum Alarmed Area Field). Estos dos campos permiten definir un número mínimo y un número máximo de pixeles, donde no se generarán alarmas. El valor mínimo es el valor límite en donde no se generará una alarma, superado este valor y por debajo del valor máximo se generará una alarma, si se supera el valor máximo la alarma se cancelará, ya que es muy probable de que se trate de un cambio de luminosidad producido por la luz del sol.

Campo Área de Filtrado Mínimo/Máximo (Min/Maximum Filtered Area Field). Estos dos campos permiten especificar el límite en pixeles que podría generar una alarma después del proceso de filtrado.

IX. Bibliografía

- http://cmt.lugcix.org/?p=138 : vigilancia con software libre
- http://www.zoneminder.com/
- http://www.debian.org/intro/about.es.html
- http://www.foscam-mexico.com
- http://www.redsinfronteras.org
- http://es.wikipedia.org/wiki/Sistema_de_alimentaci%C3%B3n_ininterrumpida
- http://www.videovigilancia.eu.com/blog/videovigilancia/estandar-de-compresion-de-video
- http://es.wikipedia.org/wiki/IEEE_802.11
- http://www.itcom.com/redesinalambricas.htm